€ 40,00

ISBN/EAN
9 788892 136434

R. Cavallo Perin - D.-U. Galetta (*a cura di*) – IL DIRITTO DELL'AMMINISTRAZIONE PUBBLICA DIGITALE

IL DIRITTO DELL'AMMINISTRAZIONE PUBBLICA DIGITALE

a cura di
Roberto Cavallo Perin e Diana-Urania Galetta

Introduzione di **Mario G. Losano**

Coordinamento editoriale di **Gherardo Carullo**

Con le novità del D.L. Semplificazioni (D.L. n. 76/2020 come convertito in legge)

G. Giappichelli Editore

A Gabriella
A Jacques Philippe Emmanuel

INDICE

pag.

II.

IL MERCATO UNICO DIGITALE EUROPEO E IL REGOLAMENTO UE SULLA PRIVACY

Francesco Rossi Dal Pozzo

pag.

III.

DIGITALIZZAZIONE E DIRITTO AD UNA BUONA AMMINISTRAZIONE (IL PROCEDIMENTO AMMINISTRATIVO, FRA DIRITTO UE E TECNOLOGIE ICT)

Diana-Urania Galetta

pag.

IV.
ATTI E PROCEDIMENTI AMMINISTRATIVI DIGITALI

Roberto Cavallo Perin e Isabella Alberti

pag.

V.

IL DOCUMENTO INFORMATICO E IL PROTOCOLLO INFORMATICO

Stefano D'Ancona

VI.

DATI, BANCHE DATI, *BLOCKCHAIN* E INTEROPERABILITÀ DEI SISTEMI INFORMATICI NEL SETTORE PUBBLICO

Gherardo Carullo

VII.

GLI STRUMENTI DELLA CARTA DELLA CITTADINANZA DIGITALE

Stefano D'Ancona e Paolo Provenzano

pag.

VIII.
TRASPARENZA E ACCESSO ALL'EPOCA DELL'AMMINISTRAZIONE DIGITALE

Stefano Rossa

IX.
LA REGOLAZIONE DI FRONTE ALLE SFIDE DELL'ICT E DELL'INTELLIGENZA ARTIFICIALE

Fabiana Di Porto

X.

GLI *SMART LEGAL CONTRACTS*: PROSPETTIVE PER L'IMPIEGO NEL SETTORE PUBBLICO-PRIVATO

Benedetta Cappiello e Gherardo Carullo

pag.

XI.

LA DIGITALIZZAZIONE DEI CONTRATTI PUBBLICI: ADEGUATEZZA DELLE PUBBLICHE AMMINISTRAZIONI E QUALIFICAZIONE DELLE IMPRESE

Gabriella M. Racca

XII.

IL PROCESSO AMMINISTRATIVO TELEMATICO

Federico Gaffuri

pag.

INDICE DEGLI AUTORI

Prefazione

L'innovazione materiale e culturale che l'informatica ha imposto alle scienze giuridiche e alle Pubbliche Amministrazioni ha ormai più di sessant'anni; ciò è avvenuto tra successi innegabili, molte resistenze e reali difficoltà, seguendo percorsi tutt'affatto lineari, come esattamente ricorda Mario G. Losano nell'introduzione al volume.

Raccogliere e interpretare le innumerevoli disposizioni che disciplinano l'amministrazione pubblica digitale, per quanto passaggio necessario, non intendeva ridursi ad un'attività di mera compilazione, finalizzata a sé stessa. L'obiettivo dei curatori di questo volume (la sfida, se vogliamo) è ben più ambizioso: si tratta di tentare di mettere in evidenza e sottolineare come, in sé, l'innovazione tecnologica sia di sistema e come sia dunque proprio da tale esperienza e cultura pregressa che essa trae oggi la forza che le è essenziale per andare oltre.

Tutti coloro che non hanno dubbi nel ritenere che la Pubblica Amministrazione sia un elemento costitutivo della Repubblica italiana, debbono riconoscere nell'Intelligenza Artificiale uno strumento capace di rivelare le oggettive potenzialità dell'amministrare pubblico, le capacità delle organizzazioni pubbliche che a ciò sono preposte, l'innovazione possibile per entrambi.

Dopo le riforme degli anni Novanta – che hanno inteso cambiare le amministrazioni in astratto – è ora il tempo dell'innovare nel concreto "amministrare": di cui occorre perciò conoscere le più intime logiche istituzionali e senza le quali nessuna innovazione è possibile in concreto, poiché trattasi di logiche che le Amministrazioni tramandano in sé medesime, reinterpretando la propria natura e tradizione, di cui occorre cogliere il potenziale (di ciascuna di esse).

Se non è pensabile una buona amministrazione senza la Costituzione è vero altresì che non c'è Costituzione senza una buona amministrazione, poiché trattasi della funzione che più di altre è chiamata a dare soddisfazione dei diritti degli individui, con pieno sviluppo della persona umana.

La buona amministrazione suppone un livello di conoscenza di maggiore potenza rispetto all'attuale, di grande precisione e intima attenzione ai fatti, al

modo di percepirli e di viverli da parte degli individui e delle formazioni sociali in cui si svolge la loro personalità.

Gli strumenti che forniscono le Tecnologie dell'Informazione e della Comunicazione (TIC/ICT) – l'intelligenza artificiale in particolare - consentono all'Amministrazione non solo di percepire esattamente i dati in sé e per sé, che sono nella disponibilità di una Pubblica Amministrazione, ma permettono altresì di cogliere il dato istituzionale dell'amministrazione così come rivelato dalle sue decisioni. Il *data analysis* può infatti mostrare quest'ultimo dato, facendo emergere le tradizioni e i caratteri d'organizzazione che appartengono ai diversi tipi d'amministrazione, infine la disciplina e l'onore di coloro che le impersonano.

Se il tipo di Amministrazione Pubblica è rilevato dall'insieme delle sue decisioni, dai suoi comportamenti nel tempo, in altre parole dal suo "andamento" (art. 97, comma 2, Cost.), appare in sé non più eludibile lo studio sistematico dell'amministrare pubblico e delle sue istituzioni pel tramite dell'Intelligenza Artificiale; intese queste pubbliche amministrazioni non solo più come parti ineludibili del nostro sistema costituzionale, ma anche come capacità che le stesse hanno di definirsi nel tempo come istituzioni.

L'intelligenza artificiale, le reti neurali e i vari altri strumenti che sono oggi disponibili nel contesto della c.d. "amministrazione digitale" consentono non solo di conoscere ciò che un'amministrazione pubblica è, ma soprattutto come la stessa può ed è capace di divenire con le sue decisioni, i suoi servizi pubblici, la fruizione delle sue banche dati: cioè, con la messa a sistema del suo "andamento" come istituzione (art. 97, comma 2, Cost.), che è elemento costitutivo, essenza, del riconoscimento costituzionale dei pubblici uffici.

Ma vi sono due altre ragioni di rilievo che sono tra esse strettamente correlate e che giustificano lo sforzo di coloro che hanno proceduto alla realizzazione del presente volume: liberare le persone dalla paura delle macchine e liberare le persone dal lavoro alienante.

Come si ricorda nel volume «nessun cibernetico aveva mai detto che le valvole pensano, proprio come nessuno ha mai detto che i neuroni pensano. È qui la confusione: a pensare è il sistema nel suo insieme … è la struttura logica di quel sistema, non già la sua particolare forma fisica».

L'intelligenza artificiale intende usare le macchine per riprodurre il pensiero umano, con asservimento di queste all'uomo; certo l'uso di *machine learning* o delle *reti neurali* cambia la capacità delle persone. Ancor più, grazie all'interazione fra intelligenza naturale e intelligenza artificiale esso consente innovazioni significative nel pensiero umano, non diversamente dagli effetti prodotti a suo tempo dal microscopio e dal telescopio.

È molto rasserenante sentirsi ricordare che la stima sul consumo necessario

al cervello umano per produrre le migliori teorie non supera quello di una piccola lampadina e che quello basale per il funzionamento dell'intero corpo umano è stimato in soli 80 watt. Al contrario, l'intelligenza artificiale consuma molta energia sicché dobbiamo rassegnarci a demandare alle macchine solo alcuni compiti oggi disimpegnati dall'uomo, quelli che diventano per l'uomo via via per lui impossibili: perché ripetitivi, troppo onerosi o precisi, comunque alienanti.

Come è giusto che sia dato il tema trattato, che impone necessariamente un approccio rivolto al futuro ed una capacità di proiettarvisi con entusiasmo e passione, si è chiesto a molti giovani di accompagnare i curatori in questo lavoro, ricevendo una forte risposta di partecipazione il cui esito si consegna ora al giudizio dei lettori. La speranza è di riuscire a trasferire in questo anno 2020, senz'altro unico nella sua innegabile complessità, almeno un poco dell'entusiasmo ricevuto.

Ivrea-Stresa, 20 agosto 2020

I curatori

Introduzione

LA LUNGA MARCIA DELL'INFORMATICA NELLE ISTITUZIONI ITALIANE

Mario G. Losano

1. L'Italia, l'amministrazione pubblica e l'informatica, oggi

In Italia i dibattiti non si esauriscono mai, anche se sovente, pur a seguito di ampi e articolati dibattiti, tutto resta nella sostanza uguale, o quasi. Questo vale anche per le discussioni sull'introduzione dell'informatica nella Pubblica Amministrazione: un'esperienza che ho vissuto di persona nel corso di oltre cinquant'anni, durante i quali sono andato scrivendo le mie proposte o le mie critiche. L'insieme di questi miei scritti costituisce un'involontaria cronistoria di quest'evoluzione: può quindi essere utile elencarli alla fine di queste pagine introduttive, mentre – alla fine di ogni paragrafo – il testo in corpo minore fa riferimento agli scritti più pertinenti, indicando fra parentesi quadra il numero d'ordine del singolo scritto.

Il dibattito su quella che si è andata via via chiamando "automazione" o "informatizzazione" o "digitalizzazione" della Pubblica Amministrazione, oppure "*e-government*", è sempre stato presente nei progetti governativi degli ultimi cinquant'anni ed è tornato autorevolmente in primo piano dal 2020 quando, nella speranza di captare i cospicui fondi stanziati dall'Unione Europea per l'Italia, il governo si è proposto di "digitalizzare" l'intero paese, in vista di una "doppia transizione verde e digitale". L'Europa si avvia dunque verso un mercato unico digitale, come illustra Francesco Rossi Dal Pozzo nel capitolo II del presente volume.

L'Italia parte da una posizione svantaggiata, come ricordava Franco Bassanini nel "Corriere della Sera" del 9 agosto 2020: «Trenta anni fa c'era, in Italia (come negli altri maggiori paesi europei), una rete unica di Tlc: quella costruita in concessione da una società controllata dallo Stato (Sip). Era tra le migliori al mondo, tra le prime a sperimentare la fibra. Sip fu poi privatizzata, e in pochi anni piombammo agli ultimi posti nelle classifiche europee». Per tornare a una rete se non unica, almeno unificata, nel dicembre 2015 venne fondata la società "Enel Open Fiber", oggi "Open Fiber", che mira a coprire tutta l'Italia con una rete in fibra ottica. Si potrà così giungere alla "digitalizzazione dell'intero paese", informatizzando – tra l'altro – anche le piccole unità dell'amministrazione locale oggi non servite da alcuna rete.

Però, per raggiungere questa digitalizzazione non basta comperare tante attrezzature informatiche: bisogna anche saperle usare, e proprio qui si manifesta il vero problema dell'Italia. Da un lato, bisogna ristrutturare la gestione sia pubblica sia privata adattandola all'informatica; dall'altro, bisogna preparare le persone all'uso intelligente degli strumenti informatici e, a questo fine, bisogna ripensare o inventare alcuni percorsi didattici negli istituti tecnici e nelle università, come nelle *Fachhochschulen* tedesche (che sono scuole tecniche di livello universitario).

In generale, l'Italia è agli ultimi posti in Europa come numero di laureati; ma, inoltre, è anche arretrata nell'uso degli strumenti informatici. Prima della crisi provocata nel 2020 dalla pandemia, l'Unione Europea aveva analizzato l'informatizzazione degli Stati membri dal 2014 al 2019 e l'Italia si era collocata al quint'ultimo posto per la digitalizzazione di famiglie, imprese e Stato. Il problema era (ed è) la sottoutilizzazione dell'infrastruttura informatica: anche quando l'amministrazione pubblica sarebbe in grado di fornire una buona prestazione informatica, quest'ultima viene attardata da complicazioni burocratiche o giuridiche (come si vedrà fra poco esaminando il diritto compatibile con l'informatica). "Il Sole 24 Ore" del 25 luglio 2019 commentava così quella quint'ultima posizione: «La stima econometrica indica come dalla crescita della dotazione digitale non stia comunque corrispondendo alcun significativo impulso sulla produttività. Ci troveremmo quindi di fronte sia a un problema di dotazione di base, sia a un vero e proprio svantaggio competitivo, determinato dalla presenza di un più debole legame, rispetto ad altre economie, fra innovazione digitale e produttività».

Cerchiamo ora di ricostruire cronologicamente i tempi e i temi di alcuni aspetti di questa evoluzione fatta più di propositi che di realizzazioni.

2. Alle origini dell'informatica giuridica

Durante la Seconda guerra mondiale il calcolo elettronico aveva ricevuto un forte impulso a fini militari, soprattutto per aiutare i fisici che lavoravano alla bomba atomica (negli Stati Uniti) o i matematici che infrangevano la crittografia dei militari tedeschi (in Gran Bretagna). Con la fine della guerra questa tecnologia poté essere usata a fini civili e si diffuse perciò dapprima nell'economia privata, poi negli apparati statali.

Questa genesi nel mondo anglo-americano implicava però una concezione del diritto diversa da quella del mondo europeo-continentale. Il *Common Law* si fonda sul precedente giurisprudenziale, mentre il *Civil Law* si fonda sulla norma legislativa. Poiché le prime case costruttrici di elaboratori elettronici erano statunitensi, i primi programmi per il reperimento delle informazioni vennero applicati alle raccolte di sentenze. Questo modello di applicazione dell'informatica al diritto interessava gli europei soprattutto dal punto di vista tecnologico, ma un vero interesse pratico giunse soltanto con la costruzione di banche di dati legislativi, e non giudiziari.

I politici e gli imprenditori europei si rendevano conto del potenziale ancora incommensurato della tecnologia informatica ed erano sottoposti alle pressioni delle grandi case costruttrici americane (per esempio, IBM o Honeywell), che attraverso il gigantesco mercato interno statunitense finanziavano la propria ricerca e sviluppo. Il *computer* e la cibernetica – questa la terminologia originaria – avevano ormai una rilevanza strategica negli anni della Guerra fredda e gli Stati europei, per evitare una totale sudditanza tecnologica rispetto agli Stati Uniti, crearono delle società nazionali per la costruzione degli elaboratori elettronici, riservando loro più o meno tacitamente il mercato della Pubblica Amministrazione.

Tra la fine degli anni '60 e gli anni '70 nacquero così la «Compagnie Internationale pour l'Informatique» (CII) in Francia e la «International Computers Limited» (ICL) in Gran Bretagna, nonché i settori informatici della società Siemens (la divisione «Siemens Data») e dell'Olivetti, la cui «Divisione elettronica» costruì dal 1957 l'Elea, il primo elaboratore elettronico italiano. Tutte le imprese europee ebbero una vita difficile, nonostante l'appoggio del proprio Stato; e particolarmente difficile fu la vita della Divisione Elettronica dell'Olivetti, che non ebbe neppure quell'appoggio.

Usando programmi per il reperimento dell'informazione (*information retrieval*) di origine statunitense o nazionale, nacquero così varie banche di dati giuridici. In Italia è rilevante il Sistema Italgiure della Corte di Cassazione, ampiamente documentato in Internet, che fa capo a un importante centro di calcolo interno alla Cassazione stessa.

Invece le regioni, costituite nel 1970 ed effettivamente operanti dal 1972, non avevano all'inizio le competenze interne per affrontare l'informatica giuridica o gestionale e perciò ricorrevano a collaborazioni esterne. Fu così che nel 1972 il Consiglio della Regione Lombardia mi affidò il progetto della prima banca di dati legislativi lombardi, che conclusi nel giugno del 1974. Se si legge oggi la relazione (ciclostilata) di quell'esperimento ci si rende conto dell'incredibile progresso compiuto dall'informatica in mezzo secolo, come è documentato nel testo di Gherardo Carullo nel capitolo VI del presente volume. Per esempio, i 6791 documenti («nel senso di articolo di legge o partizione equivalente») costituivano una quantità oggi considerata minima e gestibile con un *laptop* (ma allora occorreva un *mainframe*); ciascuno dei documenti veniva immesso nel *mainframe* attraverso una decina di schede (cartacee) perforate (con una macchina meccanica) per l'elaboratore: una montagna di carta.

In seguito, con la crescente rilevanza dell'informatica nella gestione pubblica, anche le regioni istituirono una propria infrastruttura informatica: la Regione Lombardia, per esempio, istituì nel 1981 la «Lombardia Informatica SpA» e soluzioni analoghe vennero adottate dalle altre regioni italiane, in parallelo con quanto avveniva anche nell'amministrazione pubblica centrale.

Riferimenti

Sulla storia generale dell'informatica [32]. – Sulle vicende dell'Olivetti avevo affidato una tesi a Lorenzo Soria, oggi affermato giornalista negli Stati Uniti, pubblicata nel 1979 da Einaudi con un titolo eloquente: *Informatica: un'occasione perduta. La Divisione elettronica dell'Olivetti nei primi anni del centrosinistra*. – Sugli inizi dell'informatica giuridica in Europa: *Judac* – acronimo ricavato *Jurisprudence – Data Processing – Cybernetics* – è una bibliografia di quasi 9000 titoli in inglese, tedesco, francese e russo pubblicata nel 1971 da Wilhelm Steinmüller. – Storia del calcolo e storia sociale [279] – Sulla storia dell'informatica giuridica in Italia [39-40] [258] [302] [320] [313]. – Sull'informatica giuridica nel mondo occidentale [37-40] [43-46] [56] [58] [64] [258]. – Sull'informatica giuridica nell'Europa dell'Est [31] [80-81] [234] – Altri dati bibliografici: [143] [150]. – Sull'esperimento della banca di dati legislativi della Lombardia: [6] [8] [11]. – Sull'organizzazione dell'informatica regionale [60] [76] [84].

3. L'insegnamento dell'informatica giuridica in Italia: note personali

Nel dopoguerra l'uso degli elaboratori elettronici si è inserito progressivamente in un mondo organizzato in base a tecnologie completamente diverse. Quindi bisognava anzitutto preparare al lavoro informatizzato un personale abituato al tradizionale lavoro burocratico. E bisognava preparare non soltanto il personale destinato a guidare a ogni livello i processi di automazione pub-

blica e privata, ma anche il personale che, ai margini, ne poteva temere negative conseguenze indirette sulla propria attività e che, quindi, avrebbe potuto essere un potenziale avversario delle applicazioni informatiche. L'avvento dell'informatica comportava quindi un vasto compito pedagogico.

Avevo avuto il mio primo incarico d'insegnamento nel 1968, quando già da qualche anno mi interessavo all'informatica. Venivo dal liceo classico e mi ero laureato in giurisprudenza, quindi il mio interesse per l'informatica non nacque nell'ambiente culturale da cui provenivo: esso venne da mio padre, che fu tra i primi in Italia a introdurre gli elaboratori IBM nella società di assicurazioni dove lavorava. Attraverso di lui non solo ebbi notizia delle possibili applicazioni e dei problemi concreti dei "cervelli elettronici", ma venni anche presentato alle case costruttrici presso le quali frequentai i corsi destinati ai clienti presenti e futuri. L'università italiana non aveva ancora delle facoltà di informatica, e quanto si insegnava nelle facoltà tecniche non era accessibile con la mia preparazione.

A Torino io lavoravo con Norberto Bobbio nell'università e nella casa editrice Einaudi e quelli erano gli anni in cui Bobbio si occupava anche di logica applicata al diritto: in quel contesto si formò l'amico Amedeo Conte, che divenne il maggior cultore di logica deontica in Italia. La logica formale mi sembrava troppo astratta e lontana dalla mia preparazione di giurista, ma trovai la mia via quando frequentai un corso della società IBM sulla "logica della programmazione": era il connubio tra teoria e pratica di cui andavo in cerca. Il passo successivo fu una sistematica applicazione al diritto della "logica della programmazione" e dell'informatica, che allora si chiamava "cibernetica". Nel 1969 pubblicai il mio libro *Giuscibernetica*: e, dopo queste poche righe, il lettore comprenderà perché esso è dedicato a mio padre.

A Milano mi proposi di introdurre i miei studenti allo studio (e anche, se possibile, alla concreta applicazione) dell'informatica giuridica. Il loro interesse fu subito vivo, ma le difficoltà sorgevano dal fatto che l'università italiana – come del resto quasi tutta l'amministrazione pubblica – aveva una struttura pre-informatica. Titolare della cattedra di «Teoria generale del diritto», insegnavo l'informatica giuridica per così dire sottobanco. Per i laureati nella mia materia, poi, lo sfasamento era ancora più grave: essi preparavano e difendevano una tesi di informatica giuridica, ma ai colloqui di lavoro si presentavano come laureati in teoria generale del diritto o in filosofia del diritto: materie non proprio appetibili per l'ufficio del personale di un'impresa.

Gli studenti sono come i vini: vanno ad annate. L'annata 1971 fu eccezionale per la sintonia che si creò in aula intorno a quella nuova materia che non esisteva neanche nel curriculum universitario. Nelle lezioni sviluppai gli aspetti più concreti che erano appena accennati nel libro *Giuscibernetica*: presero

così corpo le varie edizioni del *Corso di informatica giuridica*, che andarono progressivamente arricchendosi negli anni successivi fino a raggiungere i tre volumi nell'edizione 1985-86. Un'eco di quell'affiatamento si ritrova negli esempi che evocano i nomi di Ermanno e di Cesarina, due svegli studenti di quell'annata irripetibile.

All'inizio degli anni Settanta l'elaboratore elettronico era entrato in forma pienamente operativa nel mondo civile provenendo da quello militare e lo si percepiva come una Minerva tecnologica nata d'un tratto dalla mente di un Giove angloamericano. In un corso universitario era necessario spiegare anche l'origine e l'evoluzione di quella macchina prodigiosa. A questo fine la storia del calcolo – da quello meccanico a quello elettronico – mi sembrò offrire un buon radicamento culturale per quella giuscibernetica ancorata al presente e proiettata sul futuro: si ricollegava così una tecnologia contemporanea alla preparazione umanistica dalla quale provenivamo tanto io quanto i miei studenti.

La società Siemens Data – nella cui filiale italiana ero consulente dell'amministratore delegato – aveva pubblicato in Germania nel 1966 il libro su Leibniz *Rechnung mit Null und Eins* (calcolo con uno e zero), che pubblicai in italiano nel 1971: i miei studenti ritrovavano così un filosofo dei loro anni liceali come autore della matematica binaria che stavano studiando nell'informatica. Poi, all'Accademia delle Scienze di Torino, scoprii un manoscritto di Charles Babbage e un piano della sua macchina che anticipava la programmazione: quei documenti erano conservati nell'Accademia torinese perché nel 1840 Babbage aveva presentato a Torino la sua "macchina alle differenze", progenitrice del calcolatore programmato. Da Babbage passai allo svedese Georg Scheutz, che dotò quella macchina di una stampante, e al tedesco Konrad Zuse, che costruì un elaboratore nella Germania in guerra.

Le strutture meccaniche della macchina di Babbage venivano dalla meccanica greco-classica, giunta sino noi attraverso la mediazione della cultura araba: nella biblioteca di Oxford scoprii un *codex bombicinus* con affascinanti illustrazioni di automi arabi del XIII secolo; e da quelli passai poi agli automi europei, additando in essi gli antenati della robotica.

Il mio interesse per l'editoria era legato anzitutto alla mia attività nella casa editrice Einaudi, ma ben presto – cioè del 1966 – esso si intrecciò con il mio interesse per l'informatica. Quest'ultima muoveva allora i primi passi nelle case editrici che usavano tipografie che stampavano "a caldo", cioè con linotype con piombo fuso, ma che passarono ben presto a tecniche informatizzate di stampa su carta, per poi abbandonare il supporto cartaceo a favore di nuove tecniche, quali ad esempio il *compact-disc*, o CD-Rom. La fusione di questo mio duplice interesse si materializzò nella produzione dell'Enciclopedia Ei-

naudi su CD-Rom: lo "scrivere con il laser" era una nuova tecnica destinata ad essere applicata ad altri miei esperimenti editoriali.

Però la rapida evoluzione del mondo informatico portò a superare il CD-Rom con i libri elettronici (*e-books*) e con testi in linea distribuiti con Internet. Il mio CD-Rom delle sentenze del Tribunale di Milano venne sostituito da una banca di dati in linea. Ma, come sempre avviene, le nuove tecnologie non sostituirono del tutto l'ormai invecchiato CD-Rom, che conservò una sua vita di nicchia nell'ambito della memorizzazione di dati troppo vasti per essere stampati: oggi lo si trova ancora in una tasca della retrocopertina di libri che vi conservano masse di dati non stampabili. Questo passaggio alla tecnologia di nicchia è una storia che si ripete: la biro non ha sostituito la stilografica, né l'orologio digitale quello meccanico; i modelli obsoleti sono divenuti modelli di nicchia e, spesso, di lusso.

Il progressivo passaggio dal libro cartaceo a quello digitale (e, in generale, dal documento cartaceo a quello digitale) era però accompagnato dalla convinzione che il testo digitalizzato fosse tanto durevole quanto quello stampato: era generalizzato il tacito ma errato convincimento che un CD-Rom fosse durevole quanto una cinquecentina di Aldo Manuzio. In realtà, invece, tutto ciò che è digitale è precario: nel costruire i propri archivi bisogna tenere ben presente la volatilità dei documenti informatici: sul supporto informatico, *scripta volant*.

La mia passione per l'insegnamento dell'informatica giuridica non era però condiviso dall'università italiana. Presso l'università di Torino avevo fondato un Centro di Giuscibernetica, che durò tre anni soprattutto grazie all'appoggio dei colleghi stranieri. Il ministero riconobbe molto tardi l'«Informatica giuridica» come materia ufficiale. Solo l'Università del Piemonte Orientale, grazie alla lungimiranza del suo rettore, mi consentì nel 2002 di fondare un corso interfacoltà triennale di informatica giuridica, al quale partecipavano le facoltà e i docenti tanto della Facoltà di Matematica e Fisica (presso la quale passai tre anni), quanto della Facoltà di Giurisprudenza, dove il corso si assestò fino al 2009, quando io andai in pensione. E la facoltà chiuse seduta stante il corso.

Oggi quasi tutte le ex-facoltà di giurisprudenza hanno un insegnamento di informatica giuridica, intesa spesso come diritto dell'informatica (cioè come norme giuridiche regolanti l'informatica: per esempio, le norme sulla privacy), piuttosto che come informatica giuridica in senso proprio (cioè come applicazione dell'informatica a strutture pubbliche regolate dal diritto: per esempio, l'automazione del sistema fiscale).

Riferimenti

Sugli inizi del mio insegnamento dell'informatica giuridica [1-3] [52] [201] [283] [320] e i miei manuali [16-17]. – Sul Centro di Giuscibernetica, Torino, [49] [57]. –

Sul mio corso triennale di informatica giuridica [299] [309]. – Sulla storia del calcolo meccanico [9] [29] [73] [78] [146]. – Sugli automi, precursori della robotica [21] [105] [182] [286] [294] [307] e sugli automi arabi [14] [24] [297]. – Sui precursori del calcolo automatico: Babbage [5] [26] [41] [54] [251] [312] [314-315] – Leibniz [51] – Scheutz [7] [27] [65] – Zuse [28] [69] [71] [83] [310-311]. – Sul CD-Rom (Compact Disc-Read only memory) [18] [33] [36] [169] [171] [177] [186] [188] [190] [194] [202] [205] [210] [212-213] [235] [239]. – Sulla volatilità dei supporti informatici [323].

4. Per un diritto compatibile con l'informatica

Uno dei compiti fondamentali dell'attuale governo italiano, anche per gli impegni presi con l'Unione Europea, è la transizione digitale, in particolare nell'amministrazione pubblica. Per questa via si può perseguire anche un'altra finalità dichiarata prioritaria: la semplificazione e sburocratizzazione dell'intero apparato statale. Quest'apparato è oggi organizzato secondo norme giuridiche emanate quasi per intero in epoca pre-informatica, che quindi spesso ostacolano o rendono impossibile l'informatizzazione. Bisogna dunque riformare quelle norme vecchie e, al tempo stesso, aver cura che le nuove norme siano compatibili con l'informatizzazione.

Avevo segnalato ai giuspubblicisti quest'esigenza nel 1971, richiamando anche l'attenzione sulle disposizioni emanate dal Land della Baviera: queste ultime erano raccomandazioni di tecnica legislativa, e non norme giuridiche, perché sarebbe stato incostituzionale vincolare l'attività dell'organo legislativo. Inoltre quest'attenzione alla "informatizzabilità" delle disposizioni valeva per tutti i livelli dell'apparato statale, perché l'informatica è per sua natura pervasiva ed era quindi destinata a diffondersi a tutti i livelli dell'apparato pubblico. In questo modo l'insegnamento delle tecniche legislative entrava a far parte dell'insegnamento dell'informatica giuridica. Su questi temi tenni vari corsi presso gli uffici legislativi delle regioni Lombardia e Piemonte.

In particolare, la tecnica legislativa tradizionale strutturava in modo lineare le procedure regolate dal diritto, prevedendo che ad ogni alternativa si rispondesse soltanto nel senso che consentiva di progredire al passo successivo della procedura stessa. L'esempio classico è quello della norma di diritto tributario (fittizia) che preveda per una famiglia numerosa lo sgravio del 25% sull'imposta sul reddito. Per essere automatizzabile, quelle disposizioni devono quantificare che cosa è una famiglia numerosa (per esempio, "uguale o maggiore di 4 figli"): questa precisazione non può essere affidata al programmatore, perché così egli si sostituirebbe all'organo legislativo. Inoltre la disposizione è formulata in modo da essere applicata a una famiglia numerosa, perché è evi-

dente che se la famiglia non è numerosa la norma non si applica. Però quello che è "evidente" per il funzionario non lo è per il computer, al quale (mediante il programma) bisogna porre il quesito se la famiglia è numerosa o no, per poi indirizzarlo – in base alla risposta – su un ramo del programma nel caso che la risposta sia positiva, e su un altro ramo in caso di risposta negativa: questa seconda opzione è generalmente assente dai testi legislativi tradizionali. Oggi l'automazione delle procedure giuridiche è così avanzata che l'amministrazione pubblica sta giungendo ormai alla "decisione automatizzata", esaminata da Roberto Cavallo Perin e da Isabella Alberti nel capitolo IV del presente volume.

Il diritto compatibile con l'informatica è quindi più preciso e dettagliato di quello tradizionale, perché commisurato a una specifica situazione burocratica o sociale. Qui però si incontra il limite della tecnica legislativa per produrre una norma compatibile con l'informatica: la norma risulta superata al mutare della situazione burocratica o sociale. Nell'esempio precedente, l'analisi sociologica indicava come "numerosa" la famiglia con quattro figli; tuttavia, di fronte alla denatalità odierna, sarebbe equo applicare la riduzione fiscale a una famiglia con due figli. La norma formulata in modo tradizionale affidava al funzionario o al giudice lo stabilire che cosa significasse "numeroso", ed era quindi più flessibile della norma informatizzabile, per la quale quattro significa quattro, e basta. Se si vuole adeguare il diritto alla realtà, bisogna abrogare la norma vecchia e sostituirla con una nuova.

La qualità della formulazione tradizionale del diritto è messa in luce dal diritto civile tedesco vigente: esso si fonda sul "Bürgerliches Gesetzbuch" (BGB), entrato in vigore il 1° gennaio 1900 dopo un dibattito iniziato nel 1881. Esso ha potuto tenere il passo con la radicale trasformazione sociale della Germania perché l'interpretazione consente di adattare le sue norme alla realtà in continuo mutamento.

In conclusione, il diritto compatibile con l'informatica esige una manutenzione più frequente ed oculata rispetto a quella della normativa tradizionale. L'analisi sociologica diviene quindi uno strumento essenziale per il diritto compatibile con l'informatica.

In generale, si può introdurre l'informatica in una struttura pubblica preesistente e complessa solo riformando, spesso radicalmente, la struttura stessa: per questo, nel suo programma del 2020, il governo italiano associa la "digitalizzazione" con la "semplificazione" della burocrazia.

La concreta rilevanza delle tecniche legislative è però limitata da un fatto: gli uffici legislativi preparano un testo che tiene conto *anche* delle esigenze informatiche, ma che deve essere discusso in aula e approvato dopo un dibattito parlamentare, nel quale il testo originario può essere modificato in base agli emendamenti presentati dai vari partiti. In una coalizione politica conflittuale,

l'approvazione in aula di un testo si raggiunge spesso attraverso formule di compromesso per loro natura imprecise, e quindi non informatizzabili. Insomma, come ebbe a dire un frustrato tecnico del *drafting*, le tecniche legislative quando funzionano non sono necessarie, e quando sarebbero necessarie non funzionano.

Le tecniche per la stesura di testi giuridici sono rilevanti anche per i privati e per questo il loro insegnamento è utile in una facoltà di giurisprudenza, i cui laureati non diverranno tutti parlamentari, ma diverranno quasi tutti estensori testi giuridici. I contratti informatici meritano una speciale attenzione, perché essi devono tenere conto che in generale i contraenti sono tre: il committente, il fornitore del software e il fornitore del hardware. I diritti e i doveri di ciascuno devono essere accuratamente precisati, affinché sia chiaro chi è il responsabile di un eventuale malfunzionamento. Si è quindi sviluppata una tecnica per la stesura dei contratti informatici, che è stata illustrata anche agli studenti di giurisprudenza come caso specifico – e particolarmente complesso – di stesura di un documento giuridico tra privati. In presenza di un'avanzata automazione dell'amministrazione pubblica assumono particolare rilevanza alcune tipologie specifiche di contratti, come quella per gli appalti pubblici analizzata da Gabriella Racca nel capitolo XI del presente volume.

Riferimenti

Sul diritto compatibile con l'informatica: in generale [53] e in Baviera [61]. – Sulle tecniche legislative [113] [300]; e sulle difficoltà connesse [67] [178]. – Per informatizzare un settore giuridico, è necessario analizzare le procedure giuridiche (e in passato era stata d'aiuto la diagrammazione a blocchi) [10] [20] [87] [90] [115] [275]. – L'automazione dell'apparato statale esige riforme, che vanno preparate con analisi anche sociologiche [42] [59] [72] [91] [155] [304]. – Sull'informatizzazione di atti comunali e provinciali [293]. – Sulla redazione dei contratti informatici: [127] – Sui miei corsi sulle tecniche legislative: [15] [271].

5. Le leggi sulla tutela della riservatezza individuale, o privacy

Le tecniche per la memorizzazione dei dati erano in origine lente e laboriose: i dati iniziali erano in generale registrati su carta; di lì venivano poi passati su schede perforate; l'apposito lettore di schede le trasmetteva poi alla memoria dell'elaboratore. Una prima semplificazione venne dalle macchine di *data entry* che registravano i dati su un supporto magnetico direttamente trasferibile all'elaboratore. Col passare del tempo, l'immissione venne resa sempre più rapida e diretta dalla scansione dei dati cartacei (in constante diminuzione) e

dal fatto che i dati originari erano sin dall'inizio registrati su supporto magnetico (in costante crescita). In parallelo, aumentava enormemente la velocità di elaborazione e la capacità di memoria degli elaboratori. Inoltre essi non erano più isolati in un "centro di calcolo" a sé stante, ma venivano uniti dapprima con cavi telefonico, poi con Internet (altro strumento informatico passato dal mondo militare a quello civile). Insomma, la massa di dati cresceva a dismisura e veniva elaborata a velocità sovrumane, mentre la progressiva diffusione dell'informatica negli uffici tanto privati quanto pubblici coinvolgeva i dati di un numero crescente di cittadini. Di fronte a questa trasformazione dell'amministrazione pubblica, il cittadino chiedeva che si tenesse conto delle sue esigenze di sapere tempestivamente che cosa si faceva con i suoi dati, per potervi accedere ed eventualmente correggere; chiedeva cioè che si riconoscesse quel "diritto alla buona amministrazione" (informatizzata) esaminato da Diana Urania Galetta nel capitolo III del presente volume.

Poi le banche di dati cominciarono a colloquiare tra loro, cioè a scambiarsi i dati (anche di privati cittadini) al di fuori d'ogni regola giuridica: come sempre, il diritto giungeva in ritardo rispetto all'innovazione tecnologica. Il cittadino scopriva così che la società di assicurazione gli aveva stornato la polizza perché sapeva di una sua insufficienza cardiaca; l'ufficio delle imposte gli chiedeva conto di certe transazioni che il cittadino riteneva occulte; e così via. In Europa, soprattutto nei paesi scandinavi, il cittadino cominciò a sentirsi osservato da tutti i lati: questa "sindrome del pesce rosso" è all'origine delle prime leggi sulla protezione dei dati personali, cioè sulla privacy. (Simmetricamente, il cittadino divenuto trasparente cominciò ad esigere che fosse trasparente anche lo Stato informatizzato, come documenta Stefano Rossa nel capitolo VIII del presente volume).

Negli anni '70 si sviluppò un ampio dibattito che coinvolse politici, giuristi e privati cittadini e che portò all'emanazione delle prime leggi sulla protezione dei dati personali (*privacy*) con normative dapprima dei singoli Stati e, in seguito, anche dell'Unione Europea, che nel 1995 emanò la Direttiva 95/46 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati, sostituita nel 2016 dal Regolamento Generale sulla Protezione dei Dati, sovente citato in Italia come "*General Data Protection Regulation*" (GDPR, v. capitolo II, F. ROSSI DAL POZZO). Le norme sulla protezione dei dati personali costituiscono oggi il settore più sviluppato del diritto dell'informatica.

Su questa legislazione l'Italia si muoveva con notevole ritardo, nonostante il vivace dibattito culturale e politico. Limitandomi alla mia esperienza diretta, dalla metà degli anni '70 andavo illustrando la normativa straniera nei corsi universitari e sulla stampa specializzata: la legge tedesca entrò in vigore nel 1978 e un mio articolo del 1977 ne commentava gli aspetti salienti. Nel 1987 pubblicai anche una proposta di testo legislativo sulla privacy. Finalmente,

l'Italia emanò la sua Legge n. 675 il 31 dicembre 1996: l'ultimo giorno utile per non incorrere nelle sanzioni dell'Unione Europea. Ancora una volta, fu la Grecia a salvare l'Italia dall'essere l'ultima della classifica, perché la Grecia approvò la sua legge sulla riservatezza il 19 marzo 1997.

Un altro settore legislativo che è andato acquistando rilevanza è quello della protezione dei programmi, che per chi li produce rappresentano spesso un rilevante investimento: la protezione legislativa dei programmi (o *software* o, come si usa ultimamente, algoritmi), come di ogni altro prodotto dell'attività intellettuale, è oggetto di specifiche leggi che non è qui possibile esaminare e per le quali si rinvia all'apposita letteratura.

L'avvento di Internet, il collegamento fra le ormai innumerevoli banche di dati, le possibilità di furti di dati oppure di una loro alterazione e distruzione ha ormai creato una vivace branca nel vasto ambito dei *computer crimes*. A ogni violazione corrisponde una difesa e a ogni difesa un ulteriore tentativo di violazione: il sistema delle banche di dati interconnesse è ormai divenuto l'arena mondiale d'un infinito gioco di guardie e ladri.

Riferimenti

Sulla genesi e struttura della legge italiana sulla privacy: [34-35, commentario a questa legge] [106] [110] [119] [125] [131] [174: mia proposta di legge] [185] [215] [264] [237] [273] [287-291] [295] [305]. – Notizie su varie leggi sulla privacy: – in Europa [93] – in Brasile [208] [240] – in Colombia [207] [227] – in Francia [89] [129] [153] – in Germania [75] [97-99] [116] [151] [236] [319] – in Giappone [245] – in Gran Bretagna [137] [160] [230] – in Spagna [261] [267] [277-278] [285]. – Sulla protezione legislativa del *software* [121] [153] [156] [168] [172] [176] [197] [262] [270] – Sull'apparato statale e la trasparenza, la privacy e il segreto [305] [318].

6. L'informatica, una tecnologia sempre più pervasiva

Fin qui abbiamo seguito il diffondersi dell'informatica soprattutto in alcuni settori della vita pubblica: oggi viviamo in una società informatizzata, nella quale la tecnologia permette di integrare segmenti di vita sociale finora separati. Oggi la Pubblica Amministrazione dei vari Stati è informatizzata (in varia misura), come ho cercato di documentare nel corso degli anni. L'informatizzazione statale è solo un aspetto dell'informatizzazione globale: infatti non c'è settore della vita umana che si sia sottratto a questo processo: dalle assicurazioni alle biblioteche, dai giornali alla criminalità.

Oggi tutto ciò che è informatizzato è "smart": è *smart* la *city*, la *house* o *home* (grazie alla "domotica"), il *working*, la *school*, il *teaching*, il *learning*, il *phone*, persino il *wardrobe*, e così via. Però una realtà è tanto più fragile quanto più è

smart: la società informatizzata è così vulnerabile, che oggi le nuove attività ostili o addirittura belliche hanno per obiettivo le infrastrutture informatiche di una società. Si pensi alle *fake news* accusate di aver alterato le elezioni negli Stati Uniti o all'attacco informatico contro la rete distributiva dell'elettricità o contro quella dei trasporti ferroviari o aerei (attacchi che possono provocare il blocco, o *black-out*, di uno Stato): ormai gli stati maggiori pianificano il "*cyberwarfare*", la guerra elettronica, che presenta notevoli vantaggi rispetto al *warfare* classico.

Qui è inevitabile, e forse utile, una digressione linguistica. Nell'informatica si manifesta appieno l'anglolalìa oggi dominante in una società subalterna al mondo statunitense: società che, non potendo cambiare la realtà, cambia almeno la terminologia che la descrive. I fautori dello *smart thinking* dimenticano però il duplice significato di *smart* illustrato dal Webster: il primo è «to be a source of sharp pain»; il secondo è «sharp or keen», tradotto con "intelligente"; e lo stesso dizionario riconduce l'etimologia di *smart* al tedesco *Schmerz* (dolore) e al latino *mordēre* (mordere).

Siamo di fronte alla recezione acritica, nella lingua italiana, di vocaboli inglesi di cui esiste spesso un accettabile equivalente italiano. Nei tre volumi del 1985-86 del corso di informatica giuridica avevo tentato di usare una terminologia italiana ogni volta che fosse assennatamente possibile: esempio rimasto isolato. Tuttavia la diffusione dei termini inglesi a scapito di quelli italiani è anche dovuta al fatto che la costituzione italiana non indica l'italiano come lingua nazionale: i padri costituenti erano ancora sotto l'influenza dell'italianizzazione forzata introdotta dal fascismo (in base alla quale si doveva dire non *cognac*, ma – su proposta di Gabriele D'Annunzio – *arzente*; non *garçonnière*, ma *ragazziera*) e proprio per questa ragione essi stabilirono espressamente nell'art. 6 che «la Repubblica tutela con apposite norme le minoranze linguistiche», in precedenza represse.

Invece l'art. 2 della costituzione francese del 1958 si apre con le parole: «La langue de la République est le français». Quest'asserzione è tradotta in pratica dalla "Loi Toubon" – *Loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française* – che regola l'uso della lingua francese nell'ambito pubblico: infatti l'obbligo di usarla anche nell'ambito privato violerebbe la libertà d'espressione. Già prima di questa legge il francese aveva coniato il termine "informatica", crasi di "information automatique", nonché vari altri neologismi, alcuni fortunati (come *ordinateur* invece di *computer*; *logiciel* invece di *software*), altri meno fortunati (come *courriel* invece di *e-mail*; *hameçonnage* invece di *phishing* [da *hameçon*, amo: in italiano avremmo "adescamento", il cui uso condurrebbe però a fraintendimenti]). Oggi in Francia i testi legislativi e quelli dell'amministrazione pubblica si attengono alle disposizioni della "Loi Toubon".

Ma ritorniamo alla specifica *smart*-mania dei nostri giorni. La pandemia del 2020 ha diffuso lo *smart working*. La definizione che ne dà il legislatore italiano illustra – come evidenziano i corsivi che seguono – quanta *pain* possa essere contenuta in ciò che è detto *smart*. La Legge 22 maggio 2017, n. 81, definisce lo *smart working* come «una modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con *forme di organizzazione per fasi, cicli e obiettivi* e *senza precisi vincoli di orario* o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa». Ed è l'informatica ad offrire gli "strumenti tecnologici" che rendono possibile lo *smart working*.

Le prime applicazioni dello *smart working* all'amministrazione pubblica hanno generato numerose polemiche, in cui si sosteneva che i funzionari godessero in realtà di cripto-ferie retribuite in un momento di chiusura delle imprese private e, quindi, di disoccupazione diffusa. In realtà, la stessa accusa poteva essere rivolta anche ai dipendenti delle imprese private che avevano optato per lo *smart working*. Di certo, oggi, c'è solo che questa modalità di lavoro troverà varie applicazioni anche dopo la pandemia e che essa comporterà un'invasione (non è prevedibile quanto estesa) della sfera privata del singolo lavoratore, della sua famiglia e del suo domicilio.

In futuro la pervasività dell'informatica sarà moltiplicata dal perfezionamento delle reti (si pensi all'attuale dibattito sulla tecnologia 5G), dall'interconnessione delle banche di dati, dal moltiplicarsi delle reti sociali in cui gli utenti – più esibizionisti che sprovveduti – riversano dati personali anche sensibili sotto forma di parole e immagini. Il diritto tenta di opporre un fragile argine a questo *brave new world* di orwelliana ascendenza: una sfida tanto per il futuro legislatore, che dovrà emanare norme al passo con i ritmi sempre più veloci del progresso tecnologico, quanto per la Pubblica Amministrazione, chiamata ad applicare quelle norme (spesso già obsolete poco dopo il nascere) ad una realtà sociale in rapida, perpetua e imprevedibile evoluzione.

Riferimenti

Sull'informatizzazione della Pubblica Amministrazione in Brasile [203] [253] – in Francia [85] [94] [117] [156] [238] [303] – in Germania [198] [239] [317] – in Giappone [4] [66] [70] [102] [107] [243] – in Gran Bretagna [84] – in Spagna [193] [250]. – Sul flusso transnazionale dei dati [95] [114 [124] [166] [214] [231-232] [248] [291]. – La pervasività dell'informatica può essere illustrata in vari settori: assicurazioni [154] – biblioteche [12] [157] [170] [194] [241] [249] – carte di credito [282] – catasti [63] [217] – censimento [133] [198] – difesa militare [120-121] [148] [179] – editoria [36] [188] [190] [220] – finanza [132] [191] – giornalismo [246] – Islam [25] – impresa [74] [118] [122] [162] [186] [222] – istruzione programmata [47] – lessicografia [50] [276] – letteratura [306] – politica [2] [101] [111] [134]

[136] – sindacati [161] – reati [77] [154] [165] [187] [200] [228-229] [260] [274] [308] [316] – sanità pubblica [247] – scuola [164] [173] – terrorismo, [86] [301] – tribunali [55] [139] [144] [183] [189] [196] [224] [231] – università [108] [145] [163] [192] [206] [255-256] [292].

Mario G. Losano

Scritti di informatica giuridica 1966-2020

La bibliografia di tutti gli scritti di Losano – quindi non solo di quelli legati all'informatica e alla sua storia, come qui di seguito – si trova nel sito www.mariolosano.it. Rispetto a quella bibliografia generale la presente bibliografia adotta una sua autonoma numerazione progressiva. Nel mio testo precedente, i riferimenti bibliografici sono indicati tra parentesi quadra con il numero d'ordine della bibliografia che segue.

Libri

1. *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Einaudi, Torino, 1969, 205 pp. (Piccola Biblioteca Einaudi, n. 125).
2. *Corso di informatica giuridica*, Cooperativa Universitaria Editrice Milanese, Milano, 1971, VI-325 pp. (Centro di Giuscibernetica dell'Università di Torino, Quaderno n. 3).

2.1. *Informática jurídica*, Tradução de Giacomina Faldini, Editora da Universidade de São Paulo-Edição Saraiva, São Paulo, 1976, XVI-255 pp.

2.2. *Corso di informatica giuridica*. Seconda edizione ampliata, Volume 1: *L'elaborazione dei dati non numerici*, Unicopli, Milano, 1981, XXIII-316 pp.

Volume 2: *Il diritto dell'informatica*, Unicopli, Milano, 1981, pp. XXV-(317-)543 pp.

2.3. *Corso di informatica giuridica*. Terza edizione, Volume 1: *L'elaborazione dei dati non numerici*, Unicopli, Milano, 1984, XXXI-317 pp., Volume 2: *Il diritto dell'informatica*, Unicopli, Milano, 1984, XXXI-[317-543] + 16 pp.

2.3.1. *Curso de informática jurídica*, Traducción de Manuel Atienza y Juan Ruiz Manero, Tecnos, Madrid, 1984, 262 pp. [Traduzione del solo vol. 1 del 6.3.]

3. *Lições de informática jurídica*, Curso de extensão universitária no Departamento de direito economico-financiário da Facultade de Direito da Universidade de São Paulo, Seção gráfica do Tribunal de Alçada Criminal, São Paulo, 1973, IV-210 pp.

3.1. *Lições de informática jurídica*, Reprodução eletrofotostática das apostilas, Editora Resenha Tributaria, São Paulo, 1974, XVI-237 pp.

3.2. *Lezioni pauliste di informatica giuridica*, Tirrenia, Torino, 1974, VII-205 pp.

4. *Stato e automazione* [*in Giappone*], Etas Kompass, Milano, 1974, 245 pp.

5. *Babbage: la macchina analitica. Un secolo di calcolo automatico*, Etas Kompass, Milano, 1973, IX-191 pp.

5.1. *La macchina da calcolo di Babbage a Torino*, Olschki, Firenze, 2014, LXVI-170 pp.
6. *Relazione sull'esperimento di information retrieval applicato alla legislazione regionale*, Consiglio regionale lombardo, Milano, 1974, 2 voll., 223 pp.
7. *Scheutz: La macchina alle differenze. Un secolo di calcolo automatico*, Etas Libri, Milano, 1974, 164 pp.
8. *Rapporto sul sistema di information retrieval giuridico del Consiglio regionale lombardo*, Consiglio regionale lombardo, Milano, 1975, 56 pp.
9. *Machines arithmétiques. Invenzioni francesi del Settecento*, Testi originali con 15 tavole dell'epoca, Bottega d'Erasmo, Torino, 1976, VIII-117 pp.
10. *Diagrammazione a blocchi e programmazione reticolare di procedure giuridiche*, Consiglio Regionale della Lombardia, Milano, 1979, III-171 pp.
11. *L'informatica legislativa regionale. L'esperimento del Consiglio Regionale della Lombardia*, Rosenberg & Sellier, Torino, 1979, 144 pp. (La società informatica, n. 1).
12. *Informatica per le biblioteche*. vol. I: *Elementi sull'elaborazione dei dati non numerici*, Assessorato alla Cultura della Provincia di Milano, 1979, 119 pp.
13. *Introducción a la informática jurídica*, Traducción y presentación de Manuel Atienza, Universidad de Palma de Mallorca, Palma, 1982, 107 pp.
14. *Automi arabi del XIII secolo. Dal "Libro sulla conoscenza degli ingegnosi meccanismi"*, Luigi Maestri Editore, Milano, 1982, 94 pp. (con 12 tavole a colori).
15. *Proposte per innovare la tecnica legislativa*. Relazione presentata all'Ufficio di Presidenza della Regione Piemonte il 21 dicembre 1982, Consiglio Regionale del Piemonte, Torino, 1982, 107 pp.
16. *Corso di informatica giuridica*. Seconda edizione ampliata. Volume 3: *L'analisi delle procedure giuridiche*, Unicopli, Milano, 1984, XXI-544-814 pp. [Cfr. nn. 16 e 24; edizione definitiva: cfr. n. 35.]

Corso di informatica giuridica:

17.I. *Informatica per le scienze sociali*, Einaudi, Torino, 1985, XXI-547 pp.
17.II. *Il diritto privato dell'informatica*, Einaudi, Torino, 1986, XVIII-298 pp.
17.III. *Il diritto pubblico dell'informatica*, Einaudi, Torino, 1986, IV-348 pp.
18. *Scritto con la luce. Il disco compatto e la nuova editoria elettronica*, Unicopli, Milano, 1988, 128 pp.
19. *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, 213 pp.
20. *L'informatica e l'analisi delle procedure giuridiche*, Unicopli, Milano, 1989, 388 pp.
21. *Storie di automi. Dalla Grecia classica alla Belle Époque*, Einaudi, Torino, 1990, XXVIII-154 pp.
21.1. *Histórias de autômatos. Da Grécia Antiga à Belle Époque*, Tradução de Bernardo Joffily, Companhia das Letras, São Paulo, 1992, 147 pp.
22. *Saggio sui fondamenti tecnologici della democrazia*, Fondazione Adriano Olivetti, Roma 1991, 82 pp.
22.1. *Saggio sui fondamenti tecnologici della democrazia*, Fondazione Adriano Olivetti, Roma 1991, 82 pp., http://nexa.polito.it/losano-democrazia.

23. *Informatika juridike*, Përkthimi dhe parathënia nga Gjergj Sinani, Istituto per la Documentazione Giuridica, Firenze, 1994, 129 pp.
24. *Automi d'Oriente. "Ingegnosi meccanismi" arabi del XIII secolo*, Medusa, Milano, 2003, 127 pp.
25. *La Rete e lo Stato Islamico. Internet e i diritti delle donne nel fondamentalismo islamico*, Mimesis, Milano, 2017, 169 pp.

Traduzioni – "a cura di".

26. *Babbage: la macchina analitica. Un secolo di calcolo automatico*. A cura di Mario G. Losano, Etas Kompass, Milano, 1973, IX-191 pp.
27. *Scheutz. La macchina alle differenze. Un secolo di calcolo automatico*. A cura di Mario G. Losano, Etas Libri, Milano, 1974, 164 pp.
28. *Zuse. L'elaboratore nasce in Europa. Un secolo di calcolo automatico*. A cura di Mario G. Losano, Etas Libri, Milano, 1975, XVIII-184 pp.
29. *Machines arithmétiques. Invenzioni francesi del Settecento.* Testi originali con 15 tavole dell'epoca. A cura di Mario G. Losano, La Bottega di Erasmo, Torino, 1976, VIII-121 pp.
30. *I calcolatori elettronici. Applicazioni e prospettive*. A cura di Mario G. Losano, Letture di "Le Scienze", Edizione italiana di "Scientific American", Milano, 1976, 258 pp.
31. Viktor Knapp, *L'applicabilità della cibernetica al diritto*. A cura di Mario G. Losano, Einaudi, Torino, 1978, XXXVII-238 pp.
32. Hermann Goldstine, *Il computer da Pascal a von Neumann. Le radici americane dell'elaboratore moderno*. Presentazione di Mario G. Losano, Etas Libri, Milano, 1981, 396 pp.
33. Mario G. Losano – Lothar Philipps, *Diritto e CD-ROM. Esperienze italiane e tedesche a confronto*, Giuffrè, Milano, 1990, XI-118 pp.
34. Ettore Giannantonio – Mario G. Losano – Vincenzo Zeno-Zencovich, *La tutela dei dati personali. Commentario alla L. 675/1996*, Cedam, Padova, 1997, 569 pp.

34.1. Ettore Giannantonio – Mario G. Losano – Vincenzo Zeno-Zencovich, *La tutela dei dati personali. Commentario alla L. 675/1996*, Cedam, Padova, 1999, 569 pp. (seconda edizione).

35. *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*. A cura di Mario G. Losano, Laterza, Roma-Bari, 2001, XX-434 pp.

35.1. *Legea italiană în privinţa protecţiei vieţii private. Un bilanţ al primilor cinci ani*. Traducere: Alina Lazăr; Coordonator traducere şi îngrijirea ediţiei: Mihail-Constantin Eremia, All Beck, Bucureşti 2004, XXIV-480 pp.

Articoli

36. *Nuove tecniche e consuetudine editoriale: un problema giuridico*, "Graphicus", XLVII, 1966, n. 10, pp. 22-23.
37. *Cibernetica e diritto in Europa*, "Il Ponte", XXIII, 1967, n. 12, pp. 1589-1602.

38. *Computers and the Theory of Law*, "Law and Computer Technology", I, 1968, n. 3, pp. 7-9.
39. *L'informatique juridique en Italie*, "Law and Computer Technology", I, 1968, n. 6, pp. 15-17.
39.1. *L'informatica giuridica in Italia*, "Il Ponte", XXV, 1969, pp. 600-3.
40. *Giuscibernetica*, in: *Nuovi sviluppi della sociologia del diritto 1966-1967*. A cura di Renato Treves, Edizioni di Comunità, Milano, 1968, pp. 307-325.
41. *Inventori si nasce* [L'opera di Charles Babbage], "Rivista IBM", VI, 1970, n. 1, pp. 12-17.
42. *The Structure and Function of the KWIC-Index*, in: Valerio Pocar – Mario G. Losano, *Sociology of Law 1960-70. A Bibliographical Survey with a KWIC-Index*, s.l. [Milano] 1970, pp. 5-8.
43. *L'informatique juridique au Congrès Mondial de Bangkok*, in: *Law, The Computer and Government. Le Droit, l'Ordinateur et l'État*. Rapports présentés à la Conférence Mondiale de Bangkok de la Paix Mondiale par le Droit (7-12 septembre 1969). Edited by/publié par Mario G. Losano, Cooperativa Libraria Universitaria Editrice, Torino, 1970, pp. 17-22.
44. *L'informatique et la tradition juridique*, in: *Law, The Computer and Government. Le Droit, l'Ordinateur et l'État*. Rapports présentés à la Conférence Mondiale de Bangkok de la Paix Mondiale par le Droit (7-12 septembre 1969). Edited by/publié par Mario G. Losano, Cooperativa Libraria Universitaria Editrice, Torino, 1970, pp. 25-30.
45. *La "giuscibernetica"*, "Sapere", 1970, n. 728, pp. 44 sg.
46. *Introduzione all'informatica giuridica*, "Civiltà delle macchine", XVII, 1970, n. 6, pp. 22-28.
46.1. *Uvod i pravnu informatiku*, "Zbornik pravnog fakulteta u Zagrebu", XXI, 1971, n. 4, pp. 413-425.
47. *L'istruzione programmata*, "Elettra", 1971, n. 1, pp. 6-8.
48. *La cibernetica, scienza d'attualità*, "Elettra", 1971, n. 2, pp. 8-9.
49. *Il primo anno del Centro di Giuscibernetica dell'Università di Torino*, "Rivista internazionale di filosofia del diritto", XLVIII, 1971, n. 1, pp. 152-155.
50. *Lessicografia computazionale e informatica giuridica*, "Rivista internazionale di filosofia del diritto", XLXIII, 1971, n. 2-3, pp. 349-353.
50.1. *Lexicographie computationelle et informatique juridique*, in: *Linguistica, matematica e calcolatori*. Atti del convegno e della prima scuola internazionale (Pisa, 16/VIII-6/IX/1970), Olschki, Firenze, 1973, pp. 299-303.
50.2. *Lexicografia computacional e informática jurídica*, "Revista de Procuradoria Geral do Estado" (Porto Alegre), 1980, pp. 67-71.
51. *Gli otto trigrammi (pa kua) e la numerazione binaria*, in: Leibniz, *Calcolo con uno e zero*, Etas Kompass, Milano, 1971, pp. 17-37.
52. *La Juricybernétique. Genése et structure d'une discipline*, "Diogène", 1971, n. 76, pp. 99-123.
52.1. *Juricybernetics: genesis and structure of a discipline*, "Diogenes", 1971, n. 76, pp. 93-114.

52.2. *La juricibernética: génesis y estructura de una disciplina*, "Diogenes", 1971, n. 76, pp. 79-95.
52.3. *Pravna kibernetica: geneza i struktura jedne discipline*, "Strani Pravni Zivot", 1971, n. 73, pp. 3-16.
52.4. *Iuscibernetica, geneza şi structura unei discipline*, "Studii şi cercetări juridice", XVII, 1972, n. 3, pp. 447-489.
52.5. *Hojohogaku: sono kigen to kozo*, "Johoshakaigaku-Koza" (Giuscibernetica: genesi e struttura d'una disciplina, in: *Enciclopedia di informatica delle scienze sociali*, a cura di T. Kitagawa, H. Kato, K. Mushakoji, T. Yoshimura, L. Koyama), Gakken, Tokyo, 1973, vol. 6, pp. 15-24.
53. *Per un diritto compatibile con l'elaborazione elettronica*, "Rivista trimestrale di diritto pubblico", XXI, 1971, n. 4, pp. 1823-41.
53.1. *Per un diritto compatibile con l'elaborazione elettronica*, in: *Corso di informatica giuridica*, volume 2, Unicopli, Milano, 1981, pp. 319-341.
54. *Charles Babbage e la programmazione delle macchine da calcolo*, "Atti dell'Accademia delle Scienze di Torino", vol. 106 (1971-72), Accademia delle Scienze, Torino, 1971, pp. 25-37.
55. *Elaboratori elettronici e tribunali*, "Data Report", 1971, n. 3, pp. 2-5.
56. *Computerizing Research in Countries Outside North America: Italy*, "Jurimetrics Journal", XII, 1972, n. 3, pp. 135-39; pp. 150-52.
57. *Il secondo anno del Centro di Giuscibernetica dell'Università di Torino*, "Rivista internazionale di filosofia del diritto", IL, 1972, n. 1, pp. 11-114.
58. *Lo stato attuale dell'informatica giuridica in Europa*, in: *La domanda e l'offerta di giustizia in Italia*, Cedam, Padova, 1972, pp. 91-95.
59. *I compiti della sociologia nella ricerca giuscibernetica*, "Quaderni di sociologia", XXI, 1972, n. 1, pp. 97-109.
59.1. *I compiti della sociologia nella ricerca giuscibernetica*, in: *Corso di informatica giuridica*, volume 2, Unicopli, Milano, 1981, pp. 343-359.
60. *La funzione della banca di dati nell'ordinamento regionale*, "Data Report", III, 1972, n. 2, pp. 32-38.
61. *In Baviera la prima legge sul diritto compatibile con l'automazione*, "Data Report", III, 1972, n. 2, pp. 39-41.
62. *Informatique et développement*, "Informatique et automatique" (Alger) I, 1972, n. 1, pp. 43-5.
63. *Pianificare il territorio con l'elaboratore*, (Storia dei catasti. Le funzioni del catasto italiano. Verso un catasto computerizzato), "Data Report", IV, 1973, n. 2, pp. 33-43.
64. *L'informatica giuridica in Europa*, in: *Atti del colloquio internazionale su informatica e diritto. Efficienza dei sistemi automatici di informazione nella difesa sociale e garanzie dei diritti individuali (Pavia, 15-17 settembre 1972)*, Centro nazionale di prevenzione e difesa sociale, Milano, 1974, pp. 3-27).
65. *La vita di Georg Scheutz (1785-1873)*, in: *Scheutz. La macchina alle differenze. Un secolo di calcolo automatico.* A cura di Mario G. Losano, Etas Libri, Milano, 1974, pp. 7-23.

66. *Elaboratori elettronici e pubblica amministrazione in Giappone*, "Nuovogiappone" (Milano), III, 1975, n. 1, pp. 5-22.
67. *Vischiosità delle strutture amministrative e automazione della pubblica amministrazione*, in: *Atti del Congresso annuale 1975*, Associazione Italiana per il calcolo automatico (AICA), Genova (29-31 ottobre) 1975, pp. 251-254 (ciclostilato).
68. *Problemas de cibernética jurídica*, "Revista da Consultoria Geral do Estado" (Porto Alegre), V, 1975, n. 13, pp. 97-102.
69. *Konrad Zuse e il secolo europeo del calcolo automatico*, in: Zuse, *L'elaboratore nasce in Europa. Un secolo di calcolo automatico*. A cura di Mario G. Losano, Etas Libri, Milano, 1975, pp. IX-XIV.
70. *Elaboratori elettronici e pubblica amministrazione in Giappone*, "Informatica e diritto", 1975, n. 2, pp. 415-431.
71. *Le radici europee dell'elaboratore elettronico*, "Le scienze. Edizione italiana di Scientific American", gennaio 1976, n. 89, pp. 57-72.
71.1. *Presentazione – Le radici europee dell'elaboratore elettronico*, in: *I calcolatori elettronici. Applicazioni e prospettive*. A cura di Mario G. Losano, Le Scienze, Milano, 1976, pp. 7-28.
71.2. *Le radici europee dell'elaboratore elettronico*, in: *Dalla selce all'elettronica. Il cammino della tecnologia*. Presentazione di Giuseppe Biorci, Le Scienze, Milano, 1978, pp. 110-123.
72. *Automazione senza riforme: analisi della situazione dell'INPS*, in: *Atti del congresso annuale 1976*, Associazione italiana per il calcolo automatico (AICA), Milano (27-29 ottobre), 1976, pp. 807-816.
73. *Nota introduttiva*, in: *Machines arithmétiques. Invenzioni francesi del Settecento*. Testi originali con 15 tavole dell'epoca, La Bottega di Erasmo, Torino, 1976, pp. III-VIII.
74. *Gli elaboratori elettronici nel mondo della produzione*, in: *Enciclopedia della Scienza e della Tecnica Mondadori*. Annuario 1977, Mondadori, Milano, 1977, pp. 367-76.
74.1. *L'automazione delle procedure gestionali e le banche di dati*, in: *L'elaborazione elettronica. Principi di calcolo automatico*, Mondadori – The Open University, Milano, 1979, pp. 155-60.
75. *La legge tedesca sulla protezione dei dati*, "Data Report", VII, 1977, n. 2, pp. 11-16.
75.1. *A lei alemã sobre a proteção dos dados*, "Revista da Procuradoria-Geral do Estado" (Porto Alegre), XI, 1981, n. 29, pp. 11-22.
75.2. *La legge tedesca sulla protezione dei dati*, in: *Corso di informatica giuridica*, volume 2, Unicopli, Milano, 1981, pp. 489-507.
76. *Strutture organizzative per l'informatica regionale*, in: *Atti del congresso annuale 1977*, Associazione Italiana per il Calcolo Automatico (AICA), Pisa, 12-14 ottobre 1977, pp. 3-38.
76.1. *Strutture organizzative per l'informatica regionale*, "Sistemi e automazione", XXIV, febbraio 1978, n. 179, pp. 99-103.
76.2. *La situazione italiana*, in: *Corso di informatica giuridica*, volume 2, Unicopli, Milano, 1981, pp. 525-543.

77. *Dispol: un sistema integrato per il perseguimento di reati penali*, "Data Report", VII, 1977, n. 4, pp. 26-29.
78. *Una nuova macchina da calcolo del Settecento*, "Data Report", VII, 1977, n. 4, p. 40.
79. *La protezione dei dati individuali*, "Civiltà delle macchine", XXVI, 1977, n. 3-4, pp. 39-44.
79.1. *La protezione giuridica dei dati individuali*, in: *Corso di informatica giuridica*, volume 2, Unicopli, Milano, 1981, pp. 471-488.
80. *L'informatica nell'Europa orientale e l'opera di Viktor Knapp*, Prefazione a: Viktor Knapp, *L'applicabilità della cibernetica al diritto*, Einaudi, Torino, 1978, pp. IX-XXXVII.
81. *L'informatica amministrativa in Ungheria*, Presentazione a: J.F. Révész e A. Barasz, *Computerized Storage and Retrieval System for State Administration*,
"Informatica e diritto", IV, 1978, n. 1, pp. 51 sg.
82. *L'informatica è uguale per tutti*, "Rivista IBM", XIV, 1978, n. 3, pp. 11-14.
83. *Z3: il computer che ha perso la guerra*, "Data Manager", ottobre-novembre 1978, pp. 52-54.
84. *Il caso del Lamsac inglese: un ente pubblico centrale per l'automatizzazione degli enti locali*, in: *Informatica nelle amministrazioni regionali: esperienze italiane e straniere*, Istituto Regionale di Ricerca, Milano, 1978, volume III, pp. 1-25.
84.1. *Il caso del Lamsac inglese: un ente pubblico centrale per l'automatizzazione degli enti locali*, in: *L'informatica nelle regioni italiane e straniere*. A cura di Guido Martinotti e Francesca Zajczyk, Rosenberg & Sellier, Torino, 1979, pp. 165-179. (La società informatica, n. 3).
85. *Informatica e sovranità nazionale*, Prefazione a: Simon Nora e Alain Minc, *Convivere con il calcolatore*, Bompiani, Milano, 1979, pp. 9-19.
85.1. *Informatica e sovranità nazionale*, in: Simon Nora e Alain Minc, *Convivere con il calcolatore*. Seconda edizione, Bompiani, Milano, 1984, pp. 9-19. [Cfr. n. 136]
86. *Distruggere il calcolatore?*, "Civiltà delle macchine", XXVII, 1979, n. 1-3, pp. 59-64.
87. *Flow Charting and Network Analysis of Legal Procedures*, IVR World Congress, Category III, Paper No. 050, Basel, August 27th – September 1st 1979, pp. 55 (ciclostilato).
87.1. *Flow Charting and Network Analysis of Legal Procedures*, "Datenverarbeitung im Recht", IX, 1980, n. 2, pp. 179-202.
87.2. *Flow Charting and Network Analysis of Legal Procedures*, "Archiv für Rechts– und Sozialphilosophie", 1983, pp. 223-250.
88. *La sindrome del pesce rosso*, in: *La rivoluzione informatica*, Rosenberg & Sellier, Torino, 1980, pp. 51-60 (Le Monde diplomatique, Dossier 5).
88.1. *La sindrome del pesce rosso*, in: *Corso di informatica giuridica*, volume 2°, Unicopli, Milano, 1981, pp. 453-470.
89. *La legge francese sulla protezione dei dati*, "Data Report", X, 1980, n. 1, pp. 26-30.
89.1. *La legge francese sulla protezione dei dati*, in: *Corso di informatica giuridica*, volume 2°, Unicopli, Milano, 1981, pp. 509-524.
89.2. *A lei francesa sobre a proteção dos dados*, "Revista da Procuradoria-Geral do Estado" (Porto Alegre), 1984, n. 39, pp. 13-20.

90. *Computer Analysis of Legislative Procedures*, London School of Economics, Legol Project, London 1980, pp. 15 (ciclostilato).
90.1. *Computer Analysis of Legislative Procedures*, "Annali della Facoltà di Scienze Politiche dell'Università degli Studi di Milano", I, 1981, pp. 219-234.
91. *Sociologia del diritto e informatica giuridica*, "Sociologia del diritto", 1980, n. 3, pp. 181-188.
91.1. *Sociologie juridique et informatique juridique: une mise au point*, in: André-Jean Arnaud, *Critique de la raison juridique*. 1. *Où va la sociologie du droit?*, Librairie générale de droit et de jurisprudence, Paris, 1981, pp. 182-186.
92. *Diritto, logica, informatica*, in: Anna Fiaccadori, *Appunti di logica simbolica*, Unicopli, Milano, 1981, pp. 5-10.
93. *La privacy nelle legislazioni europee*, in: *Privacy e banche di dati*. A cura di Nicola Matteucci, Il Mulino, Bologna, 1981, pp. 51-66.
94. *Le origini del rapporto Tricot*, in: *Informatica e libertà. I diritti del cittadino di fronte all'automazione dei servizi amministrativi*, Rosenberg & Sellier, Torino, 1981, pp. 7-9.
95. *Flusso transnazionale dei dati ed evoluzione del diritto*, "Problemi dell'informazione", VI, 1981, n. 3, pp. 407-412.
96. *Novas técnicas para controlar a eficácia das normas jurídicas*, "Revista de Procuradoria Geral do Estado" (Porto Alegre), 1981, pp. 27-81.
97. *Tre anni di legge bavarese sulla protezione dei dati*. 1. *Origine e strutture sella legislazione bavarese*, "Data Report", XI, 1981, n. 4, pp. 12-15. [Cfr. n. 115.]
98. *La legislazione tedesca sulla protezione dei dati individuali*, in: Camera dei Deputati, *Banche dati e tutela della persona*, Servizio per la documentazione automatica, Roma 1981, pp. 170-183.
98.1. *La legislazione tedesca sulla protezione dei dati individuali*, in: *Banche dati, telematica e diritti della persona*. A cura di Guido Alpa e Mario Bessone, Cedam, Padova, 1984, pp. 275-293.
99. *Tre anni di legge bavarese sulla protezione dei dati. 2. Il rapporto annuale del garante statale dei dati*, "Data Report", XII, 1982, n. 1, pp. 23-25. [Cfr. n. 112.]
100. *Personal computer: ritratti di possibili utenti*, "Ufficiostile", XV, 1982, n. 4, pp. 60-62.
101. *Vom Parteiprogramm zum Gesetz: Probleme der Wirksamkeit*, in: *Studien zu einer Theorie der Gesetzgebung*, herausgegeben von Harald Kindermann, Springer Verlag, Berlin-Heidelberg-New York 1982, pp. 282-293.
102. *Il modello giapponese tra innovazione e tradizione*, "Critica marxista", XX, 1982, n. 5, pp. 115-124.
103. *A chi dare i dati*, "Panorama Mese", I, novembre 1982, n. 3, p. 97.
104. *Giuscibernetica*, in: *Novissimo Digesto Italiano*, Appendice, vol. III, Utet, Torino, 1982, pp. 1077-1098.
104.1. *Introducción a la informática jurídica*. Traducción y presentación de Manuel Atienza, Universidad de Palma de Mallorca, Palma 1982, 107 pp.
104.2. *Juskibernetica*, in: Mario G. Losano, *Informatika juridike*. Përkthimi dhe parathënia nga Gjergj Sinani, Istituto per la Documentazione Giuridica, Firenze, 1994, pp. 13-87.

105. *Macchine utili – macchine futili*, "Prometeo", I, maggio-luglio 1983, n. 2, pp. 68-79.
106. *La legislazione italiana sulla privacy*, "Data Manager", VIII, 1983, n. 21-22, pp. 26-29.
107. *Il personal computer in Giappone*, "Data Manager", VIII, 1983, n. 25, pp. 79-84.
108. *Informatica e nuove esigenze didattiche nelle materie giuridiche*, in: *L'università e l'evoluzione delle tecnologie informatiche*. Atti del convegno, Milano, 15-16 marzo 1983. Testi delle comunicazioni, vol. 2, Milano, 1983, pp. 5.1-5.2.
109. *A pequena e a grande informática jurídica*, "Boletim da Ordem dos Avogados" (Lisboa), maggio 1983, n. 14, pp. 4-9.
110. *I progetti di legge italiani sulla riservatezza dei dati personali*, in: *Integrazione di informatica e diritto*. Atti del convegno FAST, Milano, 1983, pp. 1-15.
110.1. *I progetti di legge sulla riservatezza dei dati personali*, "L'elettrotecnica", LXX, 1983, n. 10, pp. 943-946.
110.2. *I progetti di legge italiani sulla riservatezza dei dati personali*, "Il diritto delle radiodiffusioni e delle telecomunicazioni", XV, 1983, n. 2, pp. 275-283.
110.3. *La tutela della riservatezza in Italia*, "Sistemi e automazione", XXX, 1984, n. 244, pp. 35-38.
110.4. *I progetti di legge italiani sulla riservatezza dei dati personali*, in: *Banche dati, telematica e diritti della persona*. A cura di Guido Alpa e Mario Bessone, Cedam, Padova, 1984, pp. 150-157.
110.5. *I progetti di legge italiani sulla tutela dei dati personali*, Istituto Statistico delle Comunità Europee, Seminario "Tutela della vita privata, informatica e progressi della documentazione statistica"; Lussemburgo, 11-13 Dicembre 1984, Documento n. 7, 16 pp. [ciclostilato].
110.5.1. *Draft Legislation in Italy on the Protection of Personal Data*, Statistical Office of the European Communities, Seminar "Protection of Privacy", Automatic Data Processing and Progress in Statistical Documentation", Luxembourg, 11-13 December 1984, Document no. 7, 16 pp. [ciclostilato].
110.5.2. [ripreso nella versione inglese del volume: *Protection de la vie privée, informatique et progrès de la documentation statistique*. "Informations de l'Eurostat" – Numéro spécial, Office des publications officielles des Communautés européennes, Luxembourg 1986, pp. 275-304.]
110.5.3. *Die Italienischen Gesetzenentwürfe über den Schutz personenbezogener Daten*, Statistisches Amt der Europäischen Gemeinschaften, Seminar "Schutz del Privatsphäre, automatische Datenverarbeitung und Fortschritt der statistischen Dokumentation", Luxemburg, 11. bis 13. Dezember 1984, Dokument Nr. 7, 16 pp. [ciclostilato].
110.5.4. *Les projets de loi sur la protection des données à caractère personnel en Italie*, Office Statistique des Communautés Européennes, Seminaire "Protection de la vie privée, informatique et progrès de la documentation statistique", Luxembourg, 11-13 décembre 1984, Document No. 7, 16 pp. [ciclostilato].
110.5.5. *Les projets de loi sur la protection des données à caractère personnel en Italie*, in: *Protection de la vie privée, informatique et progrès de la documentation statistique*. "Informations de l'Eurostat" – Numéro spécial, Office des publications officielles des Communautés européennes, Luxembourg 1986, pp. 275-304.
110.6. *Os projetos de lei italianos de proteção dos dados pessoais*, "Revista da Procuradoria-Geral do Estado" (Porto Alegre, RGS), XV, 1985, n. 41, pp. 11-15.

110.7. *Los proyectos de ley italianos sobre la protección de los datos personales*, in: Antonio-Enrique Perez Luño (a cura di), *Problemas actuales de la documentación y de la informática jurídica*, Tecnos, Madrid, 1987, pp. 277-295.
111. *Le tecniche per il controllo della realizzazione dei programmi politici*, "Informatica e diritto", IX, 1983, n. 2, pp. 217-235 (con tre illustrazioni).
111.1. *Le tecniche per il controllo dei programmi politici*, in: *Trasformazione e crisi del Welfare State*. A cura di Ester Fano, Stefano Rodotà e Giacomo Marramao. Prefazione di Alberto Caracciolo, De Donato – Regione Piemonte, Bari, 1983, pp. 319-333.
112. *Il controllo dell'informazione*, "Scienze Digest", 1983, n. 12, pp. 59-60.
113. *La influencia de la informática jurídica sobre la actividad legislativa*, "Documentación administrativa" (Madrid), 1983, n. 199, pp. 107-125.
113.1. *L'influenza dell'informatica giuridica nell'attività legislativa*, in: *L'informatica giuridica e le comunità nazionali e internazionali*. In *Atti del 3° Convegno internazionale organizzato dal Centro elettronico della Corte di cassazione*, Roma 9-14 maggio 1983, Inforav, Roma 1983, vol. 1, Sess. II/7, 28 pp.
114. *Flussi transnazionali dei dati e ritardi nazionali*, "Data Manager", IX, gennaio-febbraio 1984, n. 30-31, p. 20.
115. *Analisi empirica e analisi delle procedure giuridiche*, in: *Società, norme e valori. Studi in onore di Renato Treves*. A cura di Umberto Scarpelli e Vincenzo Tomeo, Giuffrè, Milano, 1984, pp. 357-381.
116. *La magistratura ordinaria e i dati personali in Germania*, "Data Manager", IX, marzo 1984, p. 18.
117. *Prefazione alla seconda edizione*, in: Simon Nora e Alain Minc, *Convivere con il calcolatore*. Seconda edizione, Bompiani, Milano, 1984, pp. I-IV. [Cfr. n. 94.1]
118. *Verso un trasferimento di tecniche dall'impresa all'amministrazione pubblica*, "Data Manager", IX, aprile 1984, p. 20.
119. *Il progetto di legge italiano sulla privacy*, "Data Manager", IX, maggio 1984, p. 16.
120. *Guerra nucleare da equivoco informatico*, "Zerouno", giugno 1984, n. 29, pp. 21-25.
121. *Anche il software è materiale strategico?*, "Data Manager", IX, giugno 1984, n. 35, p. 27.
122. *Un difficile dibattito sui sistemi informativi del personale*, "Data Manager", IX, luglio-agosto 1984, n. 36, p. 26.
123. *L'Europa ha un cuore inquieto ad alta tecnologia*, "Panorama Mese", III, agosto 1984, n. 24, pp. 52-56.
124. *Il flusso transnazionale dei dati personali*, in: *Telematica e diritto. Tesi e proposte per la società dell'informazione: dal diritto d'autore alla deregulation.* A cura di Nino Catania, SEAT, Torino, 1984, pp. 132-136.
125. *Due "case studies" sulla protezione dei dati personali*, in: *L'automazione nell'ufficio*. A cura di Giulio Occhini. *Enciclopedia di direzione e organizzazione aziendale*, sezione IV, volume XXII, Franco Angeli Editore, Milano, 1984, pp. 498-566.
126. *Personal Computer in der juristischen Dokumentation*, in: Hermann Seegers, Fritjof Haft (Hrsg.), *Rechtsinformatik in den achtziger Jahren.* Wissenschaftliches Symposium der IBM Deutschland, Schweitzer Verlag, München 1984, pp. 183-194.

127. *Presentazione*, in: Ermanno Bonazzi – Cesare Triberti, *Guida ai contratti di informatica*. Volume 1: *Compravendita e comodato*, Unicopli, Milano, 1984, pp. 11-19.
128. *In vigore la nuova legge inglese sulla protezione dei dati*, "Data Manager", IX, settembre 1984, n. 37, p. 26.
128.1. *La nueva ley inglesa sobre la privacy*, "La Ley. Revista española de doctrina, jurisprudencia y bibliografía", 1985, n. 3, pp. 1010-1012.
129. *Cinque anni di legge francese sulla privacy*, "Data Manager", IX, ottobre 1984, n. 38, p. 24.
130. *Intanto anche la Gran Bretagna si è data una regola*, "Zerouno", dicembre 1984, n. 35, pp. 120-121.
131. *Le imprese davanti al progetto di legge sulla privacy*, "Data Manager", IX, 1984, n. 39-40, p. 29.
132. *Una legge sul trasferimento elettronico dei fondi?*, "Data Manager", X, 1985, n. 41-42, p. 24.
133. *Verso il censimento permanente*, "Data Manager", X, 1985, n. 43, p. 24.
134. *Riforma costituzionale e libertà informatica*, "Data Manager", X, 1985, n. 44, p. 22.
135. *Una porta con due chiavi per tutelare la privacy*, "Politica ed economia", XVI, 1985, n. 4, pp. 13-15.
136. *Sorgerà una Silicon Valley in Baviera. E nella Valle Padana?*, "Il moderno", I, 1985, n. 1, p. 7.
137. *La legge inglese sulla privacy*, "Data Report", XV, 1985, n. 1, pp. 11-13.
138. *Diritto e informatica*, in: *Tecnologia domani*. A cura di Antonio Ruberti, Laterza – Seat, Roma 1985, pp. 259-294.
139. *[Intervento,]* in: *La giustizia per gli anni '90. La crisi attuale e le riforme possibili*, Gruppo consigliare PCI, Regione Piemonte, Torino, 1985, pp. 61-68.
140. *Il "controllo sul controllo" e le nuove tecnologie*, "Data Manager", X, 1985, n. 45, pp. 5.
141. *Copyright & chips*, "Data Manager", X, 1985, n. 46, p. 9.
142. *Rete nazionale e banche di dati*, "Data Manager", X, 1985, n. 47, p. 25.
143. *Libri sull'informatica giuridica*, "Data Manager", X, 1985, n. 48, p. 31.
144. *Informatica giuridica, informatica giudiziaria*, "Informatica e documentazione", XII, 1985, n. 2, pp. 98-110.
145. *Ricerca e dati personali*, "Data Manager", X, 1985, n. 49-50, p. 35.
146. *L'elaboratore elettronico è nato come modello del cervello umano*, "Il moderno", I, 1985, n. 7, p. 18.
147. *Anche le banche di dati soffrono di amnesie*, "Il moderno", I, 1985, n. 7, pp. 20 sg.
148. *Difesa militare e informatica*, in: *Il potere militare nelle società contemporanee*. A cura di Gianfranco Pasquino e Franco Zannino, Il Mulino, Bologna, 1985, pp. 269-283.
149. *La videobanca in Francia*, "Data Manager", XI, 1986, n. 52-53, p. 35.
150. *Due nuove riviste di informatica giuridica*, "Data Manager", XI, 1986, n. 54, p. 35.
151. *Chi tutela il tedesco federale dai computer polizieschi?*, "Il moderno", II, 1986, n. 11, p. 14.
152. *Tutte le leggi sull'informatica*, "Data Manager", XI, 1986, n. 55, p. 37.
153. *La tutela del software oltr'Alpe*, "Data Manager", XI, 1986, n. 56, p. 41.
154. *Computer crime e assicurazioni*, "Data Manager", XI, 1986, n. 56, pp. 98-101.

[Anticipazione dei paragrafi 4 e 5 del cap. V del *Diritto privato dell'informatica*, cfr. Libri, n. 31].
155. *Informatica e scienze sociali*, "Zerouno", maggio 1986, n. 52, p. 11.
[Risposta alla recensione pubblicata ivi, n. 49, p. 106].
156. *Protezione del software: in Francia è tutelato dal diritto d'autore [intervista]*, "L'elettronica", IX, maggio 1986, n. 31, pp. 7-9.
157. *L'automazione delle biblioteche italiane*, "Data Manager", XI, 1986, n. 57, p. 37.
158. *La memoria e l'inventiva nell'età dei computer*, in: Renato Boeri – Massimo Bonfantini – Mauro Ferraresi (a cura di), *La forma dell'inventiva*, Unicopli, Milano, 1986, pp. 225-228.
159. *Il computer onesto [intervista]*, "Rinascita", XLIII, 1986, n. 24, pp. 18-19.
160. *La legge inglese sulla protezione dei dati*, "Sistemi e automazione", XXXII, luglio 1986, n. 272, pp. 758-767.
161. *I sindacati aprono all'informatica*, "Data Manager", XI, 1986, n. 58, p. 35.
162. *[Riservatezza ed economia privata]*, in: *Privacy, banche dati e sistemi informativi*, Confederazione Nazionale dell'Artigianato, Comitato Regionale dell'Emilia Romagna, Bologna, 1986, pp. 10-15, 26-27.
163. *L'informatica giuridica e l'università*, "Data Manager", XI, settembre 1986, n. 59, p. 41.
164. *Il computer, la scuola e l'umanista*, "Nuova secondaria", IV, 15 ottobre 1986, n. 2, pp. 15-16.
165. *Nuovi reati e vecchie norme: il computer crime oggi*, in: *Il dolo informatico. Come combattere il computer crime*, Atti del convegno, Banca d'America e d'Italia, Milano, 10 giugno 1986, pp. 13-19.
166. *Banche dati: quando i dati varcano le frontiere*, "Notizie Cerved", giugno 1986, n. 20, pp. 38-41.
167. *Un campanello d'allarme: il "Modì elettronico"*, "Data Manager", XI, 1986, n. 60, p. 37.
168. *Una bibliografia sulla protezione del software*, "Data Manager", XI, 1986, n. 61-62, p. 35.
169. *Dal sapere stampato alla videoenciclopedia*, "Media Duemila", IV, 1986, n. 37, pp. 66-71.
170. *Il Servizio Bibliotecario Nazionale*, in: *Per lo sviluppo della cooperazione tra le biblioteche*. Atti del Convegno, 19-20 marzo 1986. A cura di Maria Cecilia Cuturi, ICCU, Roma 1986, pp. 39-43.
171. *E adesso, la videoenciclopedia*, "L'editore", IX, dicembre 1986, n. 11, pp. 66-69.
172. *Due progetti di legge sulla tutela del software*, "Data Manager", XXI, 1987, n. 63, p. 31.
173. *Scuola secondaria e insegnamento dell'informatica*, "Data Manager", XXI, 1987, n. 64-5, p. 33.
174. *Il computer di cristallo. Progetto di legge sulla protezione dei dati personali*, "MicroMega", 1987, n. 1, pp. 159-177.
174.1. *Una legge sulla protezione dei dati personali*, "Il diritto dell'informazione e dell'informatica", III, maggio-agosto 1987, pp. 465-485.
174.2. *Un proyecto de ley sobre la protección de los datos personales en Italia*, in:

Libertad informática y leyes de protección de datos personales, Centro de Estudios Constitucionales, Madrid, 1989, pp. 61-94.

175. *Prospettive teoriche: i sistemi giuridici delle società complesse*, in: William J. Chambliss – Robert B. Seidman, *Introduzione allo studio del diritto*, Loescher, Torino, 1987, pp. 82-96.
176. *La rinuncia alla protezione del software*, "Data Manager", XII, aprile 1987, n. 66, p. 33.
177. *Il disco compatto e la videoenciclopedia*, "Nuova secondaria", 15 maggio 1987, n. 9, p. 70 sg.
178. *Informatica e tecniche legislative: un cerchio che non riesce a chiudersi*, in: *Una politica per la scienza*. Accademia delle Scienze di San Marino. Atti del congresso tenuto a Bologna il 16 gennaio 1987, Pavia, 1987, pp. 23-34.
179. *I rischi economici dell'embargo strategico*, "Data Manager", XII, maggio 1987, n. 67, p. 33.
180. *Il diritto all'informazione*, "Transizione", 1987, n. 8, pp. 37-46.
181. *I dati: beni o servizi*, "Data Manager", XII, giugno 1987, n. 68, p. 17.
182. *Automi non automatici*, "Prometeo", V, giugno 1987, n. 18, pp. 54-65.
183. *I sistemi esperti nei tribunali*, "Data Manager", XII, luglio-agosto 1987, n. 69-70, p. 17.
184. *Queste minacce vengono dall'informatica*, "Il moderno", III, settembre 1987, n. 25, p. 7.
185. *Privacy: un cittadino propone*, "Magazine 4. Bimestrale di tecnologia e cultura informatica", II, settembre-ottobre 1987, n. 4, pp. 22-29.
186. *La centrale bilanci belga su CD-ROM*, "Data Manager", XII, settembre 1987, n. 71, p. 17.
187. *Segreto professionale e furto d'informazioni*, "Data Manager", XII, ottobre 1987, n. 72, p. 17.
188. *L'editoria elettronica*, "Il moderno", III, ottobre 1987, n. 26, p. 3.
189. *Il sistema esperto entra in tribunale*, "Media Duemila", V, ottobre 1987, n. 46, pp. 72-75.
190. *L'editoria elettronica in Europa*, "Data Manager", XII, novembre 1987, n. 73, p. 17.
191. *Il computer e la finanza senza regole*, "Il moderno", III, dicembre 1987, n. 28, p. 3.
192. *Le applicazioni dell'informatica alle scienze sociali*, Relazione al convegno: *Implicazioni e applicazioni dell'informatica*, Istituto svizzero di pedagogia, Lugano-Trevano 1987, pp. 29-37.
193. *L'information retrieval giuridico in Spagna*, "Data Manager", XII, dicembre 1987, n. 74, p. 15.
194. *In biblioteca con il CD-ROM si legge meglio*, "Magazine5", II, novembre-dicembre 1987, n. 5, pp. 30-37.
195. *Gli archivi nell'èra informatica*, "Data Manager", XIII, gennaio-febbraio 1988, n. 75-76, p. 11.
196. *Tribunali, informatica e produttività*, "Data Manager", XIII, marzo 1988, n. 77, p. 13.
197. *Commento al progetto governativo di tutela dei programmi*, "Diritto dell'informazione e dell'informatica", IV, gennaio-aprile 1988, n. 1, pp. 69-79.

198. *Gli strascichi giudiziari del censimento tedesco*, "Data Manager", XIII, aprile 1988, n. 78, p. 17.
199. *L'informatica nell'amministrazione pubblica italiana*, "Data Manager", XIII, maggio 1988, n. 79, p. 15.
200. *La galera per i computer "freaks"?*, "Data Manager", XIII, giugno 1988, n. 80, p. 17.
201. *L'insegnamento del diritto e l'informatica*, "Data Manager", XIII, luglio-agosto 1988, n. 81-82, p. 17.
202. *Il compact disc: di qui all'eternità*, "Data Manager", XIII, settembre 1988, n. 83, p. 23 s.
203. *Il computer nelle scuole brasiliane*, "Data Manager", XIII, settembre 1988, n. 84, p. 17 s.
204. *Duecentomila pagine da leggere vedere ascoltare*, "Il moderno", IV, ottobre 1988, n. 36, p. 48.
205. *I problemi legali dell'editoria su CD-ROM*, in: Marco Gatti – Giulio Occhini – Mario Salvatori (a cura di), *Memorie ottiche per una nuova editoria. Libro bianco su tecnologie, mercato e prospettive di CD-ROM e videodischi in Italia*, Masson, Milano, 1988, pp. 61-67.
205.1. *Problemas legales de las ediciones sobre CD-ROM*, "ICADE. Revista de las facultades de derecho y ciencias económicas y empresariales" (Madrid), 1989, pp. 51-64.
205.2. *Os problemas legais da editoria em CD-ROM*, "Revista Ajuris" (Porto Alegre), vol. L, dicembre 1990, pp. 88-99.
206. *Tesi di laurea e personal computer*, "Data Manager", XIII, ottobre 1988, n. 85, p. 15 s.
207. *Una proposta di legge sulla privacy nella Repubblica di Colombia*, "Informatica e diritto", IV, 1988, n. 3, pp. 117-132.
207.1. *Una propuesta de ley sobre la privacy en la República de Colombia*, in: *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 97-105.
208. *L'"habeas data" nella nuova costituzione brasiliana*, "Data Manager", XIII, novembre 1988, n. 86, p. 17 s.
209. *Dalla razionalità dei sistemi all'irrazionalità dei comportamenti*, in: Enrico M. Forni (a cura di), *Teoria dei sistemi e razionalità sociale*, Cappelli, Bologna, 1986 [ma 1988], pp. 120-141.
210. *Documentarea juridică şi discurile compacte. Realizării italiene*. "Studii şi cercetări juridice" (Bucarest), XXXIII, ottobre-dicembre 1988, n. 4, pp. 371-73.
211. *Le esigenze legislative. Intervento nella tavola rotonda*. in: *Publimatica Novanta. Pubblica amministrazione ed informatica negli anni '90. Soluzioni, prospettive, proposte*. Atti del convegno, Roma 1988, vol. 2, pp. 14-1/14-3.
212. *De la pluma de ganso al rayo láser: tecnologías para los bancos de datos y las editoriales*, "Informática y derecho" (Buenos Aires), 1988, n. 2, pp. 101-151.
213. *La "Gazzetta Ufficiale" on line*, "Data Manager", XIV, gennaio-febbraio 1989, n. 87-88, p. 13 s.
214. *L'integrazione tra banche di dati: pro e contro*, "Data Manager", XIV, marzo

1989, n. 89, p. 15 s.
215. *Privacy, aborto e medici nel vuoto legislativo*, "Data Manager", aprile 1989, n. 90, p. 17 s.
216. *Programas didácticos para el derecho*, in: *Segundo encuentro sobre la informática en las facultades de derecho*, Universidad Pontificia Comillas, Madrid, 1988, pp. 223-30.
217. *Catasto e fisco: il costo della confusione*, "Data Manager", maggio 1989, n. 91, p. 15 s.
218. *L'Italia e la convenzione del Consiglio d'Europa*, "Data Manager", XIV, giugno 1989, n. 92, p. 17 s.
219. *L'Italia e la convenzione sulla privacy*, "Zerouno", giugno 1989, n. 89, pp. 32-35.
220. *Desktop Publishing: stampa l'uomo o il programma?*, "Data Manager", XIV, luglio-agosto 1989, n. 93-94, p. 9 s.
221. *Memorie ottiche e libri impossibili*, "Tempo reale", II, luglio 1989, n. 5, pp. 12-15.
222. *Gli aspetti giuridici negli accordi di cooperazione tra imprese*, in: G.C. Cairnaca – G. Colombo – S. Mariotti – C. Ciborra – G. De Michelis – M.G. Losano, *Tecnologia dell'informazione e accordi tra imprese*, Comunità, Milano, 1989, pp. 321-366.
223. *Una rete per i movimenti alternativi: Greennet*, "Data Manager", XIV, settembre 1989, n. 95, p. 19 s.
224. *Il mestiere del difensore e la tutela della privacy*, "Data Manager", XIV, ottobre 1989, n. 96, p. 19 s.
225. *Il ritmo del tempo*, "Rivista IBM", XXV, 1989, n. 3, pp. 2-6.
226. *I dischetti che parlano*, "Data Manager", XIV, novembre 1989, n. 97, p. 17 s.
227. *Premessa* a: Maria Fernanda Guerrero, *Osservazioni sulla proposta di legge sulla privacy nella Repubblica di Colombia*, "Informatica e diritto", XV, 1989, n. 1, pp. 83 s.
228. *Il virus e la criminalità informatica*, "Data Manager", XIV, dicembre 1989, n. 98, p. 17 s.
229. *Der Austausch personenbezogener Daten zwischen Polizeidienststellen im italienischen Recht*, in: *Sicherheitsstaat und Strafverteidigung, 13. Strafverteidigertag*, Köln 1989, pp. 75-84.
230. *Los orígines del "Data Protection Act" inglesa de 1984*, in: *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 9-60.
231. *Le polizie e il flusso transnazionale dei dati personali nei processi penali*, "Il diritto dell'informazione e dell'informatica", V, settembre-dicembre 1989, n. 3, pp. 841-863.
232. *Frontiere senza controlli o controlli senza frontiere?*, "Micromega", 1990, n. 1, pp. 149-159.
233. *La banca dati della Corte Costituzionale*, "Data Manager", XV, gennaio-febbraio 1990, n. 99-100, p. 19 s.
234. *Il computer dall'Ovest all'Est dopo la rivoluzione del 1989*, "Data Manager", XV, marzo 1990, n. 101, p. 17 s.
235. *Il sistema "Jusvideo": la giurisprudenza italiana su disco compatto*, in: Mario G. Losano – Lothar Philipps, *Diritto e CD-ROM. Esperienze italiane e tedesche a confronto*, Giuffrè, Milano, 1990, pp. 19-34.
236. *Leggi sulla privacy e unione valutaria tedesca*, "Data Manager", XV, aprile 1990, n. 102, p. 21 s.
237. *Gli ultimi sviluppi delle reti neuronali*, "Data Manager", XV, maggio 1990, n.

103, p. 19 s.
238. *Cadono in Francia i decreti sulla trasparenza della polizia*, "Data Manager", XV, giugno 1990, n. 104, p. 21 s.
239. *Nuovi CD-ROM giuridici in Germania*, "Data Manager", XV, luglio-agosto 1990, n. 105-6, p. 15 s.
240. *Un progetto di legge paulista sull'"Habeas Data"*, "Data Manager", XV, settembre 1990, n. 107, p. 27 s.
241. *Il sapere raddoppiato e le biblioteche dimezzate*, "Data Manager", XV, ottobre 1990, n. 108, p. 25 s.
242. *El aula de informática en la facultad de derecho*, in: Miguel Angel Davara (ed.), *III encuentro sobre la informática en las facultades de derecho (mayo 1989)*, Universidad Pontificia Comillas, Madrid, 1990, pp. 11-20.
243. *La presenza dei costruttori giapponesi in Europa*, "Data Manager", XV, novembre 1990, n. 109, p. 23 s.
244. *Predgovor hrvatskom izdanju* [prefazione all'edizione croata], in: *Pravna kibernetica. Kibernetički strojevi i modeli u pravu*. Prijevod Živko Anzulović, Književni krug, Split 1990, 120 pp.
245. *Le norme sulla privacy in Giappone*, "Data Manager", XV, dicembre 1990, n. 110, p. 29 s.
246. *Videoterminali, giornalismo e diritto al lavoro*, "Data Manager", XVI, gennaio-febbraio 1991, n. 111-112, p. 23 s.
247. *La privacy del paziente e la contabilità delle mutue*, "Data Manager", XVI, marzo 1991, n. 113, p. 31 s.
248. *Il trattato di Schengen e le frontiere europee*, "Data Manager", XVI, aprile 1991, n. 114, p. 27 s.
249. *Piccole biblioteche e grandi reti: un esempio romano*, "Data Manager", XVI, maggio 1991, n. 115, p. 23 s.
250. *Censimento e "autotutela della riservatezza" in Spagna*, "Data Manager", XVI, giugno 1991, n. 116, p. 27 s.
251. *Alle origini del computer: il bicentenario di Charles Babbage*, "Data Manager", XVI, luglio-agosto 1991, n. 117-118, p.23 s.
252. *L'integrazione delle banche di dati legislativi delle regioni*, "Data Manager", XVI, settembre 1991, n. 119, p. 30 s.
253. *La politica dell'informatica in Brasile*, "Data Manager", XVI, ottobre 1991, n. 120, p. 24 s.
254. *Gli ostacoli legislativi all'uso economico degli archivi pubblici*, "Impresa e Stato", settembre 1991, n. 15, pp. 48-50.
255. *L'informatica nella ricerca giuridica*, "Rivista IBM", XXVIII, 1992, n. 1, pp. 42-48.
256. *Prospettive dell'informatica nella ricerca e nell'insegnamento del diritto*, in: Fondazione IBM Italia (a cura di), *Calcolatori e scienze umane. Archeologia e arte, storia e scienze giuridiche e sociali, linguistica, letteratura*, Etaslibri, Milano, 1992, pp. 121-156.
257. *Para una teoría general de las leyes sobre la protección de los datos personales*, in: *Implicaciones socio-jurídicas de la tecnología de la información*. IX Encuentro, Citema, Madrid, 1991, pp. 47-60.

258. *I primi anni dell'informatica giuridica in Italia*, in: Fondazione Adriano Olivetti (a cura di), *La cultura informatica in Italia. Riflessioni e testimonianze sulle origini, 1950-1970*, Bollati Boringhieri, Torino, 1993, pp. 191-236.
259. *A tutela del privato*, "ZeroUno", giugno 1993, n. 137, pp. 56-57.
260. *Datenbanken, Datenschutz und der Kampf gegen das organisierte Verbrechen*, in: Maria-Theres Tinnefels – Lothar Philipps – Kurt Weis (a cura di), *Die dunkle Seite des Chips. Herrschaft und Beherrschbarkeit neuer Technologien*, Oldenbourg, München-Wien 1993, pp. 117-135.
260.1. *Bases de dates, vida privada i lluita contra la delincüència organitzada*,
in: Angel San Martín (a cura di), *Fin de segle. Incerteses davant un nou mil-leni*, Universitat de València, Ajuntament de Gandia, Valencia 1994, pp. 287-300.
261. *Privacy: a quando una legge italiana?* [Sulla legge spagnola sulla privacy],
"ZeroUno", settembre 1993, n. 140, pp. 78-79.
262. *Una legge? No, due.* [Il testo della nuova legge sul software non è uguale a quello approvato], "ZeroUno", ottobre 1993, n. 141, pp. 81-83.
263. *Direito, Democracia, Tecnocracia. As raízes históricas do hodierno renascimento da tecnocracia*, "Revista Brasileira de Filosofia", XLI, Janeiro-Março 1993, pp. 3-17.
264. *L'ultimo progetto italiano di legge sulla privacy*,
"Informatica e documentazione", 1993, n. 1-2, pp. 95-101.
264.1. *El proyecto de ley sobre la tutela de la persona respecto a la elaboración informática de los datos personales*, in: Miguel Angel Davara (a cura di), *Encuentros sobre informática y derecho*, Aranzadi, Pamplona 1993, pp. 11-16.
265. *Der neueste Entwurf für ein italienisches Datenschutzgesetz*, "Datenschutz und Datensicherung", 1993, n. 11, pp. 634-635.
266. *Prefazione*, in: Carlo Biagioli *et al.*, *Elementi di legimatica*, Cedam, Padova, 1993, pp. IX s.
267. *La nuova legge spagnola sulla protezione dei dati personali*, "Diritto dell'informazione e dell'informatica", IX, 1993, n. 4-5, pp. 867-894 [cfr. nn. 327, 332].
268. *Informatica giuridica*, in: *Digesto*, IV edizione, vol. IX (Discipline privatistiche), Utet, Torino, 1994, pp. 416-420.
268.1. *Informatika juridike (I)*, in: Mario G. Losano, *Informatika juridike*. Përkthimi dhe parathënia nga Gjergj Sinani, Istituto per la Documentazione Giuridica, Firenze, 1994, pp. 88-100.
270. *Das Italienische Gesetz über Computerprogramme*, "Datenschutz und Datenverarbeitung", Januar 1994, n. 1, pp. 16-19.
271. *Tecniche legislative, informatica e buon governo*, in Mario G. Losano (a cura di), *Tavola rotonda: L'informatica giuridica al servizio del legislatore*, in Giovanna Visintini (a cura di), *Il diritto dei nuovi mondi*. Atti del Convegno, Genova 5-7 novembre 1992, Cedam, Padova, 1994, pp. 523-528.
272. *Information Technology, the Law and Fuzzy Logic*, in: Losano, Mario G. (a cura di), *The Computer and Vagueness: Fuzzy Logic and Neural Nets (Munich, 20th November 1992)*, "Informatica e diritto", 1993, n. 2, (pp. 7-120), pp. 7-12.
273. *Legge organica 5/1992 del 29 ottobre, regolante il trattamento automatizzato dei dati personali*, "Diritto dell'informazione e dell'informatica", X, 1994, n. 1, pp. 119-138 [cfr. nn. 320, 332].

274. *Databases, Privacy and Organized Crime*, in: Hans-Werner Meuer (Hrsg.), *Facing the New World of Information Technology*, Saur, München-London-New Providence-Paris, 1994, pp. 13-29.
274.1. *La democracia, el crimen organizado y las leyes sobre la privacy*, "Doxa. Cuadernos de filosofía y derecho" (Alicante), 1994, n. 15-16, vol. I, pp. 447-466.
275. *Informatica e riforma della pubblica amministrazione. Per una "moderna analisi strutturata" della legislazione*, in: *L'unità del diritto. Massimo Severo Giannini e la teoria giuridica*. A cura di Sabino Cassese e altri, Il Mulino, Bologna, 1994, pp. 353-367.
276. *Prefazione – Prefácio*, In: Marcela Varejão, *Un thesaurus italo-portoghese su diritto e informatica. Testo bilingue*, Istituto per la Documentazione Giuridica, Firenze, 1994, pp. 5-15.
277. *Spagna: Statuto dell'Agenzia per la Protezione dei Dati*, "Diritto dell'informazione e dell'informatica", X,1994, n. 3, pp. 627-637 [cfr. nn. 320, 327].
278. *La nuova legge spagnola sulla protezione della privacy*, "Impresa & Stato", giugno 1994, n. 26, pp. 101-103. *Vedi anche*: 333.1. ttp://impresa.stato.mi.camcom.it.
279. *Storia delle macchine da calcolo e storia sociale*, in: *Conoscenze scientifiche e trasferimento tecnologico*, *Storia delle Scienze*, vol. 5, Giulio Einaudi Editore, Torino, 1995, pp. 294-331.
280. *Informatica giuridica*, in: *Enciclopedia delle Scienze Sociali*, Istituto dell'Enciclopedia Italiana, Roma 1994, pp. 711-719. http://www.treccani.it/enciclopedia/informatica-giuridica_(Enciclopedia-delle-scienze-sociali)/.
281. *The Schengen Treaty and Italy – Some Problems in Transnational Data Flow*, in: *Current Research Information Systems in Europe: A Step Further*, Conference Proceedings (Milan, May 11-13, 1995), Consiglio Nazionale delle Ricerche, Milano, 1995, pp. 53-56.
281.1. *El Tratado de Schengen e Italia: Problemas del flujo transnacional de datos*, "Informática y derecho" (Mérida), [1996], n. 12-15, II Congreso Internacional de informática y derecho, *Actas*, vol. II, pp. 1353-1357.
282. *L'applicazione delle leggi sulla privacy alle carte di credito*, in: Donato A. Limone (a cura di), *Dalla giuritecnica all'informatica giuridica. Studi dedicati a Vittorio Frosini*, Giuffrè, Milano, 1995, pp. 201-216.
283. *A informática jurídica vinte anos depois*, "Revista dos Tribunais", LXXXIV, maio de 1995, vol. 715, pp. 350-367.
284. *Informatica e riforma della pubblica amministrazione. Per una "Moderna analisi strutturata" della legislazione*, in: Javier Echeverría – Javier de Lorenzo – Lorenzo Peña (a cura di), *Calculemos … Matemáticas y libertad*. Homenaje al Profesor Miguel Sánchez-Mazas, Trotta, Madrid, 1996, pp. 263-271.
285. *Le norme sulla violazione della riservatezza nel nuovo codice penale spagnolo*, in: *Le norme spagnole sulla protezione dei dati personali*. "Quaderni della Sezione di teoria generale e informatica del diritto", Dipartimento Giuridico-Politico, n. 4, Cuesp, Milano, 1996, pp. 1-14.
285.1. *Le norme sulla violazione della riservatezza nel nuovo codice penale spagnolo*, "Diritto dell'informazione e dell'informatica", 1996, n. 4-5, pp. 535-550.
286. *Automi e calcolo meccanico: macchine futili e macchine utili*, "Cultura e scuola",

1996, n. 137, pp. 303-310.

287. *Das italienische Datenschutzgesetz*, "Computer und Recht", XIII, 1997, n. 5, pp. 308-312.

288. *Das italienische Datenschutzgesetz*, in: Wolfgang Kilian (Hrsg.), *EC Data Protection Directive. Interpretation – Application – Transposition. Working Conference*, Toeche-Mittler, Darmstadt 1997, pp. 145-146.

289. *Das italienische Datenschutzgesetz – schon geändert*, "Computer und Recht", XIII, 1997, n. 9, pp. 578-579.

290. *Introduzione*, pp. XI-XIV; *Commentario all'art. 9*, pp. 81-88; *Bibliografia straniera*, pp. 541-551, in: Ettore Giannantonio – Mario G. Losano – Vincenzo Zeno-Zencovich, L*a tutela dei dati personali. Commentario alla L. 675/1996*, Cedam, Padova, 1997, 569 pp.

291. *La Ley italiana sobre Protección de Datos Personales*, "Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol" (Valencia), 1997, n. 17, pp. 147-160.

291.1. *A lei italiana sobre a proteção dos dados pessoais*, http://www.teiajuridica.com/leiproda.html.

291.2. *A lei italiana sobre a proteção dos dados pessoais*, "O Direito" (Lisboa), Janeiro-Junho 1997, pp. 7-27.

292. *La bibliografia di Norberto Bobbio su Internet*, "Sociologia del diritto", XXVI, 1999, n. 2, pp. 157-167.

293. *Informatica e tecniche legislative*, in: *Tecniche di redazione degli atti normativi e amministrativi comunali e provinciali*, Giuffrè, Milano, 2000, pp. 15-34.

294. *Gli automi e la danza, ovvero degli imperfetti movimenti delle sculture*, in: *Automi, marionette e ballerine nel teatro d'avanguardia*. Catalogo della mostra del Museo di Arte Moderna e Contemporanea di Trento e Rovereto, 1° dicembre 2000-18 marzo 2001, Skira, Genéve-Milano, 2000, pp. 31-41.

294.1. *Gli automi e la danza, ovvero degli imperfetti movimenti delle sculture*, in: Mario G. Losano, *Automi d'Oriente. "Ingegnosi meccanismi" arabi del XIII secolo*, Medusa, Milano, 2003, pp. 109-126.

295. *Introduzione,* ovvero *Dei diritti e dei doveri: anche nella tutela della privacy*, in: Mario G. Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Laterza, Roma-Bari, 2001, pp. V-XX.

295.1. Legea italiană cu privire la protecţia vieţii private. Drepturi şi îndatoriri în respectarea dreptului la viaţa privată, "Analele Universităţii din Bucureşti – Drept", 2002, n. 2, pp. 70-87 [in romeno e italiano].

295.2. *Dos direitos e dos deveres: também no direito à privacidade*, "Verba Juris. Anuário da Pós-Graduação em Direito" (João Pessoa, Brasil), II, 2003, n. 2, pp. 8-28.

295.3. *Despre drepturi şi despre îndatoriri: încă despre tutela vieţii private*, in: *Legea italiană în privinţa protecţiei vieţii private. Un bilanţ al primilor cinci ani*. Traducere: Alina Lazăr; Coordonator traducere şi îngrijirea ediţiei: Mihail-Constantin Eremia, All Beck, Bucureşti 2004, pp. 1-17.

296. *La informática jurídica hacia el tercer milenio*, in: Instituto de Derecho Informático de la Universidad de la República, *Derecho informático. Tomo I. Correspondiente al año 2000*, Fundación de Cultura Universitaria, Montevideo 2001, pp. 81-101.

297. *Automi e burattini in Oriente*, in: Mario G. Losano, *Automi d'Oriente. "Ingegnosi meccanismi" arabi del XIII secolo*, Medusa, Milano, 2003, pp. 5-17.
298. *E-government: la experiencia italiana*, in: Universidad de los Andes, *Derecho de Internet y Telecomunicaciones*, Legis, Bogotá et al. 2003, pp. 3-22.
299. *Un corso universitario triennale di informatica giuridica*, "Il diritto dell'informazione e dell'informatica", 2003, n. 6, pp. 1047-1061.
299.1. *Il corso triennale di informatica giuridica*, "Revista da Escola Superior da Magistratura de Sergipe – ESMESE" (Aracaju), n. 5, 2003, pp. 15-30, ISSN 1679-785X ou 1679-7857.
299.1.1. *Il corso triennale di informatica giuridica*, http://www.esmese.com.br/documentos/divulgacao/revistas/revista_05.pdf.
299.2. Der Studiengang über Rechtsinformatik an der Università del Piemonte Orientale (Universität Ost-Piemont, Alessandria)*, in Jürgen Taeger – Andreas Wiebe (Hrsg.)*, Informatik – Wirtschaft – Recht. Regulierung der Gesellschaft. Festschrift für Wolfgang Kilian zum 65. Geburtstag, Nomos, Baden-Baden 2004, pp. 117-133.
299.3. *O curso trienal de informática jurídica na Universidade do Piemonte Oriental*, *"Prim@ facie. Revista da pós-gradução em ciências jurídicas da UFPB" [Universidade Federal da Paraíba, João Pessoa], III, 2004, n. 4, pp. 5-19.* http://www.ccj.ufpr.br/primafacie, periodicos.ufpb.br/ojs/index.php/…/3358.
299.4. *O curso trienal de informática jurídica na Universidade do Piemonte Oriental*, "Verba Juris. Anuário da Pós-Graduação em Direito" (João Pessoa, Brasil), III, 2004, n. 3, pp. 8-35.
300. *Las técnicas legislativas, de la "prudentia legislatoria" a la informática*, in: Aurelio Menéndez Menéndez – Antonio Pau Pedrón (org.), *La proliferación legislativa: un desafío para el estado de derecho*, Thompson – Civitas, Madrid, 2004, pp. 163-198 (Seminario organizado por el Colegio Libre de Eméritos en la Real Academia de Ciencias Morales y Políticas, Madrid, 11-12 de noviembre de 2003).
300.1. *Le tecniche legislative dalla "prudentia legislatoria" all'informatica,* "Il diritto dell'informazione e dell'informatica", 2004, n. 3, pp. 383-400.
301. *Privacidad y seguridad en la era del terrorismo: el deber del jurista informático,* in: Instituto de Derecho Informático de la Universidad de la República*, Derecho informático*. Tomo I. Correspondiente al año 2004, Fundación de Cultura Universitaria, Montevideo 2005, pp. 121-132.
302. *La "giuscibernetica" dopo quattro decenni.* "Diritto dell'informazione e dell'informatica", 2005, n. 4-5, pp. 727-751.
302.1. *La "iuscibernética" tras cuatro décadas*, Javier Plaza Penadés (Coord.), *Cuestiones actuales de derecho y tecnología de la información y la comunicación (TICS)*, Thomson – Aranzadi, Cizur Menor (Navarra) 2006, pp. 15-41 (Monografía Asociada a "Revista Aranzadi de Derecho y Nuevas Tecnologías", número 4).
303. *Simon Nora, un architetto della politica francese dell'informatica*, "Il diritto dell'informazione e dell'informatica", LV, 2006, n. 2, pp. 85-92.
304. *I sistemi cibernetici nel diritto: i modelli cibernetico-sociali e modelli giuridici nella società odierna*, "Analele universităţii din Bucureşti – Drept", 2007, n. 2, pp. 20-65 [in italiano, con riassunti in francese, inglese e romeno].
305. *Trasparenza o privacy? Due recenti polemiche italiane*, "Il diritto dell'informa-

zione e dell'informatica", 2008, n. 4-5, pp. 471-493.

305.1. *El conflicto entre la transparencia y la privacy en dos recientes polémicas italianas*, in: Javier Boix Reig – Ángeles Jareño Leal, *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, pp. 557-582.

306. *Come proteggere i prototipi letterari prodotti in serie?*, "Il Verri", ottobre 2008, n. 38, pp. 114-126 (Numero speciale: *Attività combinatorie. A partire dal* Tristano *di Nanni Balestrini*).

307. *Le alterne vicende delle macchine calcolanti e semoventi*, in *Corpo automi robot. Tra arte, scienza e tecnologia*, Mazzotta, Milano, 2009, pp. 51-59.

307.1. *The Ups and Downs of Calculating and Self-operating Machines*, in *Corpo automi robot. Tra arte, scienza e tecnologia*, Mazzotta, Milano, 2009, pp. 368-373.

307.2. *Postfazione. Le alterne vicende delle macchine calcolanti e semoventi*, Roberto Peverelli (ed.), *Gli automi sono fra noi*, Medusa, Milano, 2011, pp. 187-213.

308. *La* computer forensics *e l'insegnamento dell'informatica giuridica*, in Patrick Nerhot, *L'identità plurale della filosofia del diritto*, Atti del XXVI Congresso della Società Italiana di Filosofia del Diritto (Torino, 16-18 settembre 2008), Edizioni Scientifiche Italiane, Napoli, 2009, pp. 115-123.

309. *Ancora sul corso universitario triennale di informatica giuridica*, "Il diritto dell'informazione e dell'informatica", XXVI, gennaio-febbraio 2010, pp. 81-90.

310. *Il centenario di Konrad Zuse (1910-1995): il computer nasce in Europa*, "Il diritto dell'informazione e dell'informatica", XXVIII, 2012, n. 1, pp. 1-16.

311. *Il centenario di Konrad Zuse (1910-1995): il computer nasce in Europa*, "Atti della Accademia delle Scienze di Torino", Classe di Scienze Morali, Storiche e Filologiche", vol. 145 (2011), Torino, 2012, pp. 61-82.

312. *1840: Babbage*, "Turin. Storia e storie della città", aprile 2013, n. 4, pp. 18-23.

313. *Il corso triennale di informatica giuridica dell'Università del Piemonte Orientale*, in Ginevra Peruginelli – Mario Ragona (ed.), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, ESI, Napoli, 2014, pp. 119-148.

313.1. *Il corso triennale di informatica giuridica dell'Università del Piemonte Orientale*, in Ginevra Peruginelli – Mario Ragona (ed.), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, ESI, Napoli, 2014, pp. 119-148. http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/CollanaSeD/sed-12/01_05_LosanoPreview.pdf.

314. *La macchina analitica di Babbage: un fossile che viene dal futuro*, in Mario G. Losano, *La macchina analitica di Babbage*, Olschki, Firenze, 2014, V-XLVIII pp.

314.1. *La macchina analitica di Babbage: un fossile che viene dal futuro*, "Diritto dell'informazione e dell'informatica", 2015, n.1, pp. 1-42.

315. *Bibliografia degli scritti su Charles Babbage dal XX secolo in poi*, in Mario G. Losano, *La macchina analitica di Babbage*, Olschki, Firenze, 2014, XLIX-LXVI pp.

316. *New Technologies, Fight against Terrorism and Fundamental Rights: Internet and Freedom*, in Luis Tomé (ed.), *"Islamic State". The New Global Jihadist Phenomenon*, Media XXI, Porto 2015, pp. 125-163.

317. *Il progetto di legge tedesco sull'auto a guida automatizzata.* Appendice: *Il progetto di legge e le relazioni illustrative*, "Diritto dell'informazione e dell'informatica", XXXIII, 2017, pp. 1-25.

318. *Trasparenza e segreto: una convivenza difficile nello Stato democratico*, "Diritto pubblico", settembre-dicembre 2017, n. 3, pp. 658-682.
318.1. *Die Transparenz im öffentlichen Recht – Drei Beispiele eines schwer erreichbaren Ziels*, in Diana-Urania Galetta – Jacques Ziller (eds), *Das öffentliche Recht vor den Herausforderungen der Informations– und Kommunikationstechnologien jenseits des Datenschutzes – Information and Communication Technologies Challenging Public Law, Beyond Data Protection – Le droit public au défi des technologies de l'information et de la communication, au-delà de la protection des données*, Nomos Stämpfli Verlag, Baden-Baden 2018, pp. 15-34.
319. *Germania, agosto 2018: manifestazioni neonaziste, privacy e libertà d'informazione*, "Diritto dell'informazione e dell'informatica", 2018, pp. 673-688.
320. *De Kelsen a la informática jurídica: una entrevista con Mario G. Losano – From Kelsen to Legal Informatics: An Interview with Mario G. Losano* – Jose Antonio García Sáez, "Isonomía", Núm. 49, 2019, pp. 187-219. http://newisonomia.itam.mx/index.php/revista-cientifica/article/view/22.
321. *Verso l'auto a guida autonoma in Italia*, "Diritto dell'informazione e dell'informatica", 2019, pp. 423-441.
322. *Prefacio: El derecho frente a la sociedad informatizada*, in Marcelo Bauzá Reilly (ed.), *El derecho de las TIC en Iberoamérica*, La Ley Uruguay, Montevideo 2019, pp. 1-10.
323. *Scripta volant: la volatilizzazione dei documenti nell'era digitale*, "Il diritto dell'informazione e dell'informatica", XXV, 2020, n. 1, pp. 17-42.
323.1. *Scripta volant: la volatilizzazione dei documenti nell'era digitale*, "Prim@Facie" (João Pessoa), XIX, 2020, n. 40, pp. 1-34. (https://periodicos.ufpb.br/ojs2/index.php/primafacie/issue/view/2437).

I.

AMMINISTRAZIONE DIGITALE *ALGORITMICA*. IL QUADRO COSTITUZIONALE

Andrea Simoncini

SOMMARIO: 1. Premessa. Le libertà costituzionali nel XXI secolo: il potere tecnico e la trasformazione digitale. – 2. Amministrazione digitale e amministrazione *algoritmica*: la nuova frontiera del potere tecnologico. – 3. La creatività nel formante giurisprudenziale, dalla *rule of law* alla *rule of technology*: alcuni casi. – 3.1. L'esclusione automatica da gare o concorsi. – 3.2. Le decisioni algoritmiche riguardanti il personale della scuola. – 3.3. Dalla *rule of law* alla *rule of technology*. – 4. Principi costituzionali e decisioni algoritmiche: verso una "*constitutional*" rule of technology. – 4.1. Premessa: gli atti di amministrazione digitale *algoritmica*, sono (davvero) atti giuridici? – 4.2. Il divieto di atti di amministrazione digitale "esclusivamente" algoritmica. – 4.3. L'obbligo di motivazione nella amministrazione digitale "algoritmica". – 4.4. Il principio di "non discriminazione" nella amministrazione digitale "algoritmica". – 5. Spunti conclusivi. La dialettica "servo-padrone" nell'uso degli algoritmi. – Bibliografia.

1. Premessa. Le libertà costituzionali XXI secolo: il potere tecnico e la trasformazione digitale

La natura del diritto costituzionale in senso moderno (B. CONSTANT, 1819) consiste nel – quantomeno, cercare di – limitare l'uso del potere, sia esso pubblico o privato, quando questo incide sulle libertà individuali e collettive. La sua peculiarità, rispetto a molte altre aree del pensiero pratico che studiano lo stesso problema (la filosofia politica, la morale, l'etica, la sociologia, la politologia, ecc.), è che esso persegue questo scopo attraverso il diritto.

Il fine delle costituzioni è sempre stato – tra gli altri – quello di porre un fondamento giuridico e, dunque un limite giustiziabile, all'esercizio dei poteri ed in particolare dei poteri *sovrani*, ovverosia, di quei poteri capaci di conformare e restringere più o meno unilateralmente la sfera di libertà delle persone. Se ammettiamo questa definizione, per quanto sommaria, ne consegue che il

diritto costituzionale ha sempre *seguito* l'evoluzione del *tipo* di potere sovrano esistente, adeguando e adattando il suo intervento alla fisionomia che esso ha assunto nel tempo (A. SIMONCINI, 2017). La "tecnica" del potere non è mai stata neutra o indifferente, ma anzi il sistema costituzionale si è sempre "modellato" sulle sue forme concrete.

In prospettiva storica, dopo l'epoca medievale – epoca in cui l'idea stessa di un potere/sovrano *assoluto* non esiste (P. GROSSI, 1997) – due sono le stagioni fondamentali del costituzionalismo moderno.

Una prima, dalla fine del XVIII agli inizi del XX secolo, in cui il potere emergente da limitare era essenzialmente il potere militare personale e privato del sovrano; lo strumento attraverso cui ciò è avvenuto è stata l'"invenzione" della legge parlamentare (generale ed astratta) e la sua istituzione espressiva: lo Stato. Il risultato di questa grande prima rivoluzione costituzionale – quantomeno nell'Europa continentale – è stato il trasferimento del potere giuridico originario dal Sovrano allo Stato e al suo diritto legislativo (M. FIORAVANTI, 2019).

Nella seconda stagione, il trauma della degenerazione totalitaria del primo Novecento sul continente europeo, ha mostrato che il nuovo potere sovrano da delimitare era proprio quello dello Stato e, conseguentemente, il suo strumento "chiave": la legge. Nascono così, da un lato, le costituzioni "rigide" del secondo dopoguerra e, dall'altro, gli strumenti internazionali per la difesa dei diritti fondamentali. In questa seconda stagione, il principio di legalità (la cosiddetta *rule of law*) classico del primo costituzionalismo, diviene principio di "costituzionalità", principio in grado di vincolare la stessa legge. Nascono così gli ordinamenti costituzionali che oggi conosciamo: da un lato, con la loro strutturazione multilivello (P. BILANCIA, F.G. PIZZETTI, 2014), dall'altro, caratterizzati dalla forza espansiva del diritto giurisprudenziale delle corti, sia nazionali che inter- o sovra-nazionali. Una stagione in cui la stessa idea di "sovranità" nata con gli Stati nazionali e trasformata dalle costituzioni post-belliche, sembra oggi al tramonto o, quantomeno, in transizione (A. MORRONE, 2017).

Questa stagione – e veniamo così al tema che intendiamo affrontare – sebbene ancora dómini l'immaginario concettuale giuridico-politico, in realtà si è chiusa con la fine del secolo XX.

L'avvento del XXI secolo e della cosiddetta "era digitale" aprono una nuova fase per il costituzionalismo, perché esso si trova dinanzi ad un "nuovo" potere sovrano. La fenomenologia odierna della sovranità non ha più caratteri necessariamente privati o pubblici, personali o collettivi, ma essenzialmente *tecnici*. La forza da delimitare e "giustificare" non è più quella privata del re o quella pubblica dello Stato, ma un nuovo tipo di potere (*rectius*, di potenza)

che oggi può presentarsi sia sotto forma privata che pubblica. È il *paradigma tecnologico,* sempre più emergente, inteso come fattore di liberazione della persona e di innovazione sociale e, dunque, come bene irrinunciabile.

Il sovrano del XXI secolo – *superiorem non recognoscens* – assume le vesti delle tecnologie emergenti ed in particolare dei mezzi tecnici dell'informazione e della comunicazione.

La tecnica *dell'informazione*, infatti, rappresenta un settore affatto particolare della dimensione tecnologica generalmente intesa; essa infatti riguarda le modalità attraverso le quali gli esseri umani rappresentano e comunicano i dati riguardanti la realtà.

Sono dunque gli strumenti che normalmente utilizziamo per acquisire, conservare, modificare, comunicare la nostra rappresentazione del mondo; quella che con acronimo contemporaneo definiamo ICT (*Information and Communication Technology*).

È evidente che rispetto al progresso tecnologico in generale, l'evoluzione di questi particolari mezzi tecnici ha svolto un ruolo decisivo nella storia della civiltà umana.

Il passaggio dal linguaggio alla scrittura (circa 3500 a.C.), ovvero dalla scrittura alla stampa a caratteri mobili (1500 d.C.), dalla stampa alla trasmissione dei segnali elettrici e poi elettromagnetici (1800), infine dal segnale analogico a quello digitale (1950), sono tutti *turning points* decisivi che hanno segnato altrettante svolte nella stessa evoluzione della cultura e delle società umane, coinvolgendo inevitabilmente quel fenomeno sociale e culturale che è il diritto.

Queste nuove tecnologie, in realtà, "danno la misura" della capacità relazionale dell'essere umano, consentendo, facilitando ovvero restringendo e, comunque, influenzando la comunicazione.

Secondo la notissima espressione di Marshall MacLuhan, «il *medium* è il messaggio» (1964): il mezzo, di fatto, determina il contenuto del messaggio che trasmette.

È questa la ragione per cui alcune capacità tecniche sono divenute il contenuto di diritti fondamentali. Si pensi al diritto all'istruzione e all'educazione: imparare a *leggere* e *scrivere* è stato – ed è tuttora – il contenuto minimo di uno dei livelli essenziali del diritto e dell'obbligo costituzionale all'istruzione. D'altronde, l'invenzione tecnica della *scrittura* e conseguentemente della *lettura*, hanno finito per "conformare" e strutturare la grammatica stessa del nostro pensiero, consentendo un "salto evolutivo" senza paragoni alla specie *homo sapiens*.

Occorre, perciò, essere consapevoli che quella che chiamiamo "rivoluzione" o "trasformazione" digitale è, in primo luogo, una mutazione cognitiva e antropologica ed in questo essa genera una nuova forma di "potere". Non si

tratta soltanto di una nuova abilità tecnica in grado di facilitare lo svolgimento di compiti già conosciuti, ma si tratta di una serie di strumenti tecnici in grado di produrre abilità che attualmente non conosciamo.

È di questo *nuovo potere* che il diritto costituzionale oggi deve ricercare il limite ed il fondamento, se non vuol venire meno alla sua finalità originaria.

2. Amministrazione digitale e amministrazione *algoritmica*: la nuova frontiera del potere tecnologico

L'impatto della tecnologia digitale sui poteri pubblici ed in particolare sull'amministrazione è analizzato nel dettaglio in vari altri contributi di questo volume.

In questo capitolo intendiamo soffermarci su di un aspetto particolare di questa trasformazione; un aspetto caratterizzato da una forte rilevanza costituzionale e che, per questo, andrà chiarito nella sua specificità.

Ci riferiamo a quella che definiremo la dimensione *algoritmica* della più generale *amministrazione digitale*.

Il fenomeno più problematico dal punto di vista costituzionale, infatti, non è soltanto quello generale della "digitalizzazione" della Pubblica Amministrazione (sul quale si soffermano in particolare i capitoli III, IV e V del presente volume), bensì quello della amministrazione digitale *algoritmica*, come meglio preciseremo nel séguito (profilo sul quale si sofferma nel dettaglio il capitolo IV, R. CAVALLO PERIN e I. ALBERTI).

La digitalizzazione della amministrazione pubblica muove i primi passi già dagli anni '70 – a partire dagli studi di Predieri (1971) e dal noto *Rapporto Giannini* del 1979 – in cui già si auspicava l'utilizzo degli "elaboratori elettronici" nel riordino della Amministrazione dello Stato (I. MACRÌ, U. MACRÌ, G. PONTEVOLPE, 2011).

Come sappiamo, in questa materia è intervenuto, tra i primi in Europa, il D.Lgs. 7 marzo 2005, n. 82, intitolato «*Codice della Amministrazione Digitale*». Il codice seguiva la Comunicazione del 26 settembre 2003 della Commissione Europea su «Il ruolo dell'e-governement per il futuro dell'Europa», in cui veniva auspicato «l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche organizzative ed all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici ed i processi democratici e di rafforzare il sostegno alle politiche pubbliche».

Questo rilevante testo legislativo ha disciplinato l'impiego della tecnologia informatica come *modalità di documentazione, conservazione e comunicazione dell'atto amministrativo*, garantendo al documento informatico (artt. 20 e ss.)

la soddisfazione del requisito della forma scritta e l'efficacia prevista dall'art. 2702 del codice civile.

Lo scopo fondamentale era dare un quadro normativo unitario a quella che viene definita unitariamente "*amministrazione digitale*" (F. MARTINES, 2018) al fine, da un lato, di semplificare i rapporti tra cittadino e PA e, dall'altro, di rendere più efficace e ed efficiente l'azione dell'Amministrazione stessa, utilizzando gli strumenti della ICT e giungendo a sancire un vero e proprio nuovo "diritto": il diritto all'uso delle tecnologie (art. 3), fondamento della "cittadinanza digitale" (artt. 3 e ss.).

L'oggetto che prenderemo in esame in queste riflessioni, sebbene si inserisca all'interno del *genus* "amministrazione digitale", ne rappresenta una *species* particolare; quella che possiamo definire "amministrazione *algoritmica*".

Per comprendere in cosa consista la specificità di questo ambito, occorrerà prendere le mosse dalla evoluzione più recente della tecnologia digitale, dovuta all'avvento di quello che è stato chiamato *Internet of Things*, ma che rapidamente sta trasformandosi in *Internet of Everything* (A. SANTOSUOSSO, B. Di MARTINO, K. LI, L.T. YANG, A. ESPOSITO, 2017), e cioè la produzione massiva di vastissime quantità di dati (i cosiddetti "*big data*", v. capitolo VI, G. CARULLO) generati dalla diffusione capillare di dispositivi di uso comune (telefoni, carte di credito, elettrodomestici, automobili, ecc.) che, appunto, continuamente producono e trasmettono dati riguardanti le persone e le cose.

L'incremento esponenziale della quantità dei dati a disposizione, affiancato dalla crescente potenza computazionale disponibile, hanno aperto le porte ad una nuova dimensione tecnologica, in grado di elaborare queste informazioni secondo modelli e sistemi di nuova generazione che qui definiremo sinteticamente, "algoritmici".

La caratteristica propria di questi modelli algoritmici – detti anche di "intelligenza artificiale" – è che essi, sulla base dei dati da cui *apprendono* (il cosiddetto *machine learning*), sono in grado non solo di determinare misure, ma anche di effettuare valutazioni o previsioni e, quindi, *decisioni*.

Il dato, dunque, molto significativo per l'amministrazione pubblica, è che, nella prospettiva *algoritmica*, la tecnologia digitale non viene usata – soltanto – per "redigere" un atto amministrativo, per conservarlo o per trasmetterlo, ma viene usata per *determinarne il contenuto*, ovverosia per "decidere" (F. FOLLIERI, 2017).

Questa distinzione, in realtà non è nuova. La stessa giurisprudenza amministrativa ha riproposto una distinzione dottrinale in realtà risalente alla metà degli anni 2000 (C. GIURDANELLA e E. GUARNACCIA), tra atti ad *"elaborazione elettronica*" ed atti "*in forma elettronica*" (T.A.R. Lazio, sez. III-*bis*, sentenza 22 marzo 2017, n. 3769).

In base a questa classificazione, un conto è «l'atto materialmente redatto mediante lo strumento informatico e, quindi, sostanzialmente con un programma di videoscrittura»; a ben altro livello «si pone […] il cd. *atto ad elaborazione elettronica*, ossia l'atto amministrativo che è predisposto mediante il computer. In questo caso l'elaborazione del contenuto dell'atto viene affidata interamente allo strumento informatico e, quindi, in definitiva alla macchina, la quale provvede direttamente al reperimento, al collegamento e alla interrelazione tra norme e dati assumendo, conseguentemente, un ruolo strumentale rispetto all'atto amministrativo conclusivo. Nella predetta fattispecie è l'elaborazione stessa del contenuto dell'atto che si svolge elettronicamente, elaborazione che consiste, appunto, nello svolgimento dell'iter logico che conduce alla redazione dell'atto finale in relazione al rispettivo contenuto e che concretizza la sua motivazione; il documento finale che contiene la predetta elaborazione, invece, può avere qualsiasi forma ammessa dall'ordinamento e, quindi, essere anche cartaceo, come avviene negli atti amministrativi di stampo tradizionale».

Il settore sul quale ci soffermeremo per valutarne le implicazioni a livello costituzionale, quindi, è quello in cui l'amministrazione digitale non utilizza la tecnologia solo per dare forma alle decisioni prese, bensì per determinarne il *contenuto* (C. COGLIANESE, D. LEHR, 2017).

L'impiego di questi algoritmi decisionali nel settore privato è un fenomeno in una crescita travolgente, rappresentando il cuore di quello che è stato definito il "capitalismo di sorveglianza" (S. ZUBOFF, 2019). Si pensi, ad esempio, al ruolo della cosiddetta "profilazione" – tecnica attraverso la quale si predicono le preferenze e gli stili di vita delle persone, sulla base dei dati reperibili sulla rete – nelle decisioni riguardanti il marketing in generale, la determinazione delle polizze assicurative ovvero la concessione del credito bancario o la selezione del personale; altrettanto basata su algoritmi predittivi è la gran parte del settore dell'*e-commerce*, così come la cosiddetta "sharing economy", anch'essa legata a doppio filo ad elaborazioni di natura algoritmica, sia nel settore trasporti che in quello dell'*housing*; per non parlare, infine, degli algoritmi utilizzati già da molto tempo nella finanza (soprattutto nel cosiddetto *High Frequency Trading*).

Ma il settore che ha reso "visibile" a tutti questa tecnologia, spesso nascosta ovvero "oscura" (sovente i modelli algoritmici sono stati definiti delle "black" boxes: "scatole nere"; F. PASQUALE, 2015), è l'impiego degli algoritmi nel mondo del web da parte delle aziende c.d. Big Tech per realizzare i propri profitti. Sono, infatti, algoritmi quelli che trovano le risposte alle nostre domande sui motori di ricerca: si pensi al monopolista Google – ovvero a Yahoo o Bing – quando inseriamo una richiesta: chi determina l'ordine delle risposte (o, me-

glio, l'ordine con il quale appaiono sul video)? Così come altrettanti algoritmi gestiscono la visualizzazione dei post sui nostri social media (si pensi, in questo caso, al monopolista Facebook – Instagram, ma anche ad altri social media come LinkedIn o Tik Tok); perché appaiono i link ad alcuni post e non ad altri? Quando cerchiamo qualcosa da comprare su Amazon, un appartamento da affittare su Airbnb o un film da noleggiare su Netflix, chi suggerisce le proposte? E, soprattutto – visto che queste aziende vivono di pubblicità – chi decide la comparsa degli avvisi pubblicitari ogniqualvolta utilizziamo questi grandi mercati digitali?

La risposta è: algoritmi basati sui dati che immettiamo ogniqualvolta utilizziamo queste (o altre) grandi piattaforme private per avere accesso alla rete.

Una tale rivoluzione per il settore privato non poteva non avere un impatto anche sulle attività dei poteri pubblici.

Il fenomeno è evidente soprattutto ad uno sguardo comparato. Uno dei settori in cui da più tempo vengono impiegati tali sistemi è l'amministrazione fiscale. Negli Stati Uniti lo US Internal Revenue Service (IRS), l'agenzia governativa deputata alla riscossione dei tributi, ha cominciato sin dal 2005 ad usare procedure di controllo per le piccole imprese e per quelle individuali basate su analisi di *machine learning*. L'IRS ha aumentato le richieste per finanziare propri strumenti di accertamento automatizzati da 1,4 milioni USD nel 2012 ad oltre 39 milioni USD nel 2016, specificamente per sviluppare metodi migliori di *machine learning*, comprese le reti neurali, per identificare le aree emergenti di evasione. Ma si pensi al vasto campo degli *accertamenti presuntivi* nel diritto tributario italiano (dal cosiddetto "redditometro" agli "studi di settore" ovvero agli automatismi in materia di accertamento fiscale). Un altro caso di *enforcemement* automatizzato nella legislazione tributaria è il cosiddetto "*Robodebt*" australiano: un sistema di recupero automatico nel caso in cui un soggetto percepisca più prestazioni sociali di quelle a cui abbia effettivamente diritto. L'algoritmo confronta i guadagni effettivi con quelli comunicati dal datore di lavoro e, poi, incrocia questi dati con altri ottenuti dalla rete (impiego carte di credito, spese registrate, ecc.); se il cittadino ha ricevuto (in prestazioni sociali) più di quanto abbia effettivamente avuto diritto, vengono inviate automaticamente le ingiunzioni di pagamento (A. SIMONCINI [2], 2019).

Altri settori in cui le decisioni amministrative basate su algoritmi stanno crescendo in maniera esponenziale è quello dei settori ambientale, alimentare e della amministrazione finanziaria. Negli Stati Uniti, da tempo sono applicati sistemi predittivi per la selezione dei controlli sulla rischiosità di agenti chimici dalla EPA ("Toxicity Forecast – ToxCast"), così come nel campo dei controlli sulle attrezzature mediche da parte della Food and Drug Administration. An-

cora, il Massachussetts Institute of Technology sta collaborando con il Dipartimento del Tesoro USA per mettere a punto dei sistemi algoritmici predittivi per stimare il rischio sistemico nel mercato del credito al consumo. Così come altrettanto diffuso, non solo negli States ma anche in Cina, è l'utilizzo di sistemi predittivi nella attività di *law enforcement* – polizia di pubblica sicurezza – attraverso il cosiddetto "predictive policing".

Dalla Cina infine viene probabilmente l'ultima frontiera – ed anche la più inquietante – nell'utilizzo di questi sistemi predittivi: il cosiddetto *Social Credit Scoring*, un sistema governativo di classificazione della reputazione di cittadini e imprese cui correlare l'accesso a benefici economici e servizi pubblici (D. Mac Síthigh e M. Siems, 2019).

Ma l'area di impiego degli algoritmi nel settore pubblico non è limitata al settore amministrativo. Se guardiamo sempre oltreoceano, un importante "branch" che impiega sistemi automatizzati è il potere giudiziario. Il caso certamente più noto di applicazione giudiziaria di algoritmi predittivi è il cosiddetto "caso Compas", arrivato alla Corte Suprema dello Stato del Winsconsin, in cui è stato utilizzato un software prodotto da una società privata (Compas) per "calcolare" la pericolosità sociale di un imputato e dunque decidere la pena. Ma già da molto tempo nei *parole boards* americani (le corti incaricate di prendere le decisioni sulla richiesta di libertà su cauzione) vengono utilizzati algoritmi predittivi per determinare l'ammontare della cauzione da versare.

Anche in Italia abbiamo settori nei quali l'amministrazione, oltre ad essere digitale, è *algoritmica*, ovverosia utilizza sistemi automatizzati per prendere decisioni. Su questi ci soffermeremo nel prossimo paragrafo.

3. La creatività nel formante giurisprudenziale, dalla *rule of law* alla *rule of technology*: alcuni casi

Dopo aver chiarito cosa intendiamo per amministrazione algoritmica e aver offerto un seppur sintetico sguardo comparato, veniamo allo scenario italiano.

Per affrontare una "terra incognita" qual è l'amministrazione digitale algoritmica, sarà bene seguire un approccio empirico-casistico piuttosto che teorico-deduttivo, muovendo dai casi che la prassi suggerisce e dai principi che i giudici, esaminando da tali casi, hanno sin qui elaborato.

La giurisprudenza amministrativa italiana, infatti, si è trovata negli ultimi anni a decidere una serie di questioni che hanno proprio questo elemento in comune: provvedimenti della Pubblica Amministrazione determinati da sistemi di decisione automatica guidati da algoritmi (D.-U. GALETTA e J.G. CORVALÀN, 2019).

Il "terreno di coltura" che ha favorito la nascita di questi casi è duplice.

Da un lato, procedure ad evidenza pubblica nelle quali il sistema di presentazione ed accettazione delle domande è stato affidato a piattaforme telematiche (ovviamente, questa scelta è in grande espansione tra le amministrazioni pubbliche sia centrali, che locali o autonome, in cui la fase di accettazione di domande o istanze da parte di privati avviene prevalentemente per via telematica) dimodoché chiunque voglia partecipare ad un concorso, un appalto, ovvero ad una selezione, deve presentare domanda in via telematica.

In questa prima area di contenzioso, i problemi nascono di solito da provvedimenti amministrativi di esclusione adottati in via automatica dalle "procedure" stesse; decisioni "robotiche" (M. LUCIANI 2018), che, però, spesso sono il prodotto di *malfunzionamenti* del sistema (si immagini, ad esempio, una domanda che il candidato ad un concorso non sia riuscito ad inviare tempestivamente perché il sistema non è stato accessibile per un certo periodo prima del termine).

Un'altra fonte di numerosi contenziosi giudiziari è stata la Legge 13 luglio 2015, n. 107, meglio nota come "buona scuola". A seguito dell'entrata in vigore di questa legge, il Ministero dell'Istruzione ha deciso che le assegnazioni delle sedi di servizio agli insegnanti vincitori di concorso, o le decisioni sulle loro richieste di mobilità, venissero effettuate da un *software* che, tenendo conto della normativa, dei risultati dei concorsi e delle disponibilità delle sedi di servizio, provvedesse a stilare automaticamente le graduatorie per le assegnazioni ovvero per i trasferimenti.

Tale scelta ha innescato un ampio dibattito pubblico e, conseguentemente, una serie di istanze giurisdizionali, vòlte sia a richiedere l'accesso al codice sorgente del *software* che ad impugnare le decisioni prodotte dall'algoritmo e ritenute dai ricorrenti, errate, contraddittorie o irragionevoli.

Da queste vicende, seppur diverse tra loro, sono scaturite una serie di pronunce che oggi compongono un vero e proprio *corpus* giurisprudenziale sull'impiego di algoritmi decisionali da parte della Pubblica Amministrazione; *corpus* che varrà ricostruire e valutare alla luce dei principi costituzionali euronazionali.

3.1. L'esclusione automatica da gare o concorsi

Come dicevamo, una prima serie di questioni nasce da vicende tra loro sostanzialmente simili: un soggetto viene escluso "automaticamente" da una procedura amministrativa a seguito del malfunzionamento del sistema infor-

matico di accettazione delle domande (*ex multis* Cons. Stato, sez. VI, sentenza 18 maggio 2020, n. 3148).

Sempre più di frequente, bandi emanati da autorità pubbliche (ma il problema si pone analogamente per i soggetti privati) per l'ammissione a benefici ovvero per partecipare a gare o concorsi, prevedono che l'invio della domanda debba avvenire *esclusivamente* tramite un certo sportello telematico.

Altrettanto di frequente, tali sportelli o piattaforme vanno incontro a malfunzionamenti di diversa natura: non si riesce ad inviare la domanda, pur avendo seguito tutte le istruzioni, ovvero non si riesce a dimostrare che si è tentato di presentare la domanda ovvero, nonostante si sia presentata la domanda, per problemi tecnici essa non è stata esaminata, ovvero infine, la domanda, dopo essere stata presentata, è stata inavvertitamente cancellata, causando così la perdita definitiva di qualsiasi traccia anche dell'avvenuta cancellazione.

In tutte queste circostanze, i ricorrenti vengono a subire provvedimenti (espliciti o impliciti) di esclusione dalla procedura, non adottati da funzionari, ma da automatismi decisionali, e per di più, malfunzionanti.

Si dirà, dov'è la questione giuridicamente problematica? Vasta e consolidata è la giurisprudenza amministrativa sui principi giuridici da applicare alla validità (o meno) delle domande o delle istanze nei casi in cui la tardività, ovvero la mancata presentazione, derivi da cause non imputabili ai richiedenti. Si applicheranno i principi generali della Legge 7 agosto 1190, n. 241 sul procedimento amministrativo, in particolare quelli sulla partecipazione e sul dovere di soccorso procedimentale di cui agli artt. 6, 7, 8, 9, 10 e 10-*bis* della stessa legge ovvero la giurisprudenza sul codice della amministrazione digitale, che normalmente attribuiscono alla PA la responsabilità per le *sue* scelte organizzative; se l'Amministrazione decide di avvalersi di un sistema telematico di accettazione delle domande, il privato non potrà subire conseguenze negative da malfunzionamenti che non dipendano da una sua negligenza.

E infatti, com'è stato efficacemente sintetizzato dalla giurisprudenza, nel momento in cui le tecnologie informatiche vengono utilizzate dalle amministrazioni, divengono parte integrante dell'organizzazione. Conseguentemente, l'amministrazione deve essere responsabile del corretto funzionamento delle stesse. Difatti, gli obiettivi che con la digitalizzazione si intendono perseguire risulterebbero frustrati se non fosse previsto un adeguato sistema di responsabilità delle amministrazioni in relazione al loro funzionamento (B. BARMANN, 2016).

Il punto che qui interessa evidenziare è che in questi casi la giurisprudenza ha a più riprese evidenziato la manifesta irragionevolezza, ingiustizia ed irrazionalità di sistemi di presentazione delle domande di partecipazione ad un

concorso che, «a causa di meri malfunzionamenti tecnici, giunga[no] ad esercitare impersonalmente attività amministrativa sostanziale, disponendo esclusioni de facto riconducibili a mere anomalie informatiche» (T.A.R. Lazio, sez. III-*bis*, sentenza 1° giugno 2020, n. 7406).

Si sottolinea infatti che nell'ambito di un procedimento tenuto con modalità telematiche, la scadenza del termine di presentazione della domanda non può essere considerata alla stessa stregua della scadenza del termine di presentazione nell'ambito di un tradizionale procedimento cartaceo, in cui eventuali problematiche (ad esempio, scioperi aerei, incidenti, ecc.) vanno ricondotte nella comune sfera di diligenza dell'interessato. Nel caso di domande telematiche, invece, il rispetto del termine di presentazione della domanda dipende da variabili assolutamente imprevedibili e non "quantificabili" in termini di tempo, e cioè dalle concrete modalità di configurazione del sistema informativo, anche qualora la compilazione sia affidata a soggetti competenti.

E così, in queste pronunce i giudici ribadiscono quale sia il ruolo conferibile all'impiego dello strumento informatico in seno al procedimento, ossia il principio generale secondo il quale «le procedure informatiche applicate ai procedimenti amministrativi devono collocarsi in una posizione necessariamente servente rispetto agli stessi», non essendo concepibile che, per problematiche di tipo tecnico, sia ostacolato l'ordinato svolgimento dei rapporti tra privato e Pubblica Amministrazione e fra Pubbliche Amministrazioni nei reciproci rapporti (Cons. Stato, sez. VI, sentenza 18 maggio 2020, n. 3148).

Perciò, anche quando alla piattaforma telematica si deferiscano attività puramente vincolate o meccaniche e prive di qualsiasi valutazione discrezionale, la giurisprudenza ammonisce che dev'essere prevista comunque la possibilità dell'intervento umano, mediante "*procedure amministrative parallele*" di tipo tradizionale ed attivabili in via di emergenza, in caso di non corretto funzionamento dei sistemi informatici predisposti per il fisiologico inoltro della domanda.

In questa direzione, anche il ben noto principio del soccorso procedimentale prende una nuova luce. Da esso, infatti, si desumerebbe l'impossibilità generale di affidare un procedimento *esclusivamente* ad un algoritmo decisionale, giacché questo, nella sua rigidità "impersonale", non potrebbe – per sua stessa struttura (o natura?) – esercitare un'azione di soccorso (E. FREDIANI, 2016).

3.2. Le decisioni algoritmiche riguardanti il personale della scuola

Il secondo insieme di decisioni, invece, riguarda l'applicazione della Legge 13 luglio 2015, n. 107 sulla riforma della scuola (la c.d. "buona scuola").

A seguito della entrata in vigore di questa nuova legge, il Ministero del-

l'Istruzione si è trovato a dover gestire un numero rilevantissimo di richieste di prima assegnazione, ovvero di mobilità, da ordinare, selezionare e decidere sulla base sia della complessa regolamentazione normativa, sia delle diverse condizioni dei richiedenti nonché delle disponibilità delle sedi di servizio.

Il Ministero, quindi, ha deciso di affidare la redazione delle graduatorie per le assegnazioni alle sedi di servizio degli insegnanti, ovvero le decisioni sulle loro richieste di mobilità, ad un *software* prodotto da una società privata che tenesse conto di tutte le complesse variabili di natura legale e fattuale.

Le decisioni prodotte dall'algoritmo hanno però generato molteplici contestazioni, essendo spesso accusate di essere "oscure", "impazzite", "errate", insomma, incomprensibili.

Così, un sindacato di insegnanti ha chiesto di effettuare l'accesso al codice sorgente dell'algoritmo di assegnazione, sulla base dell'art. 22 della legge sul procedimento amministrativo. Il Ministero ha inizialmente rigettato l'istanza di accesso, sicché il sindacato ha impugnato il diniego dinanzi al T.A.R. Lazio.

La difesa del Ministero dinanzi al T.A.R. si è fondata su due elementi qualificanti.

Innanzitutto, il codice sorgente del programma in questione (in quanto scritto in linguaggio di programmazione e contenuto in un supporto immateriale – un *file* –) non sarebbe stato, in realtà, un documento amministrativo ai sensi della Legge n. 241/1990, né un atto amministrativo informatico ai sensi dell'art. 22, lett. D), della stessa legge; in secondo luogo, il *software*, essendo stato prodotto da una società privata, sarebbe stato protetto dalla legislazione sulla tutela dei *software* come opera dell'ingegno.

La sezione III-*bis* del T.A.R. Lazio, pronunciandosi sulla questione con la sentenza 22 marzo 2017, n. 3769 si è quindi soffermata sul tema dei rapporti tra procedimento amministrativo e le decisioni prodotte da algoritmi.

Innanzitutto, il giudice amministrativo ha sgombrato il campo dalla principale eccezione avanzata dal Ministero (secondo cui il *software* non sarebbe un documento amministrativo): l'algoritmo, determinando di fatto il contenuto dell'atto di assegnazione/trasferimento dell'insegnante, *sostanzia* il procedimento che dà vita all'atto amministrativo e, conseguentemente, dà diritto all'interessato "di prenderne visione ed estrarne copia" come stabilito dalla legge sul procedimento amministrativo.

Utilizzando, come abbiamo già osservato, una distinzione dottrinale abbastanza risalente tra "atto ammnistrativo elettronico" ed "atto amministrativo ad elaborazione elettronica", l'argomentazione del giudice amministrativo è stata stringente: è con il software che si concretizza «la volontà finale dell'amministrazione procedente»; è con il software che, in definitiva, l'amministrazione «costituisce, modifica o estingue le situazioni giuridiche individuali» anche se

lo stesso non produce effetti in via diretta all'esterno; il *software* finisce per «identificarsi e concretizzare lo stesso procedimento».

La circostanza che il software sia compilato mediante linguaggi di programmazione che sono solitamente incomprensibili non solo al funzionario che ne fa uso, ma anche al privato destinatario dell'atto stesso, «non appare dirimente atteso che, da un lato, la predetta circostanza è conseguenza della scelta, questa sì discrezionale dell'amministrazione, di ricorrere a uno strumento innovativo, quale è ancora la programmazione informatica, per la gestione di un procedimento di propria spettanza e competenza e che, dall'altro, ai fini della sua comprensione e della verifica della sua correttezza, il privato destinatario dell'atto, in particolare, può, comunque, legittimamente avvalersi dell'attività professionale di un informatico competente in materia» (così ancora T.A.R. Lazio, ult. cit.).

L'algoritmo decisionale, quindi, sostanzia l'atto amministrativo sebbene non sia scritto in lingua italiana, bensì in un linguaggio informatico compilato secondo un determinato codice di programmazione; questa precisazione consente di risolvere anche un ulteriore aspetto collaterale, ma interessante della controversia.

Dinanzi, infatti, ad una prima istanza di accesso del ricorrente, il Ministero aveva risposto consegnando effettivamente un documento denominato «Descrizione dell'algoritmo» in cui si specificava solamente che la procedura informatica utilizzata «si articola nei seguenti passi: Predisposizione dati, Input, Assegnazione ambiti e scuole, Diffusione risultati».

Orbene, il T.A.R. con il medesimo pronunciamento ha chiarito che una risposta di tal genere è evidentemente elusiva e non soddisfa in alcun modo l'interesse del ricorrente ad avere accesso al documento, dal momento che sebbene l'amministrazione abbia effettivamente fornito a parte ricorrente le istruzioni espresse in lingua italiana e in forma di algoritmo, tuttavia, «non si può escludere l'interesse e il diritto per il destinatario dell'atto […] di avere piena contezza anche del programma informatico», che può aversi solo con l'acquisizione del relativo linguaggio sorgente del software relativo all'algoritmo di cui trattasi. È evidente, infatti, che «la mera descrizione dell'algoritmo e del suo funzionamento in lingua italiana non assolve alla medesima funzione conoscitiva data dall'acquisizione diretta del linguaggio informatico sorgente» (ancora T.A.R. Lazio, ult. cit.).

È, infatti, solo all'interno del codice scritto in linguaggio informatico che si può cogliere effettivamente il contenuto della decisione e la sua motivazione.

Una volta riconosciuto il diritto di accesso, cade l'altra obiezione opposta dal Ministero: quella per cui il *software*, essendo un'opera dell'ingegno, sarebbe coperto da proprietà intellettuale e, dunque, destinato a rimanere riservato.

Il T.A.R. non nega la natura di opera dell'ingegno del *software* prodotto per conto del MIUR. Tale qualificazione tuttavia, non assume rilevanza dirimente in quanto, di norma, in materia di accesso agli atti della P.A., ai sensi dell'art. 24 della Legge 7 agosto 1990, n. 241, la natura di opera dell'ingegno dei documenti di cui si chiede l'ostensione non rappresenta una causa di per sé una causa di giustificato diniego dell'accesso.

La decisione ora richiamata nelle sue linee essenziali va segnalata anche per un *obiter dictum* di grande rilievo teorico che, come vedremo, la stessa sezione riprenderà come vera e propria *ratio decidendi* di controversie successive, salvo poi una parziale "correzione di rotta" imposta da più recenti pronunce del Consiglio di Stato.

Sostiene il T.A.R. Lazio che, soffermandosi sull'ulteriore questione dell'esatta estensione dell'ambito di operatività della specifica tipologia di atto amministrativo informatico (*rectius* algoritmico), quanto al diverso tenore della discrezionalità esercitata nella specifica materia da parte dell'amministrazione pubblica, si può giungere alla conclusione che essa è giuridicamente ammissibile e legittima quanto all'attività *vincolata* dell'amministrazione, perché *compatibile* con la logica propria dell'elaboratore elettronico. Ciò in quanto il *software* traduce gli elementi di fatto e i dati giuridici in linguaggio matematico dando vita a un ragionamento logico formalizzato che porta a una conclusione che, sulla base dei dati iniziali, è immutabile.

Come è evidente, diversa è la valutazione che deve essere compiuta per quanto riguarda l'attività *discrezionale* della Pubblica Amministrazione, nell'ambito della quale l'amministrazione ha la possibilità di scelta dei mezzi da utilizzare per la realizzazione dei fini determinati dalla legge (D. SORACE, 2014).

In questa decisione, dunque, la sezione III-*bis* del T.A.R. Lazio ha ritenuto ammissibile l'uso di un algoritmo decisionale solo in quanto nel caso di specie era coinvolto un *potere amministrativo vincolato*; ben diversa – traspare dalle motivazioni della sentenza – sarebbe stata la conclusione nel caso in cui la decisione algoritmica avesse costituito l'esercizio di un potere amministrativo *discrezionale*, dal momento che «la prevalente dottrina ritiene che l'esercizio del potere discrezionale sia, con qualche riserva, incompatibile con l'elaborazione elettronica dell'atto amministrativo».

Successivamente la stessa sezione del T.A.R. Lazio (sentenza 10 settembre 2018, nn. 9224-9230), chiamata sempre a riesaminare la vicenda della assegnazione delle sedi di servizio ai vincitori del concorso per le cattedre della scuola superiore, è tornata sull'argomento, presentando una linea argomentativa ben più decisa.

Si è sostenuto infatti che gli istituti di partecipazione, di trasparenza e di

accesso, in sintesi, di relazione del privato con i pubblici poteri, non possono essere legittimamente mortificati e compressi, soppiantando l'attività umana con quella impersonale dell'algoritmo. Se ciò accadesse, ad essere inoltre vulnerato non sarebbe solo «il canone di trasparenza e di partecipazione procedimentale, ma anche l'obbligo di motivazione delle decisioni amministrative», con il risultato «di una frustrazione anche delle correlate garanzie processuali che declinano sul versante del diritto di azione e difesa in giudizio di cui all'art. 24 Cost.», diritto che risulta compromesso tutte le volte in cui l'assenza della motivazione non permette inizialmente all'interessato e successivamente, su impulso di questi, al Giudice, «di percepire l'iter logico – giuridico seguito dall'amministrazione per giungere ad un determinato approdo provvedimentale» (T.A.R. Lazio, ult. cit.).

In tale vicenda il giudice amministrativo dunque afferma in maniera netta che «non è conforme al vigente plesso normativo complessivo e ai dettami dell'art. 97 della Costituzione, ai principi ad esso sottesi, agli istituti di partecipazione procedimentale definiti [dalla] L. 7/8/1990, n. 241, all'obbligo di motivazione dei provvedimenti amministrativi sancito dall'art. 3, stessa legge, al principio ineludibile dell'interlocuzione personale intessuto nell'art. 6 della legge sul procedimento e a quello ad esso presupposto di istituzione della figura del responsabile del procedimento, affidare all'attivazione di meccanismi e sistemi informatici e al conseguente loro impersonale funzionamento, il dipanarsi di procedimenti amministrativi», sovente incidenti su interessi, se non diritti, di rilievo costituzionale, che invece postulano «il disimpegno di attività istruttoria, acquisitiva di rappresentazioni di circostanze di fatto e situazioni personali degli interessati destinatari del provvedimento finale, attività, talora ponderativa e comparativa di interessi e conseguentemente necessariamente motivazionale, che solo l'opera e l'attività dianoetica dell'uomo può svolgere».

Il T.A.R. Lazio conclude infine sostenendo che «le procedure informatiche, […] non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere» e che pertanto, «al fine di assicurare l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento, deve seguitare ad essere il dominus del procedimento stesso, all'uopo dominando le stesse procedure informatiche predisposte in funzione servente e alle quali va dunque riservato tutt'oggi un ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo, ostando alla deleteria prospettiva orwelliana di dismissione delle redini della funzione istruttoria e di abdicazione a quella provvedimentale, il presidio costituito dal

baluardo dei valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convezione europea dei diritti dell'uomo».

Abbiamo ritenuto di dover riportare questa ampia citazione, dal tono dichiaratamente dottrinale, perché in essa il T.A.R. sembra chiudere del tutto la porta all'impiego degli algoritmi nelle decisioni amministrative. La distinzione tra amministrazione vincolata ed amministrazione discrezionale – adombrata nella sentenza precedente – sembra travolta dalla infungibilità assoluta tra la valutazione "*dianoetica*" dell'essere umano e *l'impersonale* computazione algoritmica.

Sebbene – come si vedrà *infra* – tale orientamento restrittivo sarà superato dalla successiva giurisprudenza del Consiglio di Stato, ciò che preme sin d'ora sottolineare è il ruolo decisivo della dimensione *costituzionale* – e non solo legale – che la giurisprudenza evoca nelle sue argomentazioni. In gioco non ci sono *solo* i principi della legge sul procedimento amministrativo, ma direttamente l'art. 97 Cost., di cui tale legge è attuazione, nonché gli artt. 3, 24 Cost. e l'art. 6 della CEDU.

Da tali norme, i giudici amministrativi ricavano il principio secondo cui nessuna complessità pratica può legittimare la totale devoluzione di una decisione amministrativa ad un «meccanismo informatico o matematico del tutto impersonale e orfano di capacità valutazionali delle singole fattispecie concrete, tipiche invece della tradizionale e garantistica istruttoria procedimentale, che deve informare l'attività amministrativa, specie ove sfociante in atti provvedimentali incisivi di posizioni giuridiche soggettive di soggetti privati e di conseguenziali ovvie ricadute anche sugli apparati e gli assetti della pubblica amministrazione» (ancora T.A.R. Lazio, ult. cit.).

Per conseguenza, quando la decisione va ad incidere su posizioni giuridiche soggettive non può essere sostituita *tout court* da un algoritmo, perché una decisione del genere non consentirebbe l'esercizio del più elementare diritto che ogni persona ha quando viene toccata dal potere pubblico: conoscerne le ragioni per poterle contestare in punto di fatto e di diritto.

E, significativamente, il T.A.R. chiude idealmente il cerchio interpretativo richiamando proprio la sua stessa giurisprudenza sulle "esclusioni automatiche" che abbiamo esaminato al paragrafo precedente.

3.3. Dalla *rule of law* alla *rule of technology*

Come accennavamo, l'orientamento giurisprudenziale sopra richiamato è stato in parte rivisto da alcune più recenti pronunce della sesta sezione Consiglio di Stato (ci riferiamo in particolare alle sentenze 8 aprile 2019, n. 2770, 13 dicembre 2019, nn. 8472, 8473, 8474 e 4 febbraio 2020, n. 881), che pur fa-

cendo proprie molte delle considerazioni già svolte nei giudizi di primo grado, le hanno sviluppate cercando di offrire un quadro sistematico in cui comporre armonicamente i valori in gioco, correggendo alcune asperità delle altre decisioni che abbiamo esaminato. Quadro che sarà utile qui ricostruire.

Innanzitutto, i Giudici di Palazzo Spada affermano che in linea generale l'impiego di procedure informatiche nell'azione amministrativa è una scelta che deve essere "incoraggiata", in quanto rispondente ai princìpi generali di efficienza ed economicità (art. 1 della legge sul procedimento amministrativo) nonché ai precetti costituzionali contenuti nell'art. 97 Cost.: l'algoritmo che si inserisca in procedure seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili, e in cui sia assente ogni apprezzamento discrezionale, consente di accelerare i procedimenti amministrativi, garantendo al contempo una maggiore imparzialità.

Laddove, quindi, ci si trovi dinanzi ad amministrazione "vincolata" del tutto priva di scelte discrezionali, l'impiego della automazione è assolutamente auspicabile.

Qui, però, appare chiaro che il riferimento per i giudici è all'amministrazione *digitale* in senso stretto, così come l'abbiamo definita al par. 2, quella in cui la tecnologia viene utilizzata come un mezzo – più rapido ed efficiente – per portare a termine azioni del tutto "decise" dal personale (umano) della Amministrazione pubblica.

A conferma di questa impressione il Consiglio di Stato, si spinge a ricostruire una nozione – a quanto ci consta inedita – di «regola algoritmica» intesa come «regola amministrativa generale», ovverosia, una regola giuridica espressa in forma di algoritmo (M. PAPA, 2020).

Da tale ricostruzione derivano alcuni importanti corollari: (i) essa ha piena natura giuridica, con la conseguente soggezione ai princìpi di pubblicità, trasparenza, ragionevolezza, proporzionalità; (ii) non può, per definizione, lasciare spazi applicativi discrezionali, nel senso che essa deve 'prevedere' soluzioni definite *per tutti i casi possibili, anche i più improbabili;* (iii) deve rispondere agli interessi individuati, mediati e composti *ex ante* dalla legge o dalla stessa Amministrazione, durante tutta la durata del suo impiego. Ciò comporta che l'Amministrazione, dinanzi ad algoritmi ad "apprendimento progressivo" ovvero di "*deep learning*", è chiamata a monitorare continuativamente la rispondenza dell'algoritmo ai ridetti interessi mediante "test, aggiornamenti, modalità di perfezionamento"; (iv) deve contemplare la possibilità che il giudice valuti e accerti la correttezza del processo automatizzato.

Qui l'azione del *formante giurisprudenziale* (per utilizzare il lessico di Rodolfo Sacco) è davvero creativa.

Avendo a modello il principio di legalità della amministrazione (G. FASANO, 2019), si elabora una dottrina che potremmo definire di "legalità algoritmica" in cui il concreto "provvedimento" automatizzato, dev'essere conforme all'"astratta" disposizione algoritmica.

Il Consiglio di Stato dunque, nel primo dei pronunciamenti sopra richiamati, presuppone che la decisione automatizzata avvenga nell'area della amministrazione vincolata e sancisce che l'algoritmo abbia natura di "atto amministrativo informatico", con la conseguente applicazione della disciplina generale degli atti amministrativi. Tale assunto, in realtà, viene in parte messo in dubbio nella sua assolutezza, avendo affermato (la stessa sezione del Consiglio di Stato) che «se il ricorso agli strumenti informatici può apparire di più semplice utilizzo in relazione alla c.d. attività vincolata, nulla vieta che i medesimi fini predetti, perseguiti con il ricorso all'algoritmo informatico, possano perseguirsi anche in relazione ad attività connotata da ambiti di discrezionalità». Idea, questa, che la sentenza paventa potrebbe mettere in crisi l'applicabilità stessa "*di tutta*" legge sul procedimento amministrativo all'attività amministrativa algoritmica (Cons. Stato, sez. VI, sentenza 4 febbraio 2020, n. 881, punti 8 e 12).

La seconda dottrina potremmo definirla della "trasparenza algoritmica". In questo caso il modello è, invece, il principio di trasparenza che, in caso di decisioni automatizzate, dev'essere declinato in una versione "rafforzata", quantomeno sotto tre aspetti.

In primo luogo, il Consiglio di Stato, riprendendo un aspetto già sottolineato nella giurisprudenza T.A.R., richiede che «il meccanismo con cui si concretizza la decisione robotizzata» debba essere «conoscibile», il che implica la cognizione di una regola espressa in un «linguaggio differente da quello giuridico» (il linguaggio di programmazione informatica utilizzato per formulare l'algoritmo); essa, dunque, per essere pienamente conoscibile dev'essere anche – più specificamente – «comprensibile», ovvero traducibile, per così dire, dal linguaggio macchina al linguaggio umano. Comprensibilità che va garantita sia ai cittadini che al giudice ed in tutti gli aspetti: «dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti».

In secondo luogo, la regola algoritmica non solo dev'essere «conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo», chiamato a scrutinare l'esercizio del potere. Egli infatti è chiamato a valutare, da un lato, la «correttezza del processo informatico in tutte le sue componenti: dalla sua costruzione, all'inserimento dei dati, alla loro validità, alla loro gestione», dall'altro, la «logicità e ragionevolezza della de-

cisione amministrativa robotizzata, ovvero della "regola" che governa l'algoritmo».

Immaginiamo che i giudici – dunque magistrati di formazione ed educazione essenzialmente giuridica – dovranno fare ampio ricorso alla consulenza tecnica per effettuare queste valutazioni, che però, ricordiamo, non attengono ai fatti o ai documenti oggetto del contenzioso, ma alla stessa "regola algoritmica" da applicare.

E su questo punto potrebbe, quindi, nascere qualche tensione con il principio fondamentale della giurisdizione, per il quale *iura novit curia*.

In terzo luogo, infine, la più recente giurisprudenza del Consiglio di Stato fissa il principio di imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo. Ciò proprio in forza del quadro giuridico europeo di cui si darà conto nei parr. 4.1 e 4.2, che – più o meno esplicitamente – impone di garantire la riferibilità della decisione finale all'autorità ed all'organo competente in base alla legge attributiva del potere (Consiglio di Stato, ult. cit.).

Ci troviamo, quindi, dinanzi ad una vera e propria trasfigurazione del noto principio della *rule of law* in quello che potremmo chiamare "*rule of technology*" (oppure per non indulgere troppo in definizioni anglofone, dalla "legalità dell'amministrazione" alla "legalità della tecnologia").

La giurisprudenza, in effetti, nelle sue più recenti pronunce (tra la fine del 2019 e l'inizio del 2020), ha inteso ricostruire alcuni principi di carattere generale che debbono informare l'amministrazione digitale *algoritmica*. Segnatamente: il principio di conoscibilità dell'esistenza di processi decisionali automatizzati e delle logiche utilizzate, il principio di non esclusività della decisione algoritmica e infine di non discriminazione (sui quali, sia consentito il riferimento a A. SIMONCINI [1] 2019).

Su tutti questi ci soffermeremo nel par. 4, cercando di recuperarne la dimensione costituzionale. Per ora basti evidenziare che se con il termine "rule of law" siamo abituati ad esprimere quel valore tipico delle costituzioni democratiche, per il quale i pubblici poteri sono soggetti ai principi di legalità e di trasparenza, al fine di garantire la corrispondenza dell'azione pubblica alle finalità poste dalla legge e la piena sindacabilità giudiziaria di ogni atto pubblico, ebbene, oggi la "*rule of technology*" esprime una serie di tutele "rafforzate e specifiche" al fine di garantire gli stessi obiettivi (*legalità, trasparenza, non discriminazione*), ma dinanzi ad atti amministrativi digitali "algoritmici", ovverosia, il cui contenuto sia stabilito da processi di decisione automatizzata.

Questo approdo del formante giurisprudenziale è assolutamente condivisibile come intenzione ma, come torneremo a dire, estremamente limitato nella

sua portata. I principi elaborati dal Consiglio di Stato, infatti, si applicano solo ad un certo "tipo" di algoritmi, quelli utilizzati esclusivamente per atti nell'ambito della attività *vincolata* della PA; la "regola algoritmica", infatti, è una formulazione che «non può lasciare spazi applicativi discrezionali, nel senso che deve "prevedere" soluzioni definite per tutti i casi possibili, anche i più improbabili (…) deve rispondere agli interessi individuati, mediati e composti ex ante dalla legge o dalla stessa Amministrazione (…) deve contemplare la possibilità che il giudice valuti e accerti la correttezza del processo automatizzato».

In uno dei casi di specie (i concorsi scolastici) l'algoritmo è stato impiegato soltanto per consentire l'applicazione seriale di numerose regole obiettive predeterminate (disposte su diversi livelli gerarchici e competenziali) ad un numero elevatissimo di domande; ma non vi era discrezionalità o valutazione del profilo dei candidati, bensì solo calcoli estremamente complessi a causa delle molte variabili in gioco, ma pur sempre "calcoli".

In questo modo l'area di applicazione del principio della "*rule of technology*" si restringe solo ad alcune categorie di procedure automatizzate, quelle in cui *tutti* gli elementi decisionali siano fissati *ex ante* dalla legge o dalla Amministrazione e l'automazione riguardi solo la fase "deduttiva" o "applicativa".

I problemi nascono quando, come abbiamo già accennato, ci troviamo dinanzi a *nuovi* tipi di algoritmi, elaborati soprattutto seguendo i paradigmi dell'intelligenza artificiale (A. SIMONCINI, S. SUWEIS, 2019), che non solo consentono di "applicare" principi o criteri pre-determinati, ma, tramite sistemi di "apprendimento" e di training – come ad esempio quelli del c.d. *deep learning* – consentono di effettuare vere e proprie "valutazioni", "scelte", "decisioni"; cioè, per intendersi, attività tipiche della amministrazione discrezionale (se non addirittura di quella "libera") e non solo di quella vincolata.

La logica di questi nuovi algoritmi non è di natura scientifico-deterministica, ma statistico-probabilistica e, quindi, apre scenari del tutto nuovi. Ebbene dinanzi a *questo tipo* di amministrazione digitale algoritmica, *quid juris?*

Il Consiglio di Stato, nel far riferimento anche al "deep learning" ed alle forme di "apprendimento progressivo", pur mostrando consapevolezza della evoluzione tecnologica, ha esteso principi che ben si attagliano ad atti di amministrazione vincolata, a procedure che invece sono progettate per esprimere attività del tutto diverse e che, se vogliamo mantenere all'interno del quadro costituzionale, richiedono nuovi principi.

4. Principi costituzionali e decisioni algoritmiche: verso una "*constitutional*" rule of technology

Proviamo, dunque, ad allargare la nostra riflessione all'ambito della amministrazione digitale *algoritmica* nel suo complesso, comprendendo tutte le variabili possibili – almeno allo stato attuale della evoluzione tecnologica – dei sistemi di decisione automatizzata, sia di natura deterministica che non deterministica.

Una rapidissima premessa sul parametro che utilizzeremo in questa analisi.

Ovviamente esistono principi espressamente dedicati dalla nostra Costituzione alla amministrazione, intesa sia come azione che come organizzazione, come quelli di "imparzialità e buon andamento" (art. 97, comma 1, Cost.), ovvero il principio della tutela giurisdizionale nei confronti degli atti della PA (artt. 24, 103, 113 Cost.); esistono poi numerosi principi desumibili dal sistema costituzionale e che hanno trovato applicazione nella giurisprudenza costituzionale ed in importanti interventi legislativi, immediatamente attuativi dei principi costituzionali (quali, ad esempio, la Legge 7 agosto 1990, n. 241 sul procedimento amministrativo, il più volte citato D.Lgs. 7 marzo 2005, n. 82 sulla amministrazione digitale, ovvero il Codice del processo amministrativo approvato con il D.Lgs. 2 luglio 2010, n. 104, ecc.); principi quali quello di partecipazione, del giusto procedimento, di tempestività, trasparenza, proporzionalità, semplificazione, ragionevolezza, *et al.*

A questi, inoltre, andranno affiancati i principi del diritto europeo che, già per costante giurisprudenza costituzionale e ora in virtù dell'art. 117, comma 1, Cost., costituiscono un vincolo espresso alla potestà legislativa dello Stato e delle Regioni e dunque anche direttamente alla Amministrazione (V. ONIDA, 1967).

Il riferimento al diritto eurounitario è dirimente perché, come si vedrà, non solo a livello di fonti primarie – si pensi agli artt. 41, 42 e 43 della Carta dei diritti fondamentali dell'Unione Europea – ma anche nelle sue fonti derivate – in particolare il recente regolamento sulla disciplina generale della protezione dei dati personali (Regolamento UE n. 679/2016), meglio noto come GDPR (v. capitolo II, F. ROSSI DAL POZZO) – esso ha posto principi estremamente rilevanti in materia di decisioni algoritmiche.

4.1. Premessa: gli atti di amministrazione digitale *algoritmica*, sono (davvero) atti giuridici?

Il primo profilo di carattere teorico, ma denso di conseguenze sul piano effettuale, che riguarda gli atti di amministrazione digitale algoritmica concerne la loro configurabilità come "atti".

È chiaro che qui ci troviamo, in un certo senso, ancor prima della dimensione costituzionale; si tratta di confutare una obiezione che mina alla base la stessa "pensabilità" degli atti amministrativi algoritmici (ma non di quelli meramente *digitali*), come atti.

Non possiamo negare, in realtà, che l'idea di un atto *deciso* da una macchina – e non solo trascritto, tradotto, conservato, consultato, trasmesso – sfida alla radice gli stessi fondamenti della teoria dell'atto pubblico e l'idea della "regola algoritmica" elaborata dalla giurisprudenza amministrativa.

In alcuni passaggi giurisprudenziali che abbiamo riportato, in effetti, i giudici sembrano adombrare che l'attività "*impersonale*" svolta in applicazione di regole o procedure informatiche o matematiche, in realtà, non si possa definire come una vera e propria "*attività*", ovverosia un "prodotto delle *azioni* dell'uomo" (e in particolare T.A.R. Lazio, sez. III-*bis*, sentenze 10 settembre 2018, nn. 9224-9230). Scomodando addirittura il lessico aristotelico, si giunge ad affermare che viceversa si può avere *attività* amministrativa solo quando vi sia «l'attività dianoetica del funzionario, indispensabile per ponderare i fatti e gli interessi, anche quando ci si trovi dinanzi ad una mera attività vincolata», che «le procedure informatiche, anche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possono mai soppiantare, sostituendola davvero appieno, l'attività cognitiva» che «solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere […] ostando alla deleteria prospettiva orwelliana di dismissione delle redini della funzione istruttoria […], il presidio costituito dal baluardo dei valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convezione europea dei diritti dell'uomo» (ancora T.A.R. Lazio, ult. cit.).

Seguendo questa ricostruzione, una decisione amministrativa effettuata da un automa(tismo) non può di per sé considerarsi un *atto* giuridico.

In effetti, la distinzione tra "fatto" e "atto", rappresenta una delle nozioni basilari, comune sia alla teoria del diritto privato che del diritto pubblico e amministrativo.

Nella manualistica privata e pubblica (F. GALGANO, 1985; C. MORTATI, 1967; G. ZANOBINI, 1958) si suole definire come «fatto giuridico» «ogni accadimento, naturale o umano, al verificarsi del quale l'ordinamento giuridico ricollega un qualsiasi effetto giuridico». All'interno dei fatti giuridici si collo-

cano, poi, i fatti (giuridici) *umani*, «in cui la costituzione, modificazione o l'estinzione di un rapporto giuridico si produce solo come effetto di un consapevole e volontario comportamento dell'uomo». Solo in seguito, come sottocategoria dei fatti (giuridici) umani, appaiono gli "atti giuridici".

Li si può definire, sinteticamente, come «atti o dichiarazioni di volontà». L'elemento qualificante l'atto, a differenza dal mero fatto, è che l'atto è *espressione di volontà umana*; si parla di "atti giuridici" se l'evento causativo di conseguenze giuridiche «postula un intervento umano», affermano i maestri del diritto privato (A. TORRENTE, P. SCHLESINGER, 2011), ma praticamente identica è la distinzione che troviamo nella scienza del diritto pubblico ed amministrativo.

Così, ad esempio, Mortati (1967). «Un criterio generale di differenziazione, nell'ambito dei comportamenti umani, fra "fatti" ed "atti" è quello che la fa derivare dall'elemento della volontà e, su tale base […] "Atti", in senso proprio, sono quelli risultanti dalla manifestazione di volontà di un soggetto che la legge considera produttive di mutamento nelle situazioni giuridiche se effettuate nel rispetto delle condizioni e modalità da essa prescritte». Ed in termini sostanzialmente analoghi si esprime Guido Zanobini (1958), tra i maestri del diritto amministrativo: «gli atti giuridici sono atti volontari, dal diritto riconosciuti idonei a produrre effetti giuridici. Dicendo atti volontari, intendiamo non limitare gli atti giuridici ai soli atti o manifestazioni di volontà, come gli ordini, i divieti, i permessi o i consensi, ma vogliamo comprendere sotto la stessa denominazione qualunque altra manifestazione psichica, come le dichiarazioni di conoscenza, di opinione, di desiderio perché tutti questi costituiscono atti volontari» (in termini anche O. RANELLETTI, A. AMORTH, 1964).

Sia nelle citazioni giurisprudenziali dalle quali abbiamo preso le mosse, che in questi riferimenti dottrinali, il riferimento comune è alla volontà come elemento distintivo dell'atto, ma volontà intesa come *attività psichica*; rileggendo oggi i classici della teoria generale del diritto, l'impressione che si ricava è che essi diano per assodato che la manifestazione di volontà sia una attività essenzialmente *umana*.

A questo punto, la questione che si pone è: si può immaginare un atto – quindi una manifestazione di volontà – senza un riferimento, diretto o mediato, ad una attività *umana*?

Siamo ben consapevoli che il nostro diritto positivo già conosce casi in cui la volontà dell'atto giuridico è ricondotta a soggetti che *non sono* persone fisiche attuali. Si pensi agli atti delle persone giuridiche – sia private che pubbliche – ovvero alla responsabilità penale degli enti (D.Lgs. 8 giugno 2001, n. 231) oppure, infine, alla teoria della interpretazione degli atti (ad esempio,

quelli normativi) in cui nella ricostruzione della *ratio* di un atto, quasi mai si fa riferimento esclusivo alla volontà soggettiva della persona (o delle persone) che materialmente hanno preso quella decisione (si pensi al tema della interpretazione secondo *l'intentio legislatoris* e alle teorie "originaliste" ovvero "viventi" per determinare tale *intentio*).

Non v'è dubbio, però, che l'esistenza di un atto di volizione inteso (soggettivamente o oggettivamente) come la decisione di perseguire o accettare un certo fine come movente della propria azione, sia sempre stata considerata elemento fondamentale per l'esistenza stessa di un *atto*.

Tanto ciò è vero che se tale volontà è assente o si è formata in maniera impropria, l'atto conseguente (anche se stipulato da una persona giuridica) ne risulta viziato.

L'idea della volontà come attività di tipo psichico attribuibile (attualmente o potenzialmente) ad un soggetto umano è sicuramente un elemento centrale nella teoria generale del diritto moderno e contemporaneo.

Alessandro Levi, importante filosofo del diritto italiano del primo dopoguerra, volendo precisare la natura del *volere*, chiosava: «si potrebbe dire il volere "cosciente", se l'aggiunta non apparisse superflua, tosto che si rifletta che un volere incosciente, ammesso che fosse possibile, non sarebbe propriamente volere».

Certo Levi, scrivendo negli anni '50, non poteva immaginare che l'evoluzione tecnica ci avrebbe portato ad avere oggi sistemi tecnici in grado di esprimere *volontà* (intesa come capacità di scegliere e realizzare un comportamento idoneo al raggiungimento di fini determinati) ma del tutto *incoscienti* (quali dobbiamo ritenere i sistemi di intelligenza artificiale).

Il ruolo della volontà nell'atto giuridico rappresenta l'espressione dinamica della libertà umana, che può obbedire ovvero trasgredire la regola giuridica; di qui, la *necessità* della volontà. Una volontà libera, non deformata o compressa o ingannata, è condizione necessaria ai fini della validità dell'atto giuridico. La volontà, possiamo dire, è l'altra faccia della libertà, ma come si pone questo carattere dinanzi a manifestazioni di volontà generate da macchine? Macchine che, parafrasando il codice penale, potremmo descrivere come "capaci di intendere *ma non di volere*".

Ben si può comprendere, perciò, l'inquietudine di quei giudici, che escludono in radice la qualità di *atto* per tutti i provvedimenti amministrativi il cui contenuto è determinato *in toto* da un sistema di intelligenza artificiale senza alcun apporto sensibile di un decisore umano.

In effetti, solo in apparenza può sembrare più aperta la posizione del Consiglio di Stato. Il giudice amministrativo di appello, in effetti, ha riconosciuto la natura di "atto amministrativo informatico" agli atti adottati tramite algo-

ritmi, purché utilizzati nel ristretto campo delle decisioni "vincolate" (Cons. Stato, sentenza 8 aprile 2019, n. 2770). In questi casi, affermano i giudici di Palazzo Spada, «la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima, anche se ciò avviene in via esclusiva».

Come a dire: tutta la volontà è già espressa nella regola generale, rispetto alla quale il provvedimento algoritmico non rappresenta che una mera deduzione; ragion per cui, si può ammettere la qualificazione di atto, riconducendo all'"uomo e non alla macchina" la volontà manifestata.

Questo tema, com'è noto, è già emerso, sebbene non in area gius-pubblicistica, nel dibattito sulla responsabilità (civile e penale) dei robot (siano essi autoveicoli senza guidatore, droni o macchine utensili).

Sul punto vi è stato un rilevante pronunciamento da parte del Parlamento europeo che, nel 2017, ha approvato una risoluzione intitolata, "*Carta della robotica*", in cui viene esplicitamente presa in considerazione la situazione in cui ci si trovi dinanzi a robot "autonomi", intendendo «l'autonomia di un robot […] come la capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna; […] tale autonomia è di natura puramente tecnologica e il suo livello dipende dal grado di complessità con cui è stata progettata l'interazione di un robot con l'ambiente».

Ebbene, dinanzi alla ipotesi che tali robot autonomi possano causare danni, la risoluzione, da un lato auspica, correttamente, che «il futuro strumento legislativo, a prescindere dalla soluzione giuridica che applicherà alla responsabilità civile per i danni causati dai robot in casi diversi da quelli di danni alle cose, non dovrebbe in alcun modo limitare il tipo o l'entità dei danni che possono essere risarciti, né dovrebbe limitare le forme di risarcimento che possono essere offerte alla parte lesa per il semplice fatto che il danno è provocato da un soggetto non umano»; d'altra parte, però, afferma anche che «nell'ipotesi in cui un robot possa prendere decisioni autonome, le norme tradizionali non sono sufficienti per attivare la responsabilità per i danni causati da un robot, in quanto non consentirebbero di determinare qual è il soggetto cui incombe la responsabilità del risarcimento né di esigere da tale soggetto la riparazione dei danni causati».

Ovviamente questa asserita "insufficienza" delle norme tradizionali allo scopo di identificare il responsabile di "atti" lesivi può preoccupare, soprattutto, se immaginiamo che il danno non sia (soltanto) quello materiale/biologico causato da una "macchina" fisica, ma se esso derivi da una decisione automatica adottata da un pubblico potere ed incida su libertà fondamentali.

Dinanzi a questo dilemma, la posizione di matrice giurisprudenziale che si limita ad affermare il divieto assoluto di tali atti algoritmici, rischia di essere, da un lato, anacronistica e, dall'altro, probabilmente velleitaria perché difficilmente attuabile.

La diffusione di questi strumenti è oggi difficilmente arginabile e si consideri inoltre che già a livello europeo – ma su questo torneremo più avanti in dettaglio – non esiste un divieto *assoluto* di atti algoritmici, anche quando questi incidono su libertà fondamentali (cfr. art. 22 GDPR).

Molto più realistica, quindi, sul piano del diritto costituzionale vivente, anche se altrettanto impegnativa, appare la necessità di definire *comunque* un regime giuridico proprio di questi "atti senza volontà".

Dobbiamo identificare una "*constitutional*" rule of technology che garantisca comunque la possibilità di controllare questi atti, di verificarne la conformità al sistema normativo vigente e la giustiziabilità sul piano della tutela dei diritti.

A questi profili dedicheremo i paragrafi seguenti. Ma prima di procedere occorre tuttavia considerare un argomento di chiusura sul piano sistematico, applicabile quand'anche si ritenesse che gli atti pubblici decisi da algoritmi non siano propriamente "atti giuridici".

Se, infatti, davvero accedessimo a questa ipotesi, per cui una decisione *esclusivamente* algoritmica non rappresenti di per sé un *atto* in quanto non espressiva di volontà, non resterebbe che considerarla un *fatto*; d'altra parte l'ordinamento giuridico non si occupa solo di atti, ma anche di fatti e delle loro conseguenze.

L'aspetto ovviamente più complesso è che ad un *fatto* non si può estendere il regime giuridico proprio degli *atti*. Rimarrebbe, dunque, auspicabile che l'ordinamento si desse carico di prevedere una qualificazione specifica per "fatti" particolari come le decisioni robotiche, in modo da garantire una tutela "rafforzata" dei diritti delle persone coinvolte, per utilizzare l'espressione del Consiglio di Stato.

In ogni caso, in assenza di una specifica qualificazione giuridica di tali *fatti*, l'Amministrazione (come qualsiasi privato), dinanzi a lesioni dei diritti di terzi causate da decisioni algoritmiche, rimarrebbe esposta all'ordinaria responsabilità civile, penale ed amministrativa per *fatto* antigiuridico.

4.2. Il divieto di atti di amministrazione digitale "esclusivamente" algoritmica

Posto, quindi, che sia difficile immaginare un divieto assoluto di atti di amministrazione algoritmica, occorrerà iniziare a porre i pilastri – quantomeno a livello costituzionale – del regime giuridico della amministrazione algoritmica.

Il primo principio della *constitutional rule of technology* che si è affacciato nella più recente giurisprudenza amministrativa (Consiglio Stato, sez. VI, sentenze 13 dicembre 2019, nn. 8472, 8473, 8474 e 4 febbraio 2020, n. 881) è quello del «divieto di atti di amministrazione digitale *esclusivamente* algoritmica» (A. SIMONCINI [2], 2019).

In base a questo principio, che ha trovato autorevole conferma a livello di diritto europeo, la tecnologia può affiancare, supportare, ma mai "sostituire" l'intero procedimento decisionale, ovvero intere fasi endoprocedimentali, quando questi procedimenti incidono su diritti o interessi rilevanti.

Visto specularmente, si può descrivere come il dovere, per chi materialmente nel mondo della *computer science* scrive questi programmi, dello HITL (*Human in The Loop*). Quando la PA decide di avvalersi di strumenti di valutazione o di decisione automatica dovrà essere sempre prevista la possibilità di un intervento umano nel procedimento decisionale.

Come abbiamo già sottolineato, nel caso dei sistemi automatizzati per l'ammissione di domande a procedure selettive, alcuni giudici amministrativi giungono a prevedere, come auspicio *de jure condendo*, «procedure amministrative parallele di tipo tradizionale ed attivabili in via di emergenza, in caso di non corretto funzionamento dei sistemi informatici predisposti per il fisiologico inoltro della domanda» (Cons. Stato, sez. VI, sentenza 18 maggio 2020, n. 3148).

Questo principio, di "non esclusività" della decisione automatizzata, viene derivato direttamente dai valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convezione europea dei diritti dell'uomo che devono perciò necessariamente essere "filtrati" nel procedimento amministrativo.

A sostegno esplicito di questa prospettiva è intervenuto il Regolamento 2016/679/UE (GDPR) che, riprendendo una norma già presente nella precedente Direttiva 95/46/CE, all'art. 22 afferma che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

La norma europea non specifica il tipo di decisione; dunque, dobbiamo immaginare si riferisca a qualsiasi decisione presa da soggetti pubblici o privati.

Nella normativa euro-nazionale, dunque, esiste il divieto di decisioni "esclusivamente" ("solely", nella versione inglese) automatizzate.

Su questo punto, però, occorrerà una precisazione.

Esiste, infatti, una differenza cospicua tra la normativa europea ed i principi desumibili dalla nostra costituzione nazionale che fa ritenere la prospettiva costituzionale italiana ben più *garantista* di quella comunitaria.

Il divieto di decisioni esclusivamente algoritmiche, infatti, nell'art. 22 del GDPR è soggetto ad una amplissima serie di eccezioni (tanto che viene da dubitare della sua effettività come regola …).

In base al vigente diritto europeo, infatti, una decisione algoritmica può *legittimamente* incidere sui diritti della persona *anche senza alcun intervento umano* (dunque, una decisione può essere *esclusivamente* algoritmica):

a) quando sia necessaria per concludere o eseguire un contratto tra interessato e titolare del trattamento;
b) quando sia stata autorizzata dal diritto dell'Unione o dello stato membro;
c) quando vi sia il consenso esplicito dell'interessato.

È più che evidente che la portata di queste eccezioni, nei fatti, è vastissima.

L'inserimento di clausole volte ad autorizzare l'uso automatizzato dei dati nelle condizioni generali di contratto che sottoscriviamo (normalmente senza leggere …) nell'attivazione di una qualsiasi *app* sul *web*, è frequentissimo e di fatto riduce di molto l'area di applicazione del principio.

D'altra parte, sappiamo bene – e tutta la storia dell'evoluzione della tutela legale della privacy lo dimostra – quanto oggi la possibilità di negare il consenso (il cosiddetto diritto di *opting-out*) rappresenti una forma debolissima di garanzia nella tutela dei diritti. Il nostro grado di dipendenza *pratica* dalle tecnologie e l'asimmetria tra i contraenti quando ad essere coinvolta nell'accordo è una delle c.d. Big Tech, fanno sì che la libertà o il consenso informato siano spesso mere *fictiones*, necessarie solo per sollevare dalla responsabilità civile i venditori di servizi tecnologici.

Ognuno rimane – teoricamente – libero di non dare il suo consenso … "semplicemente" non avrà accesso a servizi che, d'altra parte, sono gratuiti. Si tratterà, perciò, "solo" di rinunciare a Facebook, Instagram, Google, Google maps, Gmail, Youtube, LinkedIn, ecc. Ovvero a piattaforme tecnologiche – si pensi a quelle di videoconferenza – che in certe situazioni, e il pensiero va alla recente esperienza di *lockdown* causata dalla pandemia da COVID-19, si sono rivelate di fatto indispensabili per consentire il godimento di diritti fondamentali come quello al lavoro, all'istruzione o alla salute.

Senza poi considerare che nel caso dei procedimenti predisposti dai poteri pubblici spesso la soggezione alla decisione algoritmica è obbligatoria per legge (ovvero per norma di regolamento).

Già oggi quando l'Amministrazione si avvale di piattaforme telematiche, così come fanno le grandi compagnie private che vendono servizi digitali, normalmente richiede il preventivo consenso al trattamento dei dati ai sensi della disciplina del Codice della privacy, circostanza questa sufficiente a rendere legittima qualsiasi decisione automatica senza intervento umano.

In questi ultimi casi (di consenso prestato ovvero di esecuzione dei contratti) il GDPR pone in capo al titolare dei dati l'obbligo di garantire comunque il diritto dell'interessato ad ottenere un intervento umano o di esprimere la propria opinione o di contestare la decisione automatizzata, ma queste garanzie – nel diritto europeo – vengono meno quando la decisione automatica è prevista per legge dallo Stato membro, circostanza che ricorre spesso dinanzi a procedimenti amministrativi. Senza tener conto che dinanzi a queste eccezioni, l'intervento umano a garanzia dell'interessato avviene solo *ex post*, cioè dopo che la decisione automatica che lo riguarda è stata presa, configurando quindi, una forma di protezione solo successiva ed eventuale.

Il diritto europeo, quindi, al di là delle affermazioni di principio e di una certa opinione pubblica, è molto più favorevole all'utilizzo *esclusivo* delle decisioni automatiche di quanto possa sembrare.

Il diritto giurisprudenziale italiano, invece, – soprattutto quello espresso dai giudici amministrativi – fa un uso dei principi costituzionali nazionali e della Convenzione Europea dei Diritti dell'Uomo, molto più stringente della normativa espressa dal GDPR.

La giurisprudenza che abbiamo richiamato, infatti, è molto chiara nell'affermare che l'atto di un pubblico potere in cui vi sia una sostituzione completa della decisione umana da parte di un algoritmo ovvero di altro sistema automatizzato, è in radice illegittimo perché *incostituzionale*, prima che illegittimo ovvero in contrasto con i principi della legge sul procedimento amministrativo oppure del Codice della amministrazione digitale. L'aggancio diretto ai «valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convezione europea dei diritti dell'uomo» fanno sì che una eventuale violazione non potrebbe ritenersi sanata né dal consenso, né dall'esistenza di una previsione contrattuale e neppure – noi riteniamo – da una previsione legislativa *ad hoc*.

La tutela interna, dunque, è più ampia e più forte di quella europea.

Ci troviamo dinanzi ad uno di quei casi in cui il principio di massima espansione della tutela costituzionale gioca decisamente a favore dell'ordinamento interno rispetto a quello europeo; la garanzia del diritto fondamentale a non essere "colpiti" da decisioni "esclusivamente" algoritmiche a livello nazionale è più ampia che a livello europeo. D'altra parte, ciò non deve stupire.

Questa tensione si spiega agevolmente per la dialettica strutturale che esiste tra diritto europeo e le identità costituzionali nazionali e che ha trovato recezione nell'art. 4 del Trattato sull'Unione.

In questa materia – come spesso accade in altri settori di competenza dell'Unione Europea – emergono due modi molto diversi di concepire il bilanciamento tra i diversi valori costituzionali in gioco: da un lato, la tutela della

libertà e della dignità della persona e dei suoi dati (il cosiddetto *habeas data* (T.E. FROSINI, 2011) ovvero la *digital persona*) e dall'altra, il valore della libera circolazione dei dati, risorsa economica fondamentale per il mercato digitale. Mentre, a livello europeo, il punto di equilibrio è molto più spostato sul versante della libera circolazione ed elaborazione dei dati, a livello interno, prevale decisamente la tutela della libertà della persona dinanzi ai trattamenti automatizzati.

Sarà, quindi, molto interessante seguire il dialogo che verosimilmente si instaurerà tra questo orientamento giurisprudenziale interno e quello della Corte di giustizia dell'UE nella applicazione dell'art. 22 del GDPR.

4.3. L'obbligo di motivazione nella amministrazione digitale "algoritmica"

Il secondo pilastro della *Constitutional Rule of Technology* attinge anch'esso agli strati profondi della teoria del diritto pubblico ed è in qualche modo legato al primo.

Se il primo afferma che tutte le decisioni algoritmiche debbono prevedere la possibilità di un intervento umano, il secondo può essere espresso così: ogni decisione algoritmica deve essere basata su una motivazione umanamente comprensibile.

Come chiaramente sintetizza la giurisprudenza, vulnerato non sarebbe solo «il canone di trasparenza e di partecipazione procedimentale, ma anche l'obbligo di motivazione delle decisioni amministrative, con il risultato di una frustrazione anche delle correlate garanzie processuali che declinano sul versante del diritto di azione e difesa in giudizio di cui all'art. 24 Cost., diritto che risulta compromesso tutte le volte in cui l'assenza della motivazione non permette inizialmente all'interessato e successivamente, su impulso di questi, al Giudice, di percepire l'iter logico-giuridico seguito dall'amministrazione per giungere ad un determinato approdo provvedimentale» (T.A.R. Lazio, sez. III-*bis*, sentenza 10 settembre 2018, nn. 9224-9230).

O, in maniera ancora più netta: «l'ammissibilità dell'elaborazione elettronica dell'atto amministrativo non è legata alla natura discrezionale o vincolata dell'atto quanto invece alla possibilità, che tuttavia è scientifica e non invece giuridica, di ricostruzione dell'iter logico sulla base del quale l'atto stesso possa essere emanato per mezzo di procedure automatizzate quanto al relativo contenuto dispositivo» (T.A.R. Lazio, sez. III-*bis*, sentenza 22 marzo 2017, n. 3769).

Insomma, «la "caratterizzazione multidisciplinare" dell'algoritmo (costru-

zione che certo non richiede solo competenze giuridiche, ma tecniche, informatiche, statistiche, amministrative) non esime dalla necessità che la "formula tecnica", che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella "regola giuridica" ad essa sottesa e che la rendano leggibile e comprensibile» (Cons. Stato, sez. VI, sentenza 4 febbraio 2020, n. 881. Su cui si rinvia al capitolo III, D.-U. GALETTA).

Qui, come si vede, non è neppure in discussione la natura di amministrazione vincolata o discrezionale, bensì la mera delega di una decisione amministrativa ad una macchina, mette a rischio – *sul piano scientifico, prima che giuridico* – il diritto di ciascun interessato a conoscere la "ragione" di tale decisione, per utilizzare la formulazione dell'art. 41 della Carta dei diritti fondamentali dell'Unione Europea, in cui si sancisce il dovere della PA di "dare ragione" delle proprie decisioni.

Una decisione presa "algoritmicamente", infatti, rischia di privare *strutturalmente* il suo destinatario della possibilità di ricostruirne l'*iter* logico.

Si apre qui il tema della motivazione dell'atto amministrativo *algoritmico* e di quello *digitale*, per riprendere la distinzione che abbiamo richiamato al par. 3.1.

Nell'atto meramente digitale, ovvero *in forma elettronica*, la decisione è determinata dall'essere umano e di conseguenza anche la motivazione, sebbene espressa in forma è elettronica.

Nell'atto algoritmico, invece, il problema della motivazione ovvero della ragione alla base della scelta o della decisione, si pone in maniera tutt'affatto diversa.

Secondo una certa ricostruzione non vi sarebbero problemi a tracciare un parallelo tra i due tipi di atto amministrativo: così come non vi è nessun ostacolo per gli atti aventi forma elettronica (in tal caso anche la motivazione sarà in forma elettronica), allo stesso modo per gli atti ad elaborazione elettronica sarebbe plausibile la *motivazione elettronica* generata, appunto, mediante l'automatico reperimento, collegamento e giustapposizione di norme e dati.

Esisterebbe quindi una motivazione propria della amministrazione "algoritmica", definibile come il meccanismo automatico di "reperimento, collegamento e giustapposizione di norme e dati" (C. GIURDANELLA, E. GUARNACCIA).

Orbene, su questo punto occorre un approfondimento.

L'idea che si possa sempre determinare una motivazione, seppur "*elettronica*", degli algoritmi non tiene conto del cambio di paradigma subito dall'intelligenza artificiale negli anni più recenti (v. capitolo IV, R. CAVALLO PERIN e I. ALBERTI).

Oggi infatti ci troviamo dinanzi ad algoritmi – soprattutto quelli predittivi –

che non hanno necessariamente una logica, quantomeno nel senso filosofico o deterministico-matematico, con cui normalmente utilizziamo il termine "logica" (A. SIMONCINI, S. SUWEIS, 2019).

La maggior parte degli algoritmi di nuova generazione non si limita a dedurre in maniera deterministica conseguenze già contenute negli assiomi prefissati dal programmatore, sussumendo fatti concreti, ma in virtù dei sistemi automatici di apprendimento (*machine learning*) cui abbiamo fatto cenno in avvio, essi stessi producono i propri criteri di inferenza. Criteri che in molti casi non sono comprensibili agli stessi programmatori; ha avuto una certa notorietà il caso di due algoritmi di intelligenza artificiale incaricati di simulare tra di loro una serie di negoziazioni concatenate e che, ad un certo punto, hanno autonomamente "cambiato" la lingua della negoziazione: dall'inglese ad una lingua del tutto incomprensibile per gli umani, ma più "immediata" ed "efficiente" per le macchine; l'esperimento è stato immediatamente interrotto.

D'altra parte, questo tipo di algoritmi non è costruito per rispondere a domande circa il "*perché*" avverrà una certa cosa, ma solo ad indicare con la maggiore accuratezza possibile, la probabilità che essa avvenga (C. COGLIANESE, D. LEHR, 2017). Affinché si possa conoscere la motivazione con la quale un algoritmo prende una certa decisione, occorrerebbe che tale algoritmo fosse – non tanto *ragionevole*, perché potrebbe comunque produrre decisioni commisurate allo scopo, quanto – "*razionabile*" (dalla *rationabilitas* canonica; C. MINELLI, 2015) ovvero, come si preferisce nella terminologia tecnica più aggiornata, "*esplicabile*"; cioè interamente descrivibile nella sua strutturazione causale, in modo da poterne "ripercorrerne l'iter logico", come chiedono i giudici.

Questa qualità oggi non è un carattere *necessario* di tutti i sistemi di decisione automatica ed anzi sono rapidamente in aumento le tecnologie basate sul cosiddetto "*deep learning*" ovverosia sistemi di apprendimento automatico che simulano l'azione del cervello (M. LOLLER-ANDERSEN, E. FOLKESTAD, M. GOPINATHAN e Ø. NYGARD, 2018).

In questi casi – quand'anche si volesse riconoscere all'algoritmo la natura di "atto" (vedi *supra* par. 4.1) – esso sarebbe strutturalmente inconoscibile (o in-*esplicabile*), perlomeno con gli strumenti ordinari della logica umana.

Non è un caso che il tema più scottante nel dibattito scientifico odierno all'interno della comunità scientifica che si occupa di intelligenza artificiale sia proprio quello sulla cosiddetta "*XAI*" (ovvero *Explainable Artificial Intelligence*); detto altrimenti: come riuscire a garantire "trasparenza effettiva", ovvero "esplicabilità," agli algoritmi che per gran parte oggi sono delle "scatole nere" (F. PASQUALE, 2015).

Il diritto europeo (artt. 13, comma 2, lett. f) e 14, comma 2, lett. g) del

GDPR; sostanzialmente anticipati già dall'art. 12 della Direttiva 95/46/CE), nonché l'attuazione che ne è stata data a livello nazionale, sanciscono solennemente il principio generale per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in questo caso, a «ricevere informazioni significative sulla logica utilizzata» (artt. 13, 14 e 15 del GDPR). Ma anche in questo caso valgono i *caveat* che abbiamo già espresso sul principio di "esclusività", *sub* par. 4.2. La normativa del GDPR è intrinsecamente debole, dal momento che la mera conoscenza dell'esistenza di un algoritmo, non produce in sé nessun effetto se non si è in grado di decifrarne la logica, se cioè non potessimo comprendere perché tale procedimento metta assieme i dati in un *certo* modo e quindi giunga a *certe* conclusioni. In altri termini, che applicazione verrà data degli artt. 13 e 14 GDPR dinanzi a decisioni automatizzate delle quali non sia possibile dare «informazioni significative sulla logica» utilizzata?

Ovviamente, su questi temi sarà decisiva la giurisprudenza costituzionale nazionale e della Corte di Lussemburgo nella interpretazione di questa previsione.

Una ipotesi ermeneutica che si potrebbe prospettare è quella di una interpretazione combinata dell'art. 22 – che richiede il necessario intervento umano nelle decisioni automatiche che incidono sulle libertà (cfr. *supra* par. 4.2) – con gli artt. 13, 14 e 15 del GDPR – che attribuiscono all'interessato il diritto ad avere accesso ad informazioni significative – dalla quale risulti che la necessità dell'intervento umano si sostanzi proprio nella funzione di fornire quelle "informazioni significative sulla logica" della decisione automatizzata e che ne costituiscano, in sostanza, la motivazione.

In questo senso la formulazione dei diritti previsti agli artt. 13, 14 (obbligo per il titolare dei dati nei confronti dell'interessato alla informazione sull'esistenza di un processo decisionale automatizzato e, in tali casi, a informazioni significative sulla logica utilizzata) e 15 (diritto dell'interessato di accesso a tali processi ed alle informazioni di cui sopra) come diritti generali degli interessati, potrebbe far venir meno o quantomeno moderare, in sede di interpretazione giudiziaria sistematica, l'applicazione delle numerose eccezioni all'art. 22 che come abbiamo visto in moltissimi casi consente che decisioni automatizzate siano prese *senza intervento umano*. Anche nei casi in cui è stato prestato consenso ovvero è previsto dalle condizioni generali di contratto, l'intervento umano diventa necessario per rendere effettivi i diritti di informazione ed accesso garantiti a tutti negli artt. 13, 14 e 15.

Peraltro, su questo specifico tema è intervenuto anche il *Conseil Constitutionnel* (Décision n° 2018-765 DC du 12 June 2018), sollecitato a pronunciarsi sulla proposta francese di legge di adeguamento al GDPR.

Il *Conseil* ha respinto la *saisine* proposta da una minoranza di senatori, ritenendo in generale che l'assetto della legge di adeguamento fosse conforme a Costituzione; uno dei profili di incostituzionalità sollevato riguardava proprio il fatto che determinati algoritmi di nuova generazione, capaci di "auto-apprendimento", potessero rivedere essi stessi le regole applicate, «empêchant, selon eux, de ce fait, l'administration de connaître les règles sur le fondement desquelles la décision administrative a été effectivement prise (…) Les règles appliquées par ce dernier type d'algorithmes ne pouvant être déterminées à l'avance, il en résulterait également une méconnaissance du "principe de publicité des règlements"».

La posizione del *Conseil* è molto significativa. I giudici costituzionali francesi, infatti, hanno confermato la possibilità giuridica di una decisione amministrativa esclusivamente algoritmica, ma subordinando tale possibilità ad alcune condizioni.

Innanzitutto, le regole e i criteri sulla base dei quali è costruito l'algoritmo debbono essere predeterminati dal responsabile del trattamento (riecheggiando un po' la teoria della "regola algoritmica previa" elaborata dal Consiglio di Stato italiano, *sub* par. 3.3). Ma, soprattutto, «il responsabile del trattamento deve garantire la supervisione ("maîtrise") dell'elaborazione algoritmica e delle sue evoluzioni, in modo tale da poter spiegare in dettaglio e in una forma intelligibile all'interessato il modo in cui il trattamento è stato messo attuato nei suoi riguardi».

L'algoritmo, quindi, secondo il giudice costituzionale francese dev'essere esplicabile dal responsabile del procedimento.

Anche da questa decisione, dunque, viene un'ulteriore spinta verso l'intellegibilità della motivazione degli algoritmi decisionali, confermando quella tensione tra l'interpretazione giudiziaria interna ed una normativa europea che, in realtà, non vieta le decisioni amministrative automatizzate, ma si limita a porre in capo all'Amministrazione l'obbligo di dare «informazioni significative sulla logica» utilizzata; obbligo che nei casi di algoritmi non deterministici, come abbiamo visto, non è strutturalmente assolvibile.

4.4. Il principio di "non discriminazione" nella amministrazione digitale "algoritmica"

Il terzo pilastro *Constitutional Rule of Technology* è il principio di "non discriminazione" per via algoritmica.

Quand'anche ci trovassimo dinanzi ad un algoritmo perfettamente conoscibile e comprensibile (rispettoso del secondo principio, *supra* par. 4.3) e po-

sto anche che esso non rappresenti la motivazione esclusiva della decisione (rispettoso anche del primo principio, *supra* par. 4.2), l'algoritmo potrebbe essere *di per sé* discriminatorio e, dunque, incostituzionale per violazione del principio di uguaglianza.

Questo accade quando l'algoritmo predittivo è costruito ed addestrato su un set di dati che già in partenza è discriminatorio.

È il principio noto tra i *data scientists* come GIGO – «garbage in garbage out» – per cui un algoritmo non può che riflettere la qualità dei dati su cui è costruito.

Per chiarire quest'ultimo punto, può essere utile riprendere il dibattito che negli Stati Uniti ha seguito la nota decisione "Compas" cui abbiamo fatto cenno in precedenza (cfr. *supra* par. 2). In questo caso un giudice americano ha fatto uso di un algoritmo predittivo per determinare la pena da comminare in un processo penale. L'algoritmo utilizzato – appunto "Compas" – è prodotto dalla una società privata (Equivant) e valuta il rischio di recidiva e la pericolosità sociale di un individuo sulla base di vari dati statistici, precedenti giudiziari, questionari somministrati all'imputato stesso, nonché una serie di altre variabili che non è dato di conoscere perché coperte dalla proprietà intellettuale della società medesima.

L'algoritmo, per ciascun imputato e sulla base dei dati sopra richiamati, indica una classificazione in varie categorie di rischio, che vanno da "molto basso" a "molto alto".

Ebbene, un gruppo di esperti in computer science ha deciso di "testare" la affidabilità di questo software: ha individuato un campione di 10.000 imputati in una diversa contea (Broward, Florida) ed ha comparato il rischio di recidiva predetto dal sistema *Compas*, con il tasso di recidiva effettivamente realizzato dagli stessi imputati nei due anni successivi (i dati sono descritti in J. LARSON, S. MATTU, L. KIRCHNER e J.A. MAY).

Il risultato è che l'algoritmo presenta un margine di errore nella predizione della recidiva; e fin qui nulla di nuovo o sorprendente: il software Compas è pur sempre uno strumento orientato ad una predizione probabilistica. Il dato rilevante è, però, *come* l'algoritmo sbaglia.

Difatti l'analisi effettuata da questi studiosi mostra che l'errore nella predizione della recidiva, *sovrastima* sistematicamente il rischio per gli imputati di colore ed altrettanto sistematicamente sottostima il rischio per i bianchi.

Lo studio ha mostrato che la probabilità dell'algoritmo di sbagliare il giudizio nel caso di imputati di colore – definendoli ad alto rischio mentre in realtà non hanno compiuto nessun altro reato nei due anni successivi, i cosiddetti "falsi positivi" – era circa il doppio della probabilità di analogo errore per gli imputati bianchi (45% errore nei neri e 25% di errore nei bianchi).

Viceversa, l'algoritmo tendeva a giudicare gli imputati bianchi molto meno rischiosi di quanto effettivamente poi siano stati. L'analisi ha rilevato che gli imputati bianchi che hanno effettivamente recidivato nei successivi due anni – e che erano stati erroneamente etichettati come a basso rischio (i cosiddetti "falsi negativi") – sono quasi il doppio rispetto ai delinquenti di colore neri (48% contro 28%).

Dati ancora più discriminatori sono stati rilevati sui tassi di errore dell'algoritmo nel giudicare soggetti a rischio di recidiva *violenta* (il tasso di errore in caso di imputati bianchi che hanno effettivamente avuto recidive violente, ma erano stati erroneamente classificati a basso rischio, è stato del 63% più alto che per i neri).

Si pensi ad analoghe distorsioni che possono essere prodotte da algoritmi predittivi se utilizzati in altri settori che non siano la probabilità di recidiva: dal merito di credito, al costo delle assicurazioni, dalla profilazione per le assunzioni.

Esiste, dunque, un ulteriore problema di costituzionalità che può colpire le decisioni algoritmiche di tipo predittivo: quando esse nascano *intrinsecamente* distorte a causa dei dati di input che hanno alimentato le macchine incaricate di produrre l'algoritmo.

È, questo, il caso dell'algoritmo *geneticamente* incostituzionale; quello, cioè, che cade nella stessa fallacia che a metà del '700 Hume attribuiva alle teorie giusnaturalistiche: l'errore di derivare dall'essere (in questo caso dall'apparenza della realtà sociale, spesso ingiusta, parziale o distorta) il *dover* essere.

Di questi casi, purtroppo non vi è traccia di disposizione normativa espressa nel GDPR, anche se nei "considerando" premessi al Regolamento troviamo indicazioni estremamente significative.

Ci riferiamo in particolare al considerando n. 71 del Regolamento UE 679/2016, nella parte in cui afferma che «tenendo in considerazione le circostanze ed il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che com-

portano misure aventi tali effetti» (Regolamento 2016/679/UE, considerando n. 71, nostra la sottolineatura).

In questo passaggio, pur avendo ad oggetto un caso particolare di trattamento automatizzato, quello della *profilazione*, l'argomento è estendibile a qualsiasi altra forma di algoritmo predittivo.

Come abbiamo detto, queste prescrizioni hanno solo un valore interpretativo, in quanto contenute nella motivazione della fonte europea e non nelle sue disposizioni, ma esse debbono essere a loro volta considerate come direttamente espressive del principio generale di non discriminazione previsto sia nella Carta dei diritti fondamentali dell'Unione Europea (artt. 20 e ss) che nella Convenzione europea dei diritti dell'uomo (art. 14) che nostra Costituzione all'art. 3.

In realtà, il principio è già esistente nella giurisprudenza interna italiana cui abbiamo più volte fatto riferimento (Cons. Stato, sentenze 8 aprile 2019, n. 2770, 13 dicembre 2019, nn. 8472, 8473, 8474 e 4 febbraio 2020, n. 881) ed era stato in qualche modo auspicato dalla dottrina (A. SIMONCINI [1] 2019).

È evidente che questo principio di non discriminazione, ha una sua autonomia sul piano descrittivo-manualistico, nel senso che in effetti è frequente la possibilità di algoritmi decisionali "parziali" ovvero "biased" – per utilizzare il termine più ricorrente nella letteratura specialistica –. Per questo ne va evidenziata la incompatibilità con il nostro sistema costituzionale, dedicando uno specifico paragrafo di queste riflessioni.

Sul piano di una interpretazione orientata alla concreta applicazione del diritto, però, pensiamo che anche per quest'ultimo principio valga quanto abbiamo evidenziato per il secondo (*comprensibilità*, *supra* par. 4.3) e per il primo (non esclusività, *supra* par. 4.2); ovverosia, riteniamo che i tre principi nella loro concreta attuazione si sostengano a vicenda e sia impossibile una loro effettiva utilizzazione separata.

A ben vedere, infatti, se l'intervento umano serve a rendere conoscibile la motivazione e trasparente l'iter logico della decisione automatizzata, entrambi questi elementi sono decisivi per determinare in concreto l'esistenza o meno di una ragione discriminatoria o di una violazione del principio di eguaglianza.

Si potrebbe dire, in conclusione, che tutte e tre queste dimensioni sono necessarie per definire le coordinate dello "spazio" costituzionale in cui si muove l'amministrazione digitale algoritmica.

5. Spunti conclusivi. La dialettica "servo-padrone" nell'uso degli algoritmi

Proviamo a proporre qualche breve spunto conclusivo.

Noi pensiamo che non solo l'amministrazione digitale, ma che anche quella specificamente *algoritmica* sia destinata a crescere come importanza qualitativa ed impatto quantitativo sulla organizzazione dei poteri pubblici e nella vita dei cittadini.

In particolare, sarà molto difficile impedire all'intelligenza artificiale e le sue applicazioni di natura predittiva di entrare nei processi di decisione (pubblici e privati), giacché, per un verso, sarebbe anacronistico e per altro probabilmente ormai impossibile visto l'avanzamento della ricerca e la dimensione degli investimenti (A. SANTOSUOSSO, 2020).

Il futuro va, quindi, rapidamente verso un impiego sempre più diffuso delle tecnologie digitali e questa direzione non può (né deve necessariamente) essere cambiata. Soprattutto nell'ambito delle operazioni ripetitive o routinarie, l'automazione può produrre considerevoli risparmi e performances molto più efficaci ed efficienti.

La tecnica, però, non potrà, né dovrà, mai sostituirsi del tutto alla decisione umana, ogniqualvolta la decisione sia suscettibile di incidere sulle libertà fondamentali o i diritti costituzionali.

Questo principio vale non solo in caso di malfunzionamento degli strumenti tecnici adottati – laddove opera la responsabilità della PA per le scelte organizzative effettuate – ma anche quando la decisione è presa "ordinariamente" dalla macchina; e ciò, sia in caso di atti di natura vincolata, ma ancor più se si tratta di atti di natura discrezionale.

In questa direzione va il sistema costituzionale vivente, composto dai principi della nostra costituzione nazionale e da quelli desumibili dalla normativa europea e che si esprime in alcuni "metaprincipi" – che abbiamo proposto di chiamare *constitutional rule of technology* – posti a garanzia della amministrazione digitale algoritmica:

– il principio di *non esclusività*, per cui ogniqualvolta decisioni amministrative automatizzate possono interferire con i diritti e gli interessi della persona, occorre garantire effettivamente la possibilità di un intervento umano;

– il principio di *comprensibilità*, per cui ogni algoritmo decisionale utilizzato dalla PA per adottare un provvedimento dev'essere in grado di fornire una motivazione umanamente comprensibile della decisione (principio che assorbe, come abbiamo visto, quello di *non discriminazione*).

Il punto critico, soprattutto *pro futuro*, è che questa conclusione, desunta

sia dal diritto costituzionale euro-nazionale che da quello giurisprudenziale, è solo apparentemente appagante.

Nelle riflessioni sull'impatto della tecnica sulla amministrazione pubblica, ed in particolare di quella digitale, ricorre spesso l'idea di una natura "servente" (questo participio presente ricorre più volte nella giurisprudenza) della tecnologia rispetto all'essere umano, che invece dovrebbe comunque rimanere il "padrone" ("dominus") del procedimento e della decisione. L'idea della tecnologia "al servizio" dell'amministrazione, sembra – subliminalmente – evocare l'etimologia di *robot*, parola di origine ceca, che sta per "lavoro forzato", "schiavo".

I principi di non esclusività e di comprensibilità sembrano, appunto, essere la traduzione in termini costituzionali di questa destinazione *servente* della tecnologia.

Com'è noto, Hegel, nella *Fenomenologia dello spirito*, esamina il rapporto tra "servo e padrone", considerandolo un rapporto dialettico: l'autocoscienza dell'uno ha bisogno dell'altro per definirsi. L'impressione è che qualcosa di analogo stia accadendo nel rapporto tra decisioni umane (pubbliche o private) e tecnologia. Difatti, anche quando ribadiamo con forza che la tecnologia deve avere esclusivamente un valore "servente", in realtà non possiamo ignorare la sua travolgente "forza pratica", che tende a rendere "servo" il padrone.

Come ho cercato di dimostrare altrove (A. SIMONCINI [1], 2019), ogniqualvolta un automatismo decisionale venga inserito in un procedimento deliberativo, l'automatismo tende a "catturare" la decisione, o quantomeno a rendere estremamente difficile prescinderne.

Questo perché, da un lato, esso solleva il decisore dal *burden of motivation*, dal peso dell'esame e della motivazione; dall'altro, perché gli consente di "qualificare" la propria decisione con un crisma di "scientificità" ovvero "neutralità" che oggi circonda la valutazione algoritmica e le conferisce una peculiare – quanto infondata – "autorità". La decisione automatica quindi finirà sempre più per godere di quella che la *nudging theory* chiama la "*default-option force*": ovvero l'indubbio plusvalore "pratico" connesso alla scelta suggerita automaticamente dal sistema, rispetto alla quale ci si può discostare, ma a patto di impegnarsi in un notevole sforzo (e rischio) valutativo.

Si immagini – come è successo già nel concorso della riforma della scuola che ha dato occasione a molte delle pronunce che abbiamo esaminato – una amministrazione pubblica appesantita da procedimenti lunghi, ripetitivi e faticosi, spesso "schiava" di una normativa tutt'altro che semplice e con arretrati o tempi di attesa spesso insostenibili da parte degli utenti.

Sarà in grado di sottrarsi all'attrattiva di procedimenti impersonali, spesso immotivati, ma rapidi, veloci e – molto spesso – efficaci?

Ebbene, il rischio è che gli automatismi da "servi" divengano "padroni",

proprio in virtù della loro "attrattiva" pratica. È il mito della meccanizzazione delle attività "socialmente necessarie, ma fastidiose" che apre la strada a nuove forme organizzate di controllo politico, dal quale alcuni profeti non ascoltati ci avevano messo in guardia oltre 50 anni fa (MARCUSE, 1964) ed che riecheggia in altri pensatori contemporanei (BODEI, 2019).

Non possiamo nasconderci, infatti, che gli algoritmi esercitino un fascino discreto ma potentissimo: fanno risparmiare lavoro, tempo e, soprattutto, sembrano sollevare dal peso e dal rischio di dover motivare e rispondere di quelle motivazioni.

Proprio per questo abbiamo bisogno di un livello "costituzionale" di tutela, sovralegislativo e pronto anche ad arginare – utilizzando la propria identità – l'approccio mercantile del diritto europeo.

Una *constitutional rule of technology* che ponga al riparo valori e diritti, che altrimenti, molto probabilmente, saremmo del tutto disposti a barattare per un po' di lavoro in meno.

Bibliografia

BARMANN B., *La responsabilità della Amministrazione per il cattivo funzionamento dei sistemi informatici*, in *Giornale di diritto amministrativo*, 2016, p. 3.

BILANCIA P., PIZZETTI F.G., *Aspetti e problemi del costituzionalismo multilivello*, Giuffrè, Milano, 2004.

BODEI R., D*ominio e sottomissione. Schiavi, animali, macchine, intelligenza artificiale*, Il Mulino, Bologna, 2019.

CAVALLARO M.C., SMORTO G., *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in federalismi.it, 2019, p. 16.

CIVITARESE MATTEUCCI S., *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità*, in *Diritto pubblico*, 2019, p. 1.

CLARICH M., *Manuale di diritto amministrativo*, Il Mulino, Bologna, 2019.

COGLIANESE C. and LEHR D., *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era* (2017), *Faculty Scholarship at Penn Law. 1734.* https://scholarship.law.upenn.edu/faculty_scholarship/1734.

CONSTANT B., *La libertà degli antichi, paragonata a quella dei moderni*, 1819, ripubblicato da Einaudi, a cura di G. PAOLETTI, 2005.

DI MARTINO B., LI K., YANG L.T., ESPOSITO A., *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*, Springer, Singapore, 2017.

FASANO G., *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica,* in *MediaLaws*, 2019, p. 3.

FIORAVANTI M., *Lo Stato moderno in Europa*, Laterza, Roma-Bari, 2019.

FOLLIERI F. *Decisione amministrativa e atto vincolato*, in Federalismi.it, 2017, p. 7.

FREDIANI E., *Il dovere di soccorso procedimentale*, Editoriale Scientifica, Napoli, 2016.

FROSINI T.E., *Il diritto costituzionale di accesso a* internet, in M. PIETRANGELO (a cura di), Il diritto di accesso ad Internet, Collana ITTIG-CNR, Serie "Studi e documenti", n. 9, ESI, Napoli, 2011.

GALETTA D.-U., CORVALÀN J.G., *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in federalismi.it, 2019, p. 3.

GALGANO F., *Diritto privato*, Cedam, Padova, 1985.

GIURDANELLA C. ed GUARNACCIA E., *Elementi di diritto amministrativo elettronico*, Halley Editrice, Matelica, 2005.

GROSSI P., *L'ordine giuridico medievale*, Laterza, Roma-Bari, 1995.

LARSON J., MATTU S., KIRCHNER L. e ANGWIN J. May *How We Analyzed the COMPAS Recidivism Algorithm, Pro Publica* 23, 2016.

LEVI A., *Teoria generale del diritto*, Cedam, Padova, 1950.

LOLLER M.-ANDERSEN, FOLKESTAD E., GOPINATHAN M. E NYGARD Ø., *Current Trends in Deep Learning* in *Medium*, 28 dicembre 2018, knowitlabs.no/current-trends-in-deep-learning-85e378dc813.

LUCIANI M., *La decisione giudiziaria robotica*, in *Rivista AIC*, 2018, p. 3.

MAC SÍTHIGH D. and SIEMS M., *The Chinese social credit system: A model for other countries?,* in *EUI Working Paperes*, 2019, 1, in https://cadmus.eui.eu/bitstream/handle/1814/60424/LAW_2019_01.pdf?sequence=1&isAllowed=y.

MACLUHAN M., *Understanding Media: The Extensions of Man*, Mentor, New York, 1964.

MACRÌ I., MACRÌ U., PONTEVOLPE G., *Il nuovo Codice della amministrazione digitale*, Ipsoa, Milano, 2011.

MARCUSE H., *One-dimensional Man*, Beacon Press, Boston, 1964.

MARTINES F., *La digitalizzazione della pubblica amministrazione*, in *Rivista di diritto dei media*, 2018, p. 2.

MASUCCI A., *Atto amministrativo informatico*, *ad vocem*, in *Enciclopedia del diritto*, Giuffrè, Milano, 1997, I aggiornamento.

MASUCCI A., *L'atto amministrativo informatico*, Jovene, Napoli, 1993.

MINELLI C., *«Rationabilitas» e codificazione canonica. Alla ricerca di un linguaggio condiviso*, Giappichelli, Torino, 2015.

MORRONE A., *Sovranità*, in *Rivista AIC*, 2017, p. 3.

MORTATI C., *Istituzioni di diritto pubblico*, Tomo I, Cedam, Padova, 1967.

ONIDA V., *Pubblica amministrazione e costituzionalità delle leggi,* Giuffrè, Milano, 1967.

PAPA M., *Future crimes: intelligenza artificiale e rinnovamento del diritto penale*, in *Criminalia*, 2020.

PASQUALE F., *The Black Box Society*: *The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015.

PREDIERI A., *Gli elaboratori elettronici nell'amministrazione dello Stato*, Il Mulino, Bologna, 1971.

RANELLETTI O., AMORTH A., *Atti amministrativi* voce, in *Novissimo digesto italiano*, Utet, Torino, 1964.

SANTOSUOSSO A., *Intelligenza Artificiale e Diritto, Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano, Mondadori, 2020.

SIMONCINI A. [1], *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, p. 1.
SIMONCINI A. [2], *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 2019, p. 4.
SIMONCINI A. *Sovranità e potere nell'era digitale*, in T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di) *Diritti e libertà in internet*, Le Monnier, Firenze, 2017.
SIMONCINI A., SUWEIS S., *Il cambio di paradigma nell'intelligenza artificiale*, in *Rivista di Filosofia del Diritto*, 2019, p. 1.
SORACE D., *Diritto delle amministrazioni pubbliche. Una introduzione*, Il Mulino, Bologna, 2014.
TORRENTE A., SCHLESINGER P., *Manuale di diritto privato*, Giuffrè, Milano, 2011.
VIOLA L., *Attività amministrativa e intelligenza artificiale*, in *Ciberspazio e diritto*, 2019, pp. 1-2.
VIOLA L., *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Foro Amministrativo*, II, 2018, p. 9.
ZANOBINI G*., Corso di diritto Amministrativo,* Volume I, Giuffrè, Milano, 1958.
ZUBOFF S., *The age of surveillance capitalism*, Hacette Book Group, New York, 2019.

II.

IL MERCATO UNICO DIGITALE EUROPEO E IL REGOLAMENTO UE SULLA PRIVACY

Francesco Rossi Dal Pozzo

SOMMARIO: 1. La società dell'informazione e il ruolo dei dati. – 2. La politica dell'Unione Europea per l'instaurazione del mercato unico digitale. – 2.1. Il terzo pilastro: massimizzare il potenziale di crescita dell'economia digitale. – 3. La protezione dei dati personali. – 3.1. L'evoluzione del concetto di privacy tra diritto alla vita privata e protezione dei dati personali: profili di diritto internazionale. – 3.2. Il processo di affermazione della protezione dei dati personali nel contesto del diritto dell'Unione Europea. – 3.2.1. La prima fase: dai trattati di Roma alla Direttiva 96/45/CE. – 3.2.2. La seconda fase: la Carta UE e l'autonomia del diritto alla protezione dei dati personali. – 3.2.3. La terza fase: il Trattato di Lisbona e il bilanciamento tra diritti fondamentali. – 3.2.4. La quarta fase: la riforma della normativa in materia di protezione dei dati personali e il Regolamento Privacy. – 4. Il Regolamento 2016/679/UE. – 4.1. Un inquadramento generale della nuova disciplina dell'Unione Europea in materia di privacy. – 4.2. Le principali novità introdotte dal Regolamento (UE) 679/2016. – 4.2.1. L'estensione della nozione di dato personale. – 4.2.2. L'ambito di applicazione territoriale del Regolamento. – 4.2.3. I nuovi diritti introdotti dal Regolamento: il diritto all'oblio … – 4.2.4. … e il diritto alla portabilità dei dati. – 4.2.5. Brevi considerazioni sugli effetti delle novità introdotte dal Regolamento. – 5. L'adeguamento della normativa nazionale al Regolamento.

1. La società dell'informazione e il ruolo dei dati

Dalla fine degli anni '60 fino ad oggi, si è affermato un legame inedito, per ampiezza e significato, tra il processo di innovazione tecnologica e l'organizzazione economica e sociale europea: la c.d. "società dell'informazione". Questo modello di società si regge su una fitta rete di informazioni che il progresso tecnologico mette a disposizione dei cittadini, degli operatori economici e delle autorità pubbliche, sotto forma di dati.

A livello tecnico-informatico, infatti, dati ed informazioni sono concetti di-

stinti, ma strettamente interdipendenti (v. capitolo VI, G. CARULLO): i dati rappresentano le informazioni in un formato standard, il c.d. "codice binario", che ne consente il transito sulle reti di comunicazione, nonché l'elaborazione da parte dei computer.

L'avvento di Internet e l'affermazione del paradigma digitale su quello analogico hanno definitivamente consolidato la tendenza a convertire in dati un sempre più vasto ammontare di informazioni relative alla realtà fisica e alle esperienze personali. La navigazione web, la ricerca di contenuti sui motori di ricerca, l'acquisto di prodotti tramite siti di *e-commerce*, l'utilizzo di servizi di posta elettronica e le interazioni sui *social network* sono tutte attività tra le principali fonti dei dati in circolazione. Lo stesso vale per la diffusione dell'*Internet of Things* (IoT), una rete costituita da macchine e da dispositivi (*wearable device*, domotica, macchinari industriali intelligenti, autoveicoli a guida autonoma, ecc.), i quali, grazie alla dotazione di microprocessori e di sensori, sono in grado di generare una vasta mole di dati relativi ai cambiamenti del proprio stato e alle interazioni con l'ambiente circostante.

Questa ampia disponibilità dei dati si presta a molteplici forme di sfruttamento. Ad esempio, le pubbliche amministrazioni raccolgono i dati relativi ai propri cittadini per offrire servizi innovativi e più efficienti in diversi ambiti: trasporto pubblico, sanità, pianificazione del territorio, documentazione digitale, procedimento giudiziario telematico, pagamento di imposte e sanzioni, ecc. (v. capitolo III, D.-U. GALETTA).

Inoltre, i dati, quando elaborati o utilizzati in associazione a servizi e prodotti, possono generare un ingente valore economico. In particolare, la profilazione delle preferenze e delle abitudini di spesa dei consumatori, inferite sulla base dei dati dagli stessi dispersi nell'ambiente online, ha dato avvio a modelli economici innovativi improntati sull'offerta di beni e servizi personalizzati. E non solo, perché anche a livello macroscopico le tecnologie basate sui dati, quali i megadati (*Big Data*), il *Cloud Compuing* e l'Intelligenza artificiale, sono considerate essenziali per la competitività, l'innovazione e la digitalizzazione di tutti i settori, al punto che l'attuale stadio economico globale viene definito «data driven».

Dunque, se, in linea generale, è vero che l'odierna rivoluzione digitale ha quale substrato principale il progresso tecnologico-informatico, è altresì vero che, a ben vedere, quest'ultimo è a sua volta fondato sui dati e sulle relative modalità di impiego.

I dati rappresentano, quindi, una realtà rilevante e complessa con la quale anche il diritto si è dovuto misurare, certamente con non poca fatica, considerando l'incessante ritmo di sviluppo che ha dovuto sostenere. Un ritmo che, nello specifico, ha imposto all'ordinamento giuridico dell'Unione Europea

un'opera di costante «aggiornamento» di alcuni suoi concetti giuridici fondamentali.

Si fa riferimento, in primo luogo, al concetto di mercato unico, che è stato implementato dal legislatore dell'Unione Europea attraverso una serie di misure specifiche, racchiuse nella formula del c.d. "mercato unico digitale", con l'obiettivo di cogliere le potenzialità dirompenti correlate ai dati; in secondo luogo, al concetto di *privacy*, la cui più moderna connotazione di «*information privacy*», ossia di protezione dei dati personali, è emersa nell'ordinamento giuridico internazionale, ma ha trovato una più compiuta determinazione grazie all'azione combinata delle istituzioni dell'UE.

2. La politica dell'Unione Europea per l'instaurazione del mercato unico digitale

Nel marzo 2010, con l'obiettivo di superare la crisi finanziaria ed economica del 2008 e preparare l'economia dell'UE per le sfide del decennio successivo, la Commissione europea ha lanciato la strategia Europa 2020 (COM(2010) 2020), articolata in «sette iniziative faro», tra cui, per quanto qui interessa, la realizzazione della c.d. "Agenda digitale europea".

L'Agenda digitale europea, come precisato dalla Commissione europea nella relativa comunicazione (COM(2010) 245), era formata da una serie di proposte di azioni che l'Unione, di concerto con gli Stati membri, intendeva mettere in atto per sfruttare al meglio il potenziale offerto dal progresso tecnologico digitale e dalla rete internet. Tra queste proposte di azioni spiccava, per complessità e rilevanza, la realizzazione del «mercato unico digitale».

Oltre alla suddetta Agenda, anche altri atti hanno contribuito alla realizzazione del mercato unico digitale. Possono citarsi, a questo proposito, le comunicazioni sulla fiducia del mercato unico digitale (COM(2011) 942) e sulla *governance* del mercato unico (COM(2012) 259), con cui la Commissione europea ha sollecitato interventi normativi diretti ad adattare il commercio elettronico e i settori energetico e telecomunicazioni al *costituendo* mercato unico digitale. Sulla stessa linea si pongono anche le risoluzioni sull'*eGovernment* (2011/2178(INI)) e sul completamento del mercato unico digitale (2013/2655(RSP)), con cui il Parlamento europeo ha sottolineato l'importanza dei servizi amministrativi digitali per il mercato unico digitale, e ha individuato le aree normative preponderanti ai fini della realizzazione di tale mercato.

Sulla base delle suddette misure, nel maggio 2015, la Commissione ha adottato la Strategia sul mercato unico digitale (COM(2015) 192), definendolo

come «un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui, quale che sia la loro cittadinanza o nazionalità o il luogo di residenza, persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali».

Dal tenore letterale della definizione di mercato unico digitale emergono, da un lato, la sua diretta derivazione dal concetto di mercato unico, di cui all'art. 26 TFUE, e dall'altro lato, la sua cifra marcatamente economicistica. Nel contesto del mercato unico digitale, infatti, rientra una vasta serie di iniziative atte ad espandere l'ecosistema digitale, con ricadute dirette sul benessere dei consumatori e delle imprese.

Nello specifico, ai fini della realizzazione del mercato unico digitale, la Strategia ha individuato sedici azioni chiave interdipendenti, che devono essere attuate, attraverso l'adozione di atti normativi e non, esclusivamente a livello dell'Unione Europea. Tali azioni chiave si caratterizzano per un'elevata eterogeneità, testimoniata dal coinvolgimento, nel gruppo incaricato della loro realizzazione, di ben quattordici Commissari europei: mercato unico digitale; economia e società digitali; mercato interno, industria, imprenditoria e PMI; occupazione, affari sociali, competenze e mobilità dei lavoratori; giustizia, tutela dei consumatori e parità di genere; affari economici e finanziari, fiscalità e dogane; politica regionale; agricoltura e sviluppo rurale; stabilità finanziaria, servizi finanziari e mercato unico dei capitali; salute e sicurezza alimentare; trasporti; ricerca, scienza e innovazione; concorrenza; educazione, cultura, gioventù e sport.

Nonostante la loro eterogeneità, le azioni chiave sono state ripartite, *ratione materiae*, in «tre pilasti»: i) «migliore accesso dei consumatori e delle imprese ai beni e servizi digitali in tutta Europa»; ii) «creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi» e iii) «massimizzare il potenziale di crescita dell'economia digitale».

Ai fini della presente Trattazione sono, peraltro, essenzialmente le misure del terzo pilastro ad essere rilevanti ed è dunque su queste che si soffermerà brevemente l'attenzione.

2.1. Il terzo pilastro: massimizzare il potenziale di crescita dell'economia digitale

A differenza dei primi due pilastri, riguardanti portati tecnologici (contenuti online, servizi online) e settori (commercio elettronico, TLC, audiovisivo,

piattaforme online) *fondati sui dati*, il terzo e ultimo pilastro si occupa in modo specifico dei *dati*, considerati in sé e per sé. Esso, infatti, si propone di garantire la più ampia circolazione dei dati tra gli Stati membri, con l'intento di sfruttarne le capacità di generare valore economico. A tal proposito, come evidenziato dalla Commissione europea nelle comunicazioni «Costruire un'economia dei dati europea» (COM(2017) 9) e «A European strategy for data» (COM(2020) 66), i dati e le relative tecniche di analisi sono considerati risorse essenziali per la crescita economica ed il progresso sociale. L'utilizzo dei dati viene definito come una tendenza mondiale che presenta potenzialità enormi in vari campi (sanità, sicurezza alimentare, clima, uso efficiente delle risorse, energia, sistemi di trasporto intelligenti e città intelligenti) e che consente agli operatori del mercato, attraverso una varietà di applicazioni, di generare un ingente valore economico.

Tuttavia, per trarre vantaggio da tali opportunità, ai soggetti pubblici e privati, attivi nel mercato dei dati, deve essere garantito un accesso a quanti più ampi e diversificati *dataset* possibili. Obiettivo, questo, che tuttavia si scontra con le barriere rappresentate dai requisiti di localizzazione dei dati, imposti dalle autorità pubbliche o dagli orientamenti delle autorità amministrative, che richiedono la conservazione o l'elaborazione dei dati in un determinato formato elettronico con caratteristiche di scarsa interoperabilità. Secondo la Commissione, tali disposizioni rappresentano, di fatto, «la reintroduzione di "controlli di frontiera" digitali che frenano lo sviluppo di un'economia dei dati funzionante e dinamica».

Allo scopo di eliminare tali restrizioni e realizzare pienamente il potenziale dell'economia europea dei dati, il legislatore dell'UE ha adottato il Regolamento 2018/1807/UE (in *GUUE* L 303 del 28 novembre 2018, p. 59) in materia di circolazione dei dati non personali, i quali, come si avrà modo di osservare ampiamente in seguito (parr. 4 e ss.), sono dati che non contengono riferimenti ad una determinata persona fisica (ad es. dati sismici, metereologici, ecc.).

Tale regolamento si fonda sul c.d. "principio della libera circolazione dei dati all'interno dell'UE", il quale salvaguarda la libertà delle imprese di stipulare contratti che stabiliscano dove devono essere localizzati i dati, garantendo che il luogo individuato possa trovarsi ovunque nell'Unione.

Il regolamento, dunque, stabilisce il divieto di obblighi di localizzazione di dati, ad eccezione di quelli giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità (art. 4, par. 1). Ne consegue il dovere per gli Stati membri di informare immediatamente la Commissione europea dell'intenzione di introdurre eventuali nuovi obblighi di localizzazione dei dati (art. 4, par. 2), nonché di abrogare, entro il 30 maggio 2021, qualsiasi obbligo di localizzazione dei dati non giustificato (art. 4, par. 3). Inoltre, ai fini di una

maggiore trasparenza, gli Stati membri devono istituire un portale unico nazionale online d'informazione contenente tutti gli obblighi di localizzazione aggiornati (art. 4, par. 4).

Il regolamento prevede, altresì, che le autorità pubbliche possano richiedere l'accesso ai dati situati in un altro Stato membro e necessari per l'esercizio delle loro funzioni ufficiali, conformemente al diritto dell'Unione o nazionale (art. 5, par. 1). Per agevolare la cooperazione tra le autorità nazionali, il regolamento stabilisce l'obbligo per gli Stati membri di designare un punto di contatto unico che funge da collegamento con i punti di contatto degli altri Stati membri e la Commissione. La designazione e l'eventuale modifica di tali punti di contatto devono essere comunicate dagli Stati membri alla Commissione (art. 7, par. 1).

Inoltre, al fine di agevolare il più ampio utilizzo dei dati, il legislatore europeo, nel contesto del «Piano d'azione dell'UE per l'*eGovernment* 2016-2020 Accelerare la trasformazione digitale della pubblica amministrazione» (COM(2016) 179), ha adottato la Direttiva 2019/1024/UE (in *GUUE* L 172 del 26 giugno 2019, p. 56). La direttiva stabilisce il quadro giuridico necessario per incrementare la circolazione di particolari categorie di dati, ovvero quelli raccolti e generati dal settore pubblico degli Stati membri, come, ad esempio, i dati sociali, economici, giuridici, catastali, turistici, sanitari, geografici, ambientali, meteorologici, sismici, ecc. La direttiva si basa sul principio generale secondo cui i suddetti dati dovrebbero essere forniti in un formato elettronico di uso comune, ai cittadini e alle imprese, affinché questi se ne possano servire per fini commerciali o non commerciali.

In tale logica, la direttiva promuove l'utilizzo dei dati aperti (*open data*), ossia di dati presentati in formati che consentano il loro libero utilizzo e la loro condivisione per qualsiasi finalità. Pertanto, gli enti pubblici e le imprese pubbliche sono tenuti a mettere a disposizione i propri dati, ove possibile e opportuno per via elettronica, tramite formati aperti e leggibili, accessibili, reperibili e riutilizzabili meccanicamente (art. 1).

Gli enti pubblici devono, inoltre, esaminare le richieste di riutilizzo dei documenti rendendoli disponibili, nel suddetto formato, entro un lasso di tempo ragionevole (art. 4). Allo stesso tempo, essi devono adottare le disposizioni necessarie per facilitare la ricerca e il reperimento online dei documenti che conservano (art. 9). Tali disposizioni, peraltro, si pongono in stretto rapporto con la previsione dello sportello unico digitale, di cui al Regolamento 2018/1724/UE (in *GUUE* L 295 del 21 novembre 2018, p. 1), finalizzato ad agevolare l'accesso online alle informazioni, alle procedure amministrative e ai servizi di assistenza per cittadini UE e imprese che intendono vivere o svolgere attività economiche in altri Stati membri.

Parallelamente alle misure che incentivano la circolazione e l'utilizzo dei dati, l'Unione Europea ha mosso i primi passi anche verso la realizzazione di un quadro giuridico sull'intelligenza artificiale (IA), tecnologia strettamente connessa ai dati, in quanto motore delle elaborazioni a cui questi ultimi sono sottoposti. A tal proposito, il libro bianco della Commissione sull'intelligenza artificiale (COM(2020) 65), che segue alla strategia europea per l'IA (COM(2018) 237), definisce l'IA come un insieme di tecnologie che combina dati, algoritmi e potenza di calcolo e che, in sinergia con i dati, può occupare un ruolo essenziale per «la crescita economica sostenibile attuale e futura e il benessere sociale dell'Europa».

3. La protezione dei dati personali

3.1. L'evoluzione del concetto di privacy tra diritto alla vita privata e protezione dei dati personali: profili di diritto internazionale

L'odierno utilizzo, nel diritto dell'Unione Europea, del termine privacy, nella sua duplice accezione di diritto al rispetto della vita privata e di diritto alla protezione dei dati personali, è frutto di un lungo processo di evoluzione concettuale, che è dipeso in massima parte dall'emersione della società dell'informazione, e che ha avuto origine nell'ordinamento giuridico internazionale.

Nello specifico, il termine privacy è stato coniato nel 1890 da due giuristi americani, *Warren* e *Brandeis*, che gli hanno dedicato un saggio, intitolato «Right to privacy», traducibile con la formula «diritto al rispetto della vita privata» (S. WARREN, D. BRANDEIS, *The Right to Privacy*, 1890).

Tale diritto è stato inizialmente inteso solo in chiave negativa, cioè come obbligo rivolto alle autorità pubbliche di non interferire nella sfera privata dei propri cittadini («right to be let alone», dalla celebre definizione della Corte Suprema degli Stati Uniti d'America, caso *Public Utilities Commission c. Pollak*, 343 U.S. 451, 467 (1952)).

In tal senso, la Dichiarazione universale dei diritti dell'uomo (UDHR), adottata nel 1948 dall'Organizzazione delle Nazioni Unite, prevede, all'art. 12, che «[n]essun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni».

L'UDHR, seppur priva di natura giuridicamente vincolante, ha svolto un'influenza determinante nei confronti della successiva Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU),

il cui art. 8, par. 2, infatti, riprende dalla prima il divieto di ingerenza dell'autorità pubblica nella sfera privata del singolo. Detta disposizione precisa, inoltre, le condizioni di giustificazione di siffatta ingerenza, stabilendo che essa deve essere «prevista dalla legge e costituire una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui».

Tuttavia, se le condizioni di giustificazione costituivano già di per sé un elemento di novità rispetto ai precedenti testi pattizi, che ponevano il semplice divieto di ingerenze arbitrarie nella sfera privata da parte dell'autorità pubblica, l'aspetto più innovativo dell'art. 8 CEDU è rappresentato dal suo primo paragrafo, secondo cui «[o]gni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza».

L'art. 8, par. 1 CEDU, innanzitutto, fa della CEDU la prima fonte giuridica a riconoscere il diritto al rispetto della vita privata anche nella sua accezione positiva, che, come precisato dalla giurisprudenza della Corte EDU (C. eur. dir. uomo, *Marckx c. Belgio*, 13 giugno 1979), garantisce al singolo il diritto di formarsi liberamente una propria sfera privata, in cui sviluppare la propria identità. Inoltre, tale disposizione rappresenta la cornice teorica entro cui si è sviluppata un'ulteriore dimensione contenutistica del concetto di privacy.

Infatti, in concomitanza con la diffusione di quello che si è indicato come il paradigma tecnologico di fondo della società dell'informazione, ovvero l'elaborazione automatizzata delle informazioni sotto forma di dati, si è riconosciuta la necessità di accordare al singolo una forma di controllo sulla circolazione di quelle informazioni-dati che contribuivano a formare tale sfera privata.

Nasce così la protezione dei dati personali, la quale, pur avendo quale referente teorico il diritto al rispetto della vita privata di cui all'art. 8, par. 1 CEDU, si è sviluppata, quantomeno nella prima fase, al di fuori di quest'ambito. È infatti alla Convenzione n. 108 (Consiglio d'Europa, STCE n. 108, 1981, da ora «la Convenzione») che si deve la formulazione delle prime coordinate fondamentali di questa peculiare branca della disciplina sulla privacy, definita specificamente «information privacy».

Innanzitutto, la Convenzione garantisce sul territorio di ciascuno Stato Parte il rispetto del diritto alla vita privata di ciascuna persona fisica, con specifico riferimento al trattamento automatizzato dei suoi dati di carattere personale (art. 1). Con tale disposizione, dunque, la Convenzione ha dato una prima collocazione normativa alla protezione dei dati personali quale corollario del diritto al rispetto della vita privata.

La Convenzione, inoltre, ha introdotto alcune delle definizioni che permeeranno la materia per il tempo a venire: la nozione di *dato personale*, ossia

ciascuna informazione tramite la quale è possibile identificare una persona fisica, e il concetto di *trattamento automatizzato dei dati personali*, inteso come l'insieme delle «operazioni svolte in tutto o in parte tramite procedimenti automatizzati» tra cui figurano, nello specifico, la registrazione dei dati, l'effettuazione di operazioni logiche e/o aritmetiche su tali dati, la loro modificazione, cancellazione, estrazione o diffusione (art. 2).

Per quanto attiene all'ambito di applicazione della Convenzione, la protezione viene estesa a tutti i trattamenti di dati personali – quindi non solo a quelli effettuati dall'autorità pubblica –, tra cui, ad esempio, quelli svolti dalle autorità giudiziarie e di polizia, nonché i trattamenti effettuati dai soggetti privati, le cui attività di raccolta ed elaborazione di informazioni davano spazio ad un confronto sempre più serrato tra la tutela dei dati personali e l'interesse economico delle imprese alla conservazione e valorizzazione di cataloghi, quanto più ampi, di dati relativi ai propri consumatori (art. 3).

La Convenzione ha previsto numerose disposizioni volte a tutelare i dati personali oggetto di trattamento. A tal proposito, possono citarsi, innanzitutto, i principi atti a regolare il trattamento, in forza dei quali i dati personali devono essere: ottenuti ed elaborati lealmente e legalmente; registrati per fini determinati e legittimi; adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono trattati; esatti e, se necessario, aggiornati; conservati in una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati (art. 5). Tali disposizioni sono state integrate dalle previsioni relative ai diritti dell'individuo di essere informato della conservazione dei dati che lo riguardano e di chiedere la rettifica degli stessi (art. 8), nonché dalle garanzie specifiche per il trattamento dei dati definiti «sensibili», quali la razza, le opinioni politiche, la salute, la religione, l'orientamento sessuale o il casellario giudiziale (art. 6).

Le norme della Convenzione hanno rivestito un ruolo fondamentale anche nella giurisprudenza della Corte EDU (v. O. POLLICINO, 2014).

A tal proposito, nella sentenza *Leander c. Svezia* (Corte europea dei diritti dell'uomo, 26 marzo 1987, n. 9248/81, *Leander c. Svezia*, par. 48), la Corte EDU si è confrontata per la prima volta con la necessità di includere nel diritto al rispetto della vita privata anche l'ulteriore connotazione della protezione dei dati personali. In particolare, la Corte ha stabilito che la raccolta e il trattamento di dati personali ad opera delle autorità di polizia svedesi dovesse ricadere all'interno della disciplina prevista dall'art. 8, par. 1 CEDU.

Tale ricostruzione, avvenuta, per il vero, solo in via apodittica, ha ricevuto una più compiuta spiegazione solo in successive pronunce. Innanzitutto, la Corte ha precisato che la nozione di vita privata di cui all'art. 8, par. 1 CEDU non è suscettibile di una definizione esaustiva, ma deve essere intesa in senso

ampio, potendo «abbracciare molteplici aspetti dell'identità fisica e sociale della persona», tra cui le sue informazioni personali (Corte europea dei diritti dell'uomo, 16 dicembre 1992, n. 13710/88, *Niemietz c. Germania*, par. 29). Con la successiva sentenza *Amann c. Svizzera*, i giudici di Strasburgo hanno stabilito che in tale nozione estesa di vita privata rientrano anche le informazioni oggetto di elaborazione automatizzata e, richiamando esplicitamente la Convenzione n. 108, hanno stabilito che il trattamento dei dati personali è tutelato dall'art. 8, par. 1, CEDU (Corte europea dei diritti dell'uomo, 16 febbraio 2000, n. 27798/95, *Amann c. Svizzera*, par. 65). In altri termini, la Corte EDU, attraverso l'adeguamento della nozione di vita privata al contesto tecnologico e attraverso il riferimento alla Convenzione n. 108, ha stabilito che le informazioni non rappresentano più solo una componente statica della sfera privata, dal cui ambito è lecito escludere i terzi, a norma dell'art. 8, par. 2. Tali informazioni, quando si trovano sotto forma di dati, costituiscono piuttosto un parametro fondamentale di un'attività dinamica, ovvero il trattamento dei dati, per mezzo del quale è possibile arrecare un pregiudizio alle ragioni soggettive dell'individuo, meritevoli della tutela specifica consacrata nella disciplina sulla protezione dei dati personali.

Peraltro, la giurisprudenza della Corte EDU si è costantemente richiamata alla Convenzione n. 108 e, in tal modo, ha arricchito di contenuti la protezione dei dati personali, estendendone nel contempo la portata applicativa.

Ad esempio, nella sentenza *Gaskin c. Regno Unito*, la Corte EDU si è soffermata sul bilanciamento tra il diritto di accesso ai dati personali, introdotto dalla Convenzione, e la realizzazione di un interesse pubblico. La fattispecie riguardava il diniego opposto dal Regno Unito alla richiesta di un cittadino di accedere al fascicolo contenente tutte le informazioni raccolte dai servizi pubblici di assistenza all'infanzia, che lo riguardavano (tra cui, le condizioni in cui era vissuto e gli eventuali abusi a cui era stato sottoposto). Secondo i giudici di Strasburgo, tale diniego risultava sproporzionato, poiché dipendeva dal consenso di tutte le persone che avevano contribuito a stilare detto fascicolo, e, pertanto, comportava una violazione di un «vital interest» del ricorrente, protetto dalla Convenzione n. 108 e consacrato dall'art. 8, par. 1 CEDU (Corte europea dei diritti dell'uomo, 7 luglio 1989, n. 10454/1983, *Gaskin c. Regno Unito*, par. 49).

Di nuovo, la Corte EDU, riprendendo la categoria dei dati sensibili di cui al citato art. 6 della Convenzione, ha sostenuto che la particolare sensibilità dei dati riguardanti lo stato di salute dell'individuo richiede, al fine del loro trattamento, oneri di protezione e sicurezza più marcati. In particolare, tali oneri ricorrono quando sia necessario tutelare la riservatezza di informazioni relative alle patologie di cui è affetto un paziente, in quanto la loro divulgazio-

ne può ripercuotersi significativamente sulla sua vita privata, sociale e professionale, esponendolo allo stigma e al rischio di esclusione da parte dei consociati (Corte europea dei diritti dell'uomo, 25 febbraio 1997, n. 22009/1993, *Z. c. Finlandia*, par. 96).

Infine, con la sentenza *Rotaru*, la Corte EDU si è pronunciata sul diritto di rettifica. Nel caso di specie, il ricorrente lamentava una violazione del suo diritto alla vita privata in ragione della detenzione e dell'utilizzo, da parte del servizio di *intelligence* romeno, di un file contenente i suoi dati personali, dallo stesso ritenuti falsi. A tal proposito, la Corte EDU, richiamando espressamente la Convenzione n. 108, ha stabilito il divieto di trattamento di dati personali falsi o diffamatori, nonché il diritto dell'interessato a contestarne la fondatezza (Corte europea dei diritti dell'uomo, 4 maggio 2000, n. 28341/1995, *Rotaru c. Romania*, parr. 43 e ss.).

Tali riferimenti della Corte EDU alla Convenzione trovano la propria spiegazione soprattutto nell'opera di costante aggiornamento a cui quest'ultima, a differenza della CEDU, è stata sottoposta. A tal proposito, al fine di adeguare gradualmente i principi e le norme previste dalla Convenzione n. 108 alle continue innovazioni tecnologiche, il Comitato dei Ministri del Consiglio d'Europa ha adottato diversi atti che hanno rivestito un ruolo centrale per lo sviluppo del diritto in materia di protezione dei dati. Si tratta della raccomandazione relativa all'uso dei dati personali nell'ambito della pubblica sicurezza, i cui principi sui mezzi di conservazione dei data-set e sulla necessità di individuare a priori le persone autorizzate ad accedere a tali data-set hanno rappresentato il principale strumento di orientamento nell'ambito dei controlli effettuati dalle autorità di polizia (Consiglio d'Europa, raccomandazione n. 15, 1987); del Protocollo addizionale alla Convenzione n. 108, che introduce disposizioni in materia di flussi transfrontalieri dei dati verso le parti non contraenti, i c.d. paesi terzi (Consiglio d'Europa, protocollo STCE n. 181, 2001); e, infine, del protocollo addizionale che ha adeguato le tutele offerte dalla Convenzione al settore digitale (Consiglio d'Europa, protocollo STCE n. 223, 2018). Tali continui aggiornamenti del quadro giuridico della Convenzione ne hanno fatto un punto di riferimento non solo per la Corte EDU, bensì anche per il diritto dell'Unione Europea.

3.2. Il processo di affermazione della protezione dei dati personali nel contesto del diritto dell'Unione Europea

L'*acquis communautaire* in materia di protezione dei dati personali si caratterizza per un processo di sviluppo peculiare.

La disciplina sulla protezione dei dati, infatti, ha avuto origine con un atto di diritto derivato, ossia la Direttiva 96/45/CE, per poi evolversi grazie all'apporto della giurisprudenza della Corte di giustizia, fondata sulle tradizioni costituzionali comuni agli Stati membri, sulla Convenzione n. 108 e sulle indicazioni provenienti dalla Corte EDU. La disciplina in questione, quindi, si è consolidata nel diritto primario, segnatamente, nella Carta dei diritti fondamentali e nel Trattato di Lisbona, e, infine, è stata oggetto di un marcato aggiornamento con l'adozione del Regolamento (UE) 679/2016, ossia di nuovo con un atto di diritto derivato.

Tale processo di sviluppo, dall'aspetto «circolare», può essere idealmente suddiviso in quattro fasi principali, che meritano di essere approfondite singolarmente.

3.2.1. La prima fase: dai trattati di Roma alla Direttiva 96/45/CE

Nel periodo intercorrente tra la firma dei trattati di Roma e l'entrata in vigore del trattato di Lisbona, si registra un'evoluzione dell'approccio della Comunità europea in materia di tutela dei diritti fondamentali, attraverso la giurisprudenza della Corte di giustizia (G. TESAURO, 1992).

Già con la sentenza *Stauder* del 1969 (Sentenza della Corte di giustizia del 12 novembre 1969, ECLI:EU:C:1969:57), la Corte di giustizia si era fatta carico, in un contesto di primordiale integrazione politica degli ordinamenti nazionali, del compito di tutelare i diritti fondamentali della persona, in quanto parte dei principi generali del diritto, sia pure nei limiti della loro compatibilità con la struttura e le finalità della allora Comunità economica europea (F. BALDUCCI ROMANO, 2015). In questa risalente pronuncia, emerge l'obbligo per gli Stati membri di individuare, tra le possibili misure in grado di conseguire l'obiettivo prefissato, quelle meno pregiudizievoli per i diritti della persona, incluso il diritto al rispetto della vita privata – sebbene non ancora nella sua dimensione di protezione dei dati personali.

Infatti, tale pronuncia si inseriva in un contesto in cui la Comunità europea era priva di competenza in tale materia e, quindi, rimetteva l'effettiva protezione dei dati personali alle legislazioni che i singoli Stati membri avevano adottato in conseguenza della loro adesione alla Convenzione n. 108. Esemplari, in quest'ultimo senso, sono le legislazioni adottate dal Land tedesco dell'Assia nel 1970 (*Datenschutzbeauftragter*) e dalla Svezia nel 1973 (*Datalagen*), cui hanno fatto seguito quelle della Francia (*Loi relative à l'informatique, aux fichiers et aux libertés* del 1977), della Germania (*Bundesdatenschutsgesetz* del 1977), del Regno Unito (*Data Protection Act* del 1984) e dei Paesi Bassi (*Wet Persoonregistraties* del 1989).

Tuttavia, le discrepanze tra le legislazioni degli Stati membri in materia di

protezione dei dati personali contribuivano ad ostacolare la loro trasmissione fra i territori dell'UE. Di queste difficoltà ne risentivano, *in primis*, gli operatori economici del settore delle Tecnologie dell'Informazione e della Comunicazione (ICT), le cui attività era strettamente correlate all'utilizzo dei dati, ma, a livello più generale e considerata la pervasività dell'utilizzo dei dati in molti comparti produttivi, anche i meccanismi di funzionamento dello stesso mercato unico. Pertanto, era emersa la necessità – già richiamata nella risoluzione del Parlamento europeo sulla tutela dei diritti dei cittadini di fronte al crescente progresso tecnologico nel settore dell'informatica (in *GUCE* C 60 del 13 marzo 1975, p. 49) – di apprestare un'armonizzazione delle discipline nazionali sulla protezione dei dati personali per garantire anche lo sviluppo del mercato unico. Alla luce di tale interdipendenza, non stupisce che il primo atto in materia di protezione dei dati personali, la Direttiva 95/46/CE (in *GUCE* L 281 del 23 novembre 1995, p. 31), sia stato fondato sull'art. 100 A del TCE (oggi art. 114 TFUE), che consentiva l'adozione di misure di ravvicinamento delle normative degli Stati membri per garantire l'unificazione del mercato unico. E, in questa chiave, deve leggersi anche l'obiettivo principale della direttiva che, esplicitato fin dal suo stesso titolo, consisteva nel garantire un giusto equilibrio fra un livello elevato di tutela della vita privata delle persone e la libera circolazione dei dati personali all'interno dell'Unione Europea.

Nello specifico, la direttiva ha ripreso dalla Convenzione n. 108 e dalla seguente giurisprudenza della Corte EDU la concezione della protezione dei dati come corollario del diritto al rispetto della vita privata (art. 1, par. 1) e ha individuato nel trattamento dei dati il fulcro della normativa (art. 3, par. 1). Per contro, rispetto a dette precedenti fonti, la direttiva si caratterizza per un più ampio e completo quadro di norme, soprattutto dal carattere definitorio. Si fa riferimento, anzitutto, alle definizioni riferite ai soggetti coinvolti nel trattamento dei dati, come, ad esempio, quella di «interessato» – ossia la persona fisica (sono escluse, invece, le persone giuridiche) identificabile attraverso il trattamento dei suoi dati personali (art. 2, lett. a) – e quelle di «responsabile del trattamento» e di «incaricato del trattamento». In particolare, si evidenzia come questi soggetti non si distinguano per una caratterizzazione formale, posto che entrambi possono essere persona fisica o giuridica, autorità pubblica, servizio o qualsiasi altro organismo, ma in base all'attività svolta: mentre il responsabile determina le finalità e gli strumenti del trattamento di dati personali, l'incaricato si limita ad elaborare i dati personali per conto del primo (art. 2, lett. d) ed e).

Anche il sistema di tutele previste in favore dell'interessato risulta maggiormente articolato. Oltre ai principi di qualità dei dati, già previsti dalla Convenzione, la direttiva specifica, altresì, le basi giuridiche su cui deve essere

fondato il trattamento. Infatti, l'art. 7 della direttiva dispone che il trattamento dei dati è lecito soltanto qualora ricorra una delle seguenti condizioni: il consenso prestato dall'interessato in maniera inequivocabile; l'esecuzione del contratto concluso con l'interessato; l'adempimento di un obbligo legale al quale è soggetto il responsabile del trattamento; la salvaguardia di un interesse vitale dell'interessato; l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; il perseguimento dell'interesse legittimo del responsabile del trattamento.

Nella stessa logica, la direttiva conferisce all'interessato un ampio ventaglio di diritti, tra cui, in particolare, il diritto ad ottenere dal responsabile del trattamento le informazioni riguardanti i suoi dati personali oggetto di trattamento (art. 11), il diritto di accedere a tali dati (art. 12, lett. a), il diritto di opposizione, per ragioni legittime, ai trattamenti di dati (art. 14) e il diritto a non essere sottoposto ad una decisione fondata esclusivamente su un trattamento automatizzato di dati, volto a valutare taluni aspetti della personalità dell'interessato, quali il rendimento professionale, l'affidabilità creditizia, il comportamento nella vita quotidiana, ecc. (art. 15).

Inoltre, la direttiva ha disposto l'obbligo, per ciascuno Stato membro, di dotarsi di una o più autorità pubbliche indipendenti, incaricate di sorvegliare l'applicazione delle disposizioni di attuazione della direttiva stessa (art. 28). Peraltro, quest'ultima disposizione, nella prospettiva di costante influenza reciproca tra gli ordinamenti comunitario e internazionale, è stata successivamente prevista anche dagli artt. 1 e 15, par. 5 del citato Protocollo addizionale alla Convenzione n. 108, del 2001.

A dette autorità si affianca il c.d. Gruppo dell'Art. 29, così denominato per via della sua istituzione a norma dell'art. 29 della direttiva. Tale gruppo è organo consultivo e indipendente composto da un rappresentante non solo di ciascuna autorità di protezione dei dati nazionali, ma anche dell'*istituendo* Garante europeo della protezione dei dati (istituito dal Regolamento (CE) 45/2001, in *GUUE* L 8 del 12 gennaio 2001, p. 1) e della Commissione europea.

Orbene, la direttiva ha rappresentato, a livello comunitario, il primo intervento di diritto positivo in materia di protezione dei dati personali. Tuttavia, essa si è dovuta confrontare con i limiti connessi alla sua natura di atto di diritto derivato che, conformemente all'ordinamento giuridico dell'UE, non trova applicazione diretta negli ordinamenti degli Stati membri. Come osservato a più riprese dalla Corte di giustizia dell'Unione Europea, nonostante l'intento della direttiva – come meglio specificato nei *consideranda* nn. 8 e 10 – fosse di prevedere un'armonizzazione completa, essa è stata recepita in modo diverso nei vari Stati membri, soprattutto con riferimento ai principi dettati dalla direttiva (Corte di giustizia UE, sentenza 6 novembre 2003, C-101/01, ECLI:EU:C:2003:596,

punti 95 e ss.; Corte di giustizia UE, sentenza 16 dicembre 2008, C-524/06, ECLI:EU:C:2008:724, punto 50).

A tal proposito, la Corte di giustizia ha stabilito che l'obiettivo consistente nel garantire un livello di protezione equivalente in tutti gli Stati membri reca con sé la necessità che il citato art. 7 della Direttiva 95/46/CE sia interpretato quale elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito. Ne consegue che gli Stati membri non possono «né aggiungere nuovi principi relativi alla legittimazione del trattamento dei dati personali, né prevedere requisiti supplementari che vengano a modificare la portata di tali principi» (Corte di giustizia UE, sentenza 24 novembre 2011, cause riunite C-468/10 e C-469/10, ECLI:EU:C:2011:777, punto 32, e giurisprudenza ivi richiamata).

Nonostante i numerosi interventi della Corte di giustizia UE, nella pratica, l'adozione delle diverse legislazioni nazionali di recepimento, rese ancora più lontane tra loro dai differenti approcci interpretativi dei giudici nazionali, hanno causato un'applicazione disomogenea delle disposizioni e dei principi della direttiva.

Un ulteriore limite connaturato alla direttiva riguardava il suo ristretto ambito di applicazione materiale. Infatti, come è noto, a far data dall'entrata in vigore del trattato del trattato di Maastricht 1° novembre 1993, e sino all'applicazione del trattato di Lisbona il 1° dicembre 2009, l'ordinamento giuridico dell'Unione Europea era basato su tre pilastri. Sulla base di tale presupposto, l'art. 3, par. 2 della direttiva, in conformità all'art. 100 A TCE, ne ha limitato il campo di applicazione alle sole materie incluse nel primo pilastro, restando quindi esclusi i trattamenti «effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario», quali la pubblica sicurezza, la difesa e la sicurezza dello Stato.

3.2.2. La seconda fase: la Carta UE e l'autonomia del diritto alla protezione dei dati personali

Stante i suddetti limiti della Direttiva 96/45/CE, la Comunità europea ha sottoposto la disciplina sulla privacy ad un processo di evoluzione, di cui la proclamazione della Carta UE costituisce un elemento imprescindibile (F. DONATI, 2001, p. 83).

La Carta UE, al fine di «rafforzare la tutela dei diritti fondamentali, alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici», ha espressamente riconosciuto, insieme al tradizionale diritto alla tutela della vita privata di cui all'art. 7, anche il «diritto alla protezione dei dati di carattere personale», così rubricato dall'art. 8.

I due diritti si distinguono in termini di contenuto, portata e formulazione (Corte di giustizia UE, conclusioni dell'avvocato generale *Sharpston* 17 giugno 2010, cause riunite C-92/09 e C-93/02, ECLI:EU:C:2010:353, punto 71).

In termini di contenuto, mentre il diritto al rispetto della vita privata, di matrice tradizionale e passiva, vieta le interferenze di terzi nella sfera personale del singolo, tranne nei casi prestabiliti di interesse pubblico, la protezione dei dati personali è vista come un diritto moderno e attivo, che instaura un sistema di controlli ed equilibri, volti a proteggere le persone fisiche ogniqualvolta siano trattati i loro dati personali, con esclusione dei soli casi in cui si esuli dal campo di applicazione del diritto UE, ovvero si versi in situazioni che ricadono sotto la competenza esclusiva degli Stati membri.

Per quanto attiene, invece, al campo di applicazione, la tutela offerta dal diritto al rispetto della vita privata si estende alle sole situazioni in cui tale vita privata sia stata effettivamente compromessa. Pertanto, nonostante la Corte di giustizia, sulla scorta degli orientamenti giurisprudenziali della Corte EDU, abbia inteso la nozione di vita privata in senso ampio, la valutazione circa l'esistenza o meno di un'ingerenza nella vita privata dipende dal contesto e dalle circostanze di ciascun caso. Per contro, il diritto alla protezione dei dati personali ha un campo di applicazione più esteso, in quanto trova applicazione per il solo fatto che un qualunque dato personale – compresi quelli di dominio pubblico e non incidenti sulla sfera intima dell'individuo –, sia stato oggetto di trattamento (Corte di giustizia UE, sentenza 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01, *Österreichischer Rundfunk e al.*, ECLI:EU:C:2003:294). In altri termini, tutte le operazioni di trattamento dei dati personali sono soggette a una protezione adeguata, indipendentemente dal loro impatto sulla vita privata. Pertanto, se è ben possibile che il trattamento dei dati personali possa pregiudicare anche il diritto al rispetto della vita privata, tuttavia, non è necessario dimostrare una siffatta violazione affinché siano applicabili le norme sulla protezione dei dati personali.

Infine, a differenza dello scarno contenuto dell'art. 7, l'art. 8 non si limita a sancire il diritto alla protezione dei dati personali, ma ne enuncia anche i corollari fondamentali, che, mutuati dagli artt. 6, 7, 12, 14 e 28 della Direttiva 95/46/CE, prevedono i principi che regolano il trattamento dei dati ed i diritti ad esso connessi, spettanti all'interessato (art. 8, par. 2), nonché il controllo di un'autorità indipendente (art. 8, par. 3).

La codificazione, a mezzo della Carta UE, del diritto alla protezione dei dati personali ha avuto due conseguenze principali.

In primo luogo, come evidenziato dalla Commissione europea, essa «ha messo maggiormente in luce l'angolazione della Direttiva 96/45/CE sotto il profilo del rispetto dei diritti fondamentali» (COM(2003) 265), e ciò, nono-

stante la Carta UE fosse inizialmente priva di valore giuridico vincolante. A tal proposito, infatti, la giurisprudenza della Corte di giustizia, sulla base dell'art. 8 della Carta UE, ha interpretato le disposizioni di tale direttiva secondo un approccio teleologico, orientato a valorizzarne il rispetto dei diritti fondamentali in luogo delle contrastanti libertà economiche (Corte di giustizia UE, sentenza 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01, ECLI:EU:C:2003:294; Corte di giustizia UE, sentenza 6 novembre 2003, causa C-101/01, ECLI:EU:C:2003:596). Ne è conseguito un ridimensionamento della dimensione «mercantilistica» della direttiva, in ragione di una maggiore attenzione per i diritti delle persone fisiche sottoposte al trattamento dei dati personali.

In secondo luogo, la suddetta codificazione ha dato avvio al processo di autonomizzazione del diritto alla protezione dei dati personali rispetto alla tutela della vita privata.

In realtà, tale processo ha inizialmente faticato ad emergere, tanto a livello giurisprudenziale, quanto a livello normativo.

Esemplari, in questo senso, sono state la sentenza *Promusicae* della Corte di giustizia, in cui è stata affermata l'esistenza di un nuovo diritto fondamentale, a tutela dei dati personali «e, quindi, della vita privata» (Corte di giustizia UE, sentenza 29 gennaio 2008, causa C-275/06, ECLI:EU:C:2008:54) e la decisione quadro 2008/977/GAI (in *GUUE* L 350 del 30 dicembre 2008, p. 60) che, pur dettando la disciplina sulla protezione dei dati personali limitatamente all'ambito della cooperazione giudiziaria e di polizia in materia penale, non manca di precisare, al considerando n. 48, che essa garantisce, oltre al diritto alla protezione dei dati di carattere personale di cui all'art. 8 della Carta UE, anche «il pieno rispetto del diritto alla tutela della vita privata di cui all'art. 7 della Carta».

Pertanto, così come già osservato in merito alla giurisprudenza CEDU, alla Convenzione n. 108 e alla Direttiva 96/45/CE, i due diritti, quantomeno in questa fase, seppur previsti come fattispecie autonome e distinte, sono stati tuttavia interpretati come inscindibilmente connessi tra loro.

3.2.3. La terza fase: il Trattato di Lisbona e il bilanciamento tra diritti fondamentali

L'entrata in vigore del Trattato di Lisbona il 1° dicembre 2009 segna un ulteriore passo fondamentale per lo sviluppo della disciplina sulla protezione dei dati personali.

Innanzitutto, l'art. 6, par. 1 TUE, disponendo che «[l]'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a

Strasburgo, che ha lo stesso valore giuridico dei trattati», ha elevato lo *status* giuridico della Carta UE a diritto primario dell'UE. Ne consegue che i diritti contenuti nella Carta UE esplicano i propri effetti tanto nei confronti delle istituzioni, degli organismi e degli organi dell'UE nell'adempimento dei loro doveri, quanto verso gli Stati membri nell'attuazione del diritto dell'UE.

Per quanto riguarda l'art. 16, par. 2 TFUE, esso ha sostituito l'art. 286 TCE, ampliandone notevolmente la portata. Infatti, quest'ultima disposizione si limitava a prevedere l'applicabilità degli atti comunitari relativi al diritto alla protezione dei dati personali anche ai trattamenti di dati effettuati da istituzioni e organismi della Comunità. Diversamente l'art. 16, par. 2 TFUE attribuisce al legislatore europeo la facoltà di adottare, mediante procedura legislativa ordinaria, «una normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla loro libera circolazione da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, affidando il rispetto di tali norme ad autorità indipendenti». In altri termini, la base giuridica di cui all'art. 16, par. 2 TFUE ha sancito la nuova competenza dell'Unione Europea in materia di protezione dei dati personali; competenza che è specifica e, quindi, scevra dagli angusti confini della realizzazione del mercato interno che aveva contraddistinto la base giuridica della Direttiva 95/46/CE.

Infine, l'art. 16, par. 1 TFUE ha incluso il diritto alla protezione dei dati personali tra i principi fondamentali del diritto UE. In tal senso, il Trattato di Lisbona ha dato nuovo impulso al processo di autonomizzazione del diritto alla protezione dei dati personali, che si palesa nell'acquisita centralità di tale diritto nell'ambito delle operazioni di bilanciamento con gli altri diritti fondamentali.

A tal proposito, come stabilito dalla Corte di giustizia, la tutela dei dati personali, accordata al singolo, non costituisce una prerogativa assoluta, ma deve essere considerata alla luce della sua funzione sociale, economica e di pubblica sicurezza (Corte di giustizia UE, sentenza 9 novembre 2010, cause riunite C-92/09 e C-93/09, ECLI:EU:C:2010:662, punto 48). I dati personali rappresentano, infatti, una componente essenziale dell'identità di ciascun individuo, la cui tutela, pur dovendo essere preservata con ogni mezzo, deve comunque rispettare precisi confini, nell'ottica di una pacifica convivenza tra l'interesse privato e l'interesse pubblico in gioco. Talora questa tensione fra interessi contrapposti viene risolta dalla Corte, nel suo ruolo di «guardiana costituzionale» dell'ordinamento dell'Unione, a favore della centralità del diritto alla protezione dei dati personali, pur in presenza di opposte istanze securitarie, a seguito di un attento bilanciamento tra diritti fondamentali differenti (M. CARTABIA, 2018).

Il punto di partenza di siffatto bilanciamento è l'art. 52, par. 1 Carta UE, che richiama la menzionata formulazione dell'art. 8, par. 2 CEDU. In particolare, l'art. 52 stabilisce la legittimità delle limitazioni all'esercizio del diritto di cui all'art. 8, purché: 1) tali limitazioni siano previste dalla legge, 2) rispettino il suo contenuto essenziale e 3) il principio generale di proporzionalità, 4) siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'UE o all'esigenza di proteggere i diritti e le libertà altrui.

Pertanto, nel dare applicazione a detto art. 52, in prima battuta, è necessario accertare se la limitazione del diritto alla protezione dei dati personali sia prevista dalla legge. In particolare, tale legge, secondo la dottrina della c.d. «qualità della legge» elaborata dalla Corte EDU, deve essere sufficientemente chiara e prevedibile per quanto riguarda il significato e la natura delle misure applicabili, dovendo consentire al cittadino di immaginare le conseguenze della propria condotta (Corte di giustizia UE, conclusioni dell'Avvocato generale Villalón 14 aprile 2011, causa C-70/10, ECLI:EU:C:2013:781, punto 100).

In seconda battuta, si deve verificare se la limitazione apportata al diritto non ne pregiudichi il «contenuto essenziale». Come stabilito dalla Corte di giustizia, tale formula deve essere interpretata restrittivamente. Pertanto, anche qualora si fosse in presenza di un'ingerenza particolarmente grave dell'art. 8, quest'ultima, tuttavia, può non essere tale da pregiudicarne il contenuto essenziale (Corte di giustizia UE, sentenza 8 aprile 2014, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, punto 40; per quanto attiene al pregiudizio del contenuto essenziale del diritto al rispetto della vita privata v. Corte di giustizia UE, sentenza 6 ottobre 2015, causa C-362/14, ECLI:EU:C:2015:650, punto 94).

In terzo luogo, occorre valutare se le limitazioni siano adottate «nel rispetto del principio di proporzionalità». Viene, dunque, rimarcato il ruolo del principio di proporzionalità quale criterio in base al quale realizzare il bilanciamento del diritto alla protezione dei dati personali con gli altri diritti fondamentali parimenti tutelati dal diritto UE. Ad esempio, la Corte di giustizia, richiamando tale principio, ha affermato l'inapplicabilità di una normativa nazionale che stabilisca a priori ed in modo definitivo il risultato del bilanciamento dei diritti e degli interessi contrapposti, senza consentire un diverso risultato in ragione delle specifiche circostanze del caso concreto (Corte di giustizia UE, sentenza 24 novembre 2011, cause riunite C-468 e 469/10, ECLI:EU:C:2011:777, punto 47).

Infine, si deve valutare se le limitazioni apportate siano necessarie e rispondano effettivamente a «finalità di interesse generale riconosciute dall'Unione» o «all'esigenza di proteggere i diritti e le libertà altrui». Sotto quest'ultimo aspetto, il diritto alla protezione dei dati personali si è spesso scontrato con altre libertà, tra cui, in particolare, la libertà di espressione (Corte di giustizia UE, sentenza 16 dicembre 2008, causa C-73/07, ECLI:EU:C:2008:727, e sen-

tenza 16 febbraio 2012, causa C-360/10, ECLI:EU:C:2012:85). La libertà di espressione è sancita dall'art. 11 della Carta UE e si sostanzia nella duplice dimensione di diritto di divulgare le informazioni e diritto di accedervi. Il rapporto tra tale libertà e il diritto alla protezione dei dati personali deve essere valutato caso per caso tenendo conto di un insieme di parametri tra cui rileva, in particolare, la natura dell'informazione di cui trattasi. Alla luce di tale parametro, infatti, deve confrontarsi, da un lato, la sensibilità o l'attualità delle informazioni oggetto di divulgazione o di accesso in riferimento alla vita privata della persona cui si riferiscono, e, dall'altro lato, l'interesse pubblico alla disponibilità dell'informazione. A livello teorico, quindi, se le informazioni in questione si connotano per un elevato grado di sensibilità (come nel caso dei dati sensibili di cui all'art. 8 della Direttiva 95/46/CE) e per un'evidente obsolescenza delle stesse, la protezione dei dati personali dovrebbe prevalere sul diritto del pubblico generale di avere accesso all'informazione. Per contro, qualora risulti che l'interessato è una figura pubblica o che l'informazione non attiene ad aspetti sensibili della sua vita privata, oppure, ancora, che la stessa risulta essere attuale, allora il diritto fondamentale alla protezione dei dati dovrebbe arretrare di fronte all'interesse pubblico alla divulgazione di tale informazione.

Invece, per quanto attiene alle «finalità di interesse generale», come precisato nelle Spiegazioni allegate alla Carta, queste coincidono sia con gli obiettivi generali dell'UE sanciti dall'art. 3 TUE (la giustizia e la protezione sociale, e la creazione di uno spazio di libertà, sicurezza e giustizia in cui sia assicurata la libera circolazione delle persone), sia con gli altri interessi tutelati da disposizioni specifiche dei trattati (ad esempio, l'art. 4, par. 1 TUE e gli artt. 35, parr. 3, 36 e 346 TFUE). In tema, la sentenza probabilmente più nota è la pronuncia *Digital Rights Ireland* (Corte di giustizia UE, sentenza 8 aprile 2014, cause riunite C-293/12 e C-594/12, cit.), con la quale la Corte ha dichiarato invalida la Direttiva 2006/24/CE, c.d. direttiva «*data retention*», sulla conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione (in *GUUE* L 105 del 13 aprile 2006, p. 54). Tale direttiva, a giudizio della Corte, non prevedeva, come richiesto dagli artt. 7, 8 e 52 par. 1 della Carta UE, garanzie proporzionate ad assicurare una protezione efficace dei dati personali contro i rischi di utilizzi abusivi e di accessi illeciti da parte delle autorità pubbliche. Infatti, sebbene l'utilizzo di tali dati personali da parte delle autorità nazionali competenti poteva rispondere effettivamente a un obiettivo di interesse generale, ossia la pubblica sicurezza, al tempo stesso, tale pratica era sproporzionata rispetto alla necessità di garantire il rispetto del diritto alla protezione dei dati personali.

3.2.4. La quarta fase: la riforma della normativa in materia di protezione dei dati personali e il Regolamento Privacy

Le suddette modifiche a livello di diritto primario hanno imposto al legislatore europeo un complessivo ripensamento della disciplina sulla protezione dei dati personali.

Il «dopo Lisbona» è venuto a coincidere con il processo di revisione della Direttiva 95/46/CE, il quale, attivatosi con la consultazione pubblica del luglio 2009 (*Summary of replies to the public consultation about the future legal framework for protecting personal data*, Brussels, 4 November 2010), ha visto un primo segnale di svolta con il programma di Stoccolma 2010-14 (in *GUUE* C 115, 4 maggio 2010, p. 1).

Tale programma, infatti, si proponeva l'obiettivo di istituire «un'Europa fondata sui diritti fondamentali», così come sanciti dalla Carta UE e dalla CEDU, con particolare riferimento «ai diritti dei cittadini nella società dell'informazione», tra cui spiccava espressamente il diritto alla protezione dei dati personali. In particolare, il programma evidenziava la necessità di adottare una «strategia globale» in materia di protezione dei dati all'interno dell'Unione e nell'ambito delle relazioni con i paesi terzi.

Il tema della «globalità» della strategia ricorre, altresì, nella successiva Comunicazione della Commissione in materia di dati personali (COM(2010) 609, p. 3), ove si specifica che, per far fronte alle sfide poste dalla rapidità dell'evoluzione tecnologica – ormai compiutamente digitale –, nonché dalla globalizzazione, «l'UE deve mettere a punto un approccio globale generale e coerente onde garantire che il diritto fondamentale di ciascuno alla protezione dei dati personali sia pienamente rispettato all'interno e all'esterno dell'UE».

Sulla base di questi presupposti, la comunicazione ha tratteggiato le azioni che la Commissione stessa si impegnava a porre in essere, tra cui, nello specifico, la proposta di un atto legislativo per la revisione del quadro giuridico sulla protezione dei dati che fosse in grado di consolidare la posizione dell'UE nei confronti della protezione dei dati personali in tutte le politiche europee, comprese le attività di contrasto e la prevenzione della criminalità.

Tali indicazioni hanno confermato chiaramente l'intenzione dell'UE di superare definitivamente, anche con riferimento alla disciplina in materia di protezione dei dati, la struttura a pilastri che aveva caratterizzato la Direttiva 95/46/CE.

Peraltro, l'obiettivo di istituire un quadro giuridico globale in materia di protezione dei dati personali si incardinava nella nuova base giuridica introdotta dall'art. 16, par. 2 TFUE, che, come sottolineato dalla suddetta comunicazione, consentiva «di disporre di un unico strumento giuridico per discipli-

nare la protezione dei dati, e ciò anche nei settori della cooperazione di polizia e della cooperazione giudiziaria in materia penale».

Ciononostante, il 25 gennaio 2012, la Commissione europea ha adottato la proposta di riforma della normativa in materia di protezione dei dati personali, detta anche «*data protection package*», costituita, in tale fase, dalla Proposta di Regolamento concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (COM(2012) 11), e dalla Proposta di Direttiva concernente la tutela 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, e la libera circolazione di tali dati (COM(2012) 10).

La scelta di questo doppio canale ha rappresentato un compromesso tra il suddetto obiettivo di realizzare un quadro «globale» di protezione dei dati personali e l'esigenza di tenere debitamente in conto della situazione concreta in cui avrebbe trovato applicazione la nuova disciplina.

Infatti, l'azione della direttiva del 1995 aveva prodotto, in relazione al proprio campo di applicazione – il primo pilastro –, un'armonizzazione tra i sistemi nazionali, che, seppur con i limiti evidenziati, aveva gettato le fondamenta di una normativa unica per tutta l'Unione, nella forma del regolamento. Per contro, tale armonizzazione non si era verificata all'interno del terzo pilastro, relativamente al quale la citata decisione quadro 2008/977/GAI non era stata in grado di ridurre le distanze tra gli ordinamenti nazionali. Come evidenziato dalla Commissione europea nella Relazione di accompagnamento alla suddetta proposta di direttiva, «la decisione quadro 2008/977/GAI [aveva] un campo di applicazione limitato, in quanto si applica[va] solo al trattamento transfrontaliero dei dati e non alle attività di trattamento effettuate dalla polizia e dalle autorità giudiziarie a livello strettamente nazionale. (…) Inoltre, per sua natura e contenuto, la decisione quadro lascia[va] un ampio margine di manovra alle legislazioni nazionali degli Stati membri nell'attuazione delle sue disposizioni».

D'altra parte, già la Dichiarazione n. 21, allegata all'atto finale della conferenza intergovernativa che ha adottato il Trattato di Lisbona (in *GUUE* C 326 del 26 ottobre 2012, p. 337), aveva esplicitato che la specificità del settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia avrebbe potuto richiedere l'adozione di «norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati».

Suddette proposte normative sono state sottoposte ad un processo di approvazione piuttosto lungo (oltre quattro anni), che ha visto l'intervento di numerosi organi dell'UE: il Comitato delle Regioni e il Comitato economico e sociale europeo, i quali si sono espressi favorevolmente in merito alle propo-

ste; il Garante europeo della protezione dei dati, il cui parere (2012/C 192/05) non ha fatto mancare alcuni rilievi critici in ordine alla direttiva, giudicata uno «strumento giuridico autonomo che forni[va] un livello di protezione inadeguato, di gran lunga inferiore a quello della proposta di regolamento»; e, infine, il Gruppo dell'Art. 29, il quale se, da un lato, ha accolto positivamente «un testo che riflett[eva] l'accresciuta importanza della protezione dei dati nell'ordinamento giuridico dell'Unione europea», tuttavia, dall'altro lato, non ha fatto mancare critiche alla scelta della Commissione – dettata da «motivi politici» – di presentare una proposta di direttiva distinta per quanto riguarda il settore della polizia e della giustizia penale (Parere 01/2012 del 23 marzo 2012 – WP 191 sulle proposte di riforma in materia di protezione dei dati).

A conclusione di questo lungo e complesso *iter* legislativo, sono stati emanati il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che ha abrogato la Direttiva 95/46/CE (in *GUUE* L 119 del 4 maggio 2016, p. 1), e la Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che ha abrogato la decisione quadro 2008/977/GAI (in *GUUE* L 119 del 4 maggio 2016, p. 89).

In seguito, il *data protection package* è stato completato con l'adozione di due ulteriori misure.

In primo luogo, il Regolamento (UE) 2018/1725, che ha esteso le regole previste dal Regolamento (UE) 2016/679 e dalla Direttiva (UE) 2016/680 ai trattamenti di dati personali effettuati dalle istituzioni, organi, uffici e agenzie dell'UE (in *GUUE* L 259 del 21 novembre 2018, p. 39). Sulla base di tale regolamento, inoltre, con decisione del 15 maggio 2020, il Garante europeo della protezione dei dati ha adottato il proprio regolamento interno (in *GUUE* L 204 del 26 giugno 2020, p. 49).

In secondo luogo, posto che la strategia per il mercato unico digitale aveva prefissato il riesame della Direttiva 2002/58/CE relativa alla vita privata nell'ambito delle comunicazioni elettroniche, la Commissione europea ha adottato la proposta di regolamento c.d. "*e-privacy*", che garantisce il rispetto della vita privata, la riservatezza delle comunicazioni e la tutela dei dati a carattere personale nel settore delle comunicazioni elettroniche, in coerenza tanto con il già visto nuovo Codice delle comunicazioni elettroniche, quanto con il Regolamento 2016/679/UE (COM(2017) 10).

4. Il Regolamento 2016/679/UE

4.1. Un inquadramento generale della nuova disciplina dell'Unione Europea in materia di privacy

Il Regolamento 2016/679/UE (di seguito anche solo "il Regolamento") ha dunque abrogato la Direttiva 95/46/CE e, a norma del suo art. 99, è divenuto applicabile in tutti i 28 (oggi 27) Stati membri dell'Unione Europea, a decorrere dal 25 maggio 2018.

Esso, come anticipato, si fonda sull'art. 16, par. 2 TFUE, che conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati.

Il Regolamento, dopo il consueto preambolo esplicativo – per il vero molto esteso, consistendo in ben 173 *considerande*, imprescindibili ai fini ermeneutici – si struttura in 11 Capi, composti da 99 articoli, numeri che, assai più elevati rispetto ai 34 articoli della precedente Direttiva 95/46/CE, segnano il diverso e maggiore peso affidato dal legislatore dell'UE alla normativa in materia di protezione dei dati personali.

Coerente con tale impostazione è anche la forma dell'atto normativo adottato: il regolamento, in luogo della direttiva. Come è noto, tra gli atti di diritto derivato dell'Unione Europea, a norma dell'art. 288 TFUE, il regolamento ha portata generale ed è obbligatorio e direttamente applicabile, in tutti i suoi elementi, in ciascuno degli Stati membri. Per il legislatore europeo, quindi, tale tipologia di atto rappresenta lo strumento idoneo a fornire un quadro giuridico solido e coerente che assicuri, in tutta l'Unione, l'applicazione "omogenea" delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali (*considerande* nn. da 7 a 10), anche grazie a poteri di controllo e sanzionatori «equivalenti» in tutti gli Stati membri, nonché alla cooperazione efficace tra le preposte autorità nazionali (*considerande* nn. da 10 a 13).

Insomma, uno strumento normativo in grado di superare l'insoddisfacente risultato conseguito dalla direttiva, che non aveva impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione (*considerando* n. 9).

Comunque, se già la forma del Regolamento costituisce, nel contesto della disciplina sulla privacy, una prima novità di rilievo, essa non è di certo l'unica.

Infatti, per quanto il Regolamento riprenda, quasi letteralmente, alcune disposizioni della direttiva (per citarne solo alcune, l'oggetto e le finalità di cui all'art. 1, l'ambito di applicazione materiale di cui all'art. 2 e l'impianto dei

principi sul trattamento dei dati di cui all'art. 7 e ss.), e operi alcune modifiche soltanto di carattere «estetico» al precedente testo normativo (ad esempio, il responsabile e l'incaricato del trattamento che, nel nuovo testo legislativo, sono stati rispettivamente sostituiti, solo nel nome, dal titolare e dal responsabile del trattamento), esso ha il merito di aver introdotto alcune novità che hanno profondamente mutato l'intera disciplina. Ciò sarebbe dimostrato, peraltro, dal periodo di transizione di due anni concesso agli Stati membri e alle parti interessate per prepararsi adeguatamente all'adozione del nuovo quadro giuridico, con uno sforzo solo in parte mediato dai successivi interventi chiarificatori della Commissione europea (quali le due comunicazioni sull'applicazione del Regolamento nell'UE (COM(2018) 43) e (COM(2019) 374)) e del neonato Comitato europeo per la protezione dei dati che, a norma degli artt. 68 e ss. del Regolamento, ha sostituito il Gruppo Art. 29 nei suoi compiti consultivi.

Nello specifico, tra le principali novità introdotte dal Regolamento possono annoverarsi, senza pretesa di esaustività, un impianto definitorio modernizzato e arricchito, per esempio, con le fattispecie dei dati sensibili genetici e biometrici (art. 4, nn. 13 e 14) e con specifiche previsioni sulle tecniche di profilazione – di cui si dirà meglio in seguito.

Inoltre, il Regolamento ha esteso, in termini sia di qualità, che di quantità, la categoria dei diritti accordati all'interessato. Sotto il profilo qualitativo, il Capo III, rubricato «Diritti dell'interessato», ha conferito dignità di singoli diritti a disposizioni che nella Direttiva 95/46/CE erano concentrate in poche ed eterogenee norme. A tal proposito, ai diritti di informazione (art. 14) e di accesso (art. 15), si affiancano ora le singole fattispecie dei diritti di rettifica dei dati (art. 16), di limitazione del trattamento (art. 18) e di opposizione ad un processo decisionale automatizzato (art. 21). Invece, per quanto attiene al profilo quantitativo, il Regolamento ha introdotto i nuovi diritti in materia di cancellazione dei dati (art. 17), portabilità dei dati (art. 20), reclamo ad un'Autorità di controllo (art. 77), ricorso giurisdizionale effettivo contro le decisioni assunte da un'autorità di controllo (art. 78), oppure contro il titolare del trattamento o il responsabile del trattamento (art. 79).

Costituiscono una novità anche le norme relative alla gestione del rischio in base al «principio di responsabilizzazione» del titolare del trattamento (c.d. "*accountability*"). Con tale espressione si intende l'obbligo per il titolare del trattamento di adottare una serie di misure tecniche ed organizzative, adeguate a garantire i principi di protezione dei dati, sulla base di una valutazione che tenga conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. Dunque, il Regolamento, in molti casi specifici, non effettua la scelta sul tipo di misure da adottare, ma ne rimette, per l'appunto,

la responsabilità al titolare del trattamento, che è chiamato a formulare una valutazione preventiva, sulla quale fondare la propria condotta (*ex multis*, artt. 24, 25, 35).

Rispetto alla precedente disciplina, il Regolamento dedica ampio spazio al consenso, declinato tanto in termini generali, quanto in riferimento a fattispecie particolari.

Sotto il primo aspetto, il Regolamento definisce il consenso dell'interessato come «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*» (art. 4, n. 11). Tale consenso può costituire la base legittima di un trattamento dei dati, solo se all'interessato sia stata offerta l'effettiva possibilità di scelta se accettare o meno i termini proposti o rifiutarli senza subire pregiudizio. In caso contrario, il consenso non può costituire una base valida per il trattamento, rendendo illecita l'attività di trattamento (art. 7).

Per quanto riguarda il secondo aspetto, le fattispecie particolari riguardano il consenso al trattamento di dati personali prestato dal minore, che è lecito solo ove lo stesso abbia almeno 16 anni (art. 8), e il consenso prestato in riferimento al trattamento dei dati personali relativi alle condanne penali e ai reati, o a connesse misure di sicurezza, che deve avvenire soltanto sotto il controllo dell'autorità pubblica (art. 10).

Occupano un posto di rilievo anche le nuove disposizioni relative alle Autorità di controllo indipendenti. Al Capo VI (artt. 51-59) sono fissati i requisiti di indipendenza, le competenze, i compiti e i poteri. In particolare, il Regolamento dota le autorità di controllo di rilevanti poteri sanzionatori, fondati su sanzioni amministrative pecuniarie e altre misure di tipo correttivo rimesse alla discrezione delle autorità stesse.

Le suddette novità – e quelle che saranno qui di seguito approfondite –, per quanto differenti tra di loro, possono essere osservate da una medesima prospettiva, che presuppone un adeguamento della disciplina europea sulla privacy, nella sua accezione di diritto alla protezione dei dati personali, al mutato contesto tecnologico degli ultimi vent'anni. In altre parole, il Regolamento costituisce l'ultimo stadio di quel processo di evoluzione del concetto di *privacy* che, come visto inizialmente, è stato reso impellente dall'affermazione della società dell'informazione. A tal proposito, esso trova la propria ragione nel necessario confronto con le nuove sfide per la protezione dei dati personali decretate dalla rapidità dell'evoluzione tecnologica a livello globale, tra cui il considerevole aumento dei flussi transfrontalieri di dati personali all'interno dell'ormai funzionante mercato unico digitale, e l'utilizzo senza prece-

denti di tali dati da parte delle imprese private e delle autorità pubbliche (*considerand*a nn. 5 e 6). In questa stessa logica può leggersi anche l'art. 97, par. 5 del Regolamento, che incarica la Commissione europea di presentare «opportune proposte di modifica del presente regolamento tenuto conto, in particolare, degli sviluppi delle tecnologie dell'informazione e dei progressi della società dell'informazione». Infine, deve altresì sottolinearsi che il Regolamento conclude quel percorso di autonomizzazione del diritto alla protezione dei dati personali, che, iniziato con l'art. 8 della Carta Ue e poi proseguito con l'art. 16 par. 2 TFUE, è qui testimoniato dall'assenza di qualsivoglia richiamo al diverso diritto al rispetto della vita privata, il quale, diversamente, aveva sempre accompagnato, nella costruzione della disciplina sulla privacy europea, l'evoluzione del diritto alla protezione dei dati personali.

4.2. Le principali novità introdotte dal Regolamento (UE) 679/2016

4.2.1. L'estensione della nozione di dato personale

Il regolamento trova applicazione con riferimento esclusivo al trattamento dei dati personali. L'art. 4, par. 1 del Regolamento definisce i dati personali come «qualsiasi informazione riguardante una persona fisica identificata o identificabile (…)», con l'ulteriore specificazione che «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

Per contro, a norma degli artt. 2 e 3 del menzionato Regolamento (UE) n. 2018/1807 (par. 2.3), tutti i dati che non ricadono in tale categoria sono definiti dati non personali. Possono dunque definirsi tali i dati anonimi (quali, ad esempio, le informazioni di natura meteorologica, geografica, macroeconomica, sociale, ecc.) e quei dati personali che, sottoposti a processi di anonimizzazione, sono privati dei riferimenti alla persona fisica sottoposta al relativo trattamento.

I confini tra tali categorie, seppur rigorosamente marcati a livello teorico, risultano in concreto più sfumati.

Infatti, l'utilizzo di tecniche di re-identificazione, che consentono, attraverso la consultazione incrociata di vasti e numerosi archivi digitali, di inferire le informazioni su un individuo da dati non personali, rende particolarmente controversa l'aprioristica collocazione dei dati nelle suddette categorie giuridiche di appartenenza.

Il profilo della re-identificazione era già stato oggetto dell'attenzione del Gruppo Art. 29 (Parere 4/2007 del 20 giugno 2007 – WP 136 sul concetto di dati personali e Parere 06/2013 del 5 giugno 2013 – WP 207 sui dati aperti e sul riutilizzo delle informazioni del settore pubblico) e dello scrutinio della Corte di giustizia (Corte di giustizia UE, sentenza 19 ottobre 2016, causa C-582/14, ECLI:EU:C:2016:779), secondo cui l'art. 2, lett. a), della Direttiva 95/46/CE sulla definizione di dato personale, doveva essere interpretato nel senso che un indirizzo di protocollo Internet (indirizzo IP) dinamico, registrato da un fornitore di servizi online in occasione della consultazione da parte di un utente di un sito Internet, costituiva un dato personale, qualora detto fornitore fosse stato in grado di identificare la persona interessata grazie ad ulteriori informazioni nella sua disponibilità (sul tema v. anche Corte di giustizia, sentenza 20 dicembre 2017, causa C-434/16, ECLI:EU:C:2017:582) (v. capitolo VI, G. CARULLO).

In tema di re-identificazione, il Regolamento appresta una duplice tutela.

In prima battuta, esso prevede che, al fine di stabilire l'identificabilità di una persona e, quindi, la natura personale o meno dei dati, è opportuno considerare tutti gli altri dati ed i mezzi di cui si può ragionevolmente avvalere il soggetto che pone in essere il trattamento, tra cui è necessario considerare alcuni fattori obiettivi, quali i costi e il tempo necessario per l'identificazione, le tecnologie disponibili al momento del trattamento e i possibili futuri sviluppi tecnologici (considerando n. 26).

In seconda battuta, il Regolamento individua, nelle tecniche di pseudonimizzazione del dato, il giusto compromesso tra la necessità di ridurre i rischi di re-identificazione e le possibilità di molteplici utilizzi del dato, avvertite come preminenti dagli operatori economici che sfruttano le più recenti tecniche di raccolta ed elaborazione algoritmica dei dati (c.d. "Big Data analitycs").

La pseudonimizzazione è una misura prevista dall'art. 4, par. 5 del Regolamento quale strumento di sicurezza del trattamento dei dati personali, utilizzabile su valutazione del titolare. Essa riduce la correlabilità dei dati personali alla persona fisica cui ineriscono, sostituendo, in maniera non definitiva, gli elementi del dato che permettono l'identificazione, con un codice unico, ossia uno pseudonimo (per esempio, un *nickname*). In tal modo, da un lato, il valore informativo del dato personale sostituito dallo pseudonimo può essere facilmente recuperato per utilizzi ulteriori, e, dall'altro lato, è assicurato un adeguato livello di tutela dell'interessato. Infatti, posto che i dati sottoposti a pseudonimizzazione possono essere facilmente attribuiti a una persona fisica, essi sono considerati dati personali a tutti gli effetti e, come tali, sono soggetti agli obblighi di protezione sanciti dal Regolamento.

Pertanto, con la suddetta duplice impostazione, il Regolamento fa ricadere nel proprio ambito di tutela sia i dati pseudonimizzati, sia i casi limite di quei

dati, i quali, per quanto anonimi, possono ricondurre ad una determinata persona fisica, se sottoposti a re-identificazione. In altri termini, il Regolamento opera una delimitazione della nozione stessa di dato anonimo, che è speculare all'estensione del concetto di dato personale, con lo scopo di ampliare il suo campo di applicazione.

4.2.2. L'ambito di applicazione territoriale del Regolamento

L'art. 3 del Regolamento ne delimita l'ambito di applicazione territoriale.

Tale disposizione riveste un ruolo centrale per l'intera disciplina in materia di privacy, in quanto concretizza l'indirizzo politico dell'Unione Europea di garantire una protezione dei dati personali quanto più estesa e adatta a regolare un flusso di dati che è diventato a tutti gli effetti globale (Corte di giustizia UE, sentenza 16 luglio 2020, causa C-311/18, ECLI:EU:C:2020:559).

A tal fine, l'articolo in esame si fonda su due criteri principali: il criterio dello stabilimento sul territorio ed il criterio di collocazione fisica e geografica degli interessati.

Nello specifico, il primo criterio stabilisce che il Regolamento si applica «al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione» (art. 3, par. 1).

Secondo tale disposizione – che riprende gli approdi della Corte di giustizia UE nei noti casi *Google Spain* (Corte di giustizia UE, sentenza 13 maggio 2014, causa C-131/12, ECLI:EU:C:2014:317, punto 52) e *Weltilmo* (Corte di giustizia UE, sentenza 1° ottobre 2015, C 230/14, ECLI:EU:C:2015:639, punti 29 e ss.) –, perché siano applicabili le norme del Regolamento, sono necessari e sufficienti la presenza in territorio dell'Unione, per mezzo di uno stabilimento, di un titolare o di un responsabile, e un trattamento dei dati che, pur svolgendosi in un paese terzo, rientri nell'ambito delle attività di tale stabilimento.

Devono, quindi, chiarirsi i concetti di «stabilimento» e di «trattamento che rientra nell'ambito di attività dello stabilimento».

Per quanto attiene al primo aspetto, se il titolare o il responsabile del trattamento svolgono un'attività effettiva e reale, anche minima, tramite un'organizzazione stabile nel territorio di uno Stato membro, deve ritenersi che essi abbiano uno stabilimento nell'UE. Il caso tipico è quello della filiale o succursale di impresa.

Come chiarito dalle recenti Linee guida sull'ambito territoriale del Comitato Europeo per la protezione (*Guidelines 3/2018 on the territorial scope of the GDPR, Article 3*, Versione 2.1 del 12 novembre 2019), la definizione di «stabilimento» deve essere intesa in senso ampio, soprattutto in riferimento a quegli

operatori economici che, nell'UE, offrono servizi esclusivamente tramite Internet. Ne consegue che, in alcune circostanze, la presenza nell'UE di un solo dipendente o agente di un'impresa extra UE, che agisca con un grado sufficiente di indipendenza, costituisce stabilimento.

Ben più complessa appare la connessione tra il trattamento, svolto in paesi terzi, e l'attività svolta dallo stabilito nell'UE. In particolare, per determinare se il trattamento, sebbene effettuato in paesi terzi, sia comunque riferibile all'attività di un'impresa stabilita nell'Unione, le suddette Linee guida precisano la necessità di una valutazione caso per caso, fondata su due condizioni. In primo luogo, deve sussistere un rapporto stretto tra il responsabile o l'incaricato del trattamento sito in un paese terzo e l'impresa stabilita nell'UE. In secondo luogo, l'impresa stabilita nell'UE deve ricavare i propri profitti da un'attività correlata al trattamento effettuato in un paese terzo.

Qualora non ricorrano le suddette condizioni, il Regolamento può trovare comunque applicazione in virtù del criterio di collocazione fisica e geografica degli interessati, previsto dall'art. 3, par. 2. Infatti, questo secondo criterio stabilisce l'applicabilità delle norme del Regolamento «al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione».

Le menzionate linee guida precisano che, al fine della valutazione della presenza di un interessato nel territorio dell'Unione, sia determinante la sua semplice ubicazione geografica, non potendosi limitare l'applicazione del criterio in base allo *status* giuridico dell'interessato i cui dati personali sono oggetto di trattamento. Tale impostazione è coerente sia con il considerando n. 14 del Regolamento, secondo cui «la protezione offerta dal presente regolamento dovrebbe applicarsi alle persone fisiche, indipendentemente dalla loro nazionalità o dal loro luogo di residenza», sia con l'art. 8 della Carta UE, che prevede che «tutti» abbiano diritto alla protezione dei loro dati personali. Inoltre, detta ubicazione deve essere valutata nel momento in cui ha luogo l'attività in questione, ossia al momento dell'offerta di beni o servizi o al monitoraggio del comportamento, indipendentemente dalla loro durata.

Tuttavia, come precisato dalle linee guida, per l'applicazione dell'art. 3, par. 2 non è sufficiente un trattamento di dati personali di un interessato che si trovi nell'Unione, dovendosi vieppiù verificare una delle due opzioni relative all'offerta di beni o servizi o al monitoraggio del comportamento.

Come specificato dalle suddette linee guida, l'«offerta di beni o la prestazione di servizi», di cui all'art. 3, par. 2, lett. a), comprende, in particolare, l'offerta di servizi della società dell'informazione, definita all'art. 1, par. 1, lett. b) della Direttiva 2015/1535/UE (in *GUUE* L 241, del 17 settembre 2015, p. 1) come «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi». Tuttavia, il fatto che l'art. 3, par. 2, lett. a) preveda la non obbligatorietà di un pagamento da parte dell'interessato, dimostra una piena presa di coscienza da parte del Regolamento delle modalità di svolgimento delle transazioni online, fondate, più che sul prezzo, sullo scambio di dati personali degli utenti.

È opportuno altresì fare riferimento al contenuto del considerando n. 23 del Regolamento, il quale specifica che, per determinare se il titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno valutare alcuni parametri, quali l'utilizzo di una «lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione».

Per determinare, invece, se un'attività di trattamento sia assimilabile al monitoraggio del comportamento dell'interessato (art. 3, par. 2, lett. b), è necessario verificare se la persona fisica sia tracciata su Internet tramite il ricorso a tecniche di profilazione (considerando n. 24).

Il riferimento alla «profilazione» è un evidente indice dell'attenzione del legislatore europeo per i più recenti sviluppi in ambito tecnologico. In particolare, attraverso il richiamo a tale nozione, viene fatto riferimento ad una tecnica di trattamento automatizzato dei dati personali molto invasiva, posto che, a norma dell'art. 4, par. 4, attraverso di essa è possibile valutare «aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato». La profilazione non si caratterizza solo per un elevato livello di invasività nei confronti della vita privata e dei dati personali dell'interessato, bensì anche per un rilevante grado di diffusione. A tal proposito, infatti, come sottolineato dalle suddette linee guida, rientrano nella categoria della profilazione un'ampia gamma di attività di controllo, quali la pubblicità comportamentale, l'attività di geo-localizzazione a fini di marketing, il tracciamento online attraverso l'uso di cookie, le indagini e gli studi comportamentali basati su profili personalizzati. Tali attività hanno attirato l'attenzione del Parlamento europeo, il quale, nella risoluzione del 18 giugno 2020 sulla politica di concorrenza – relazione annuale 2019 (2019/2131(INI),

punto n. 105), ha invitato la Commissione «a vietare alle piattaforme di visualizzare pubblicità micro-mirata e ad accrescere la trasparenza per gli utenti».

Conclude la portata dell'art. 3 il suo terzo ed ultimo comma, che prevede l'applicabilità del Regolamento anche al trattamento dei dati personali, effettuato da un titolare del trattamento che non è stabilito nell'Unione, e che, tuttavia, si trovi in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (per esempio, le ambasciate e i consolati degli Stati membri dell'UE situati in paesi terzi).

4.2.3. I nuovi diritti introdotti dal Regolamento: il diritto all'oblio…

L'intento del Regolamento di apprestare una tutela adeguata al mutato ecosistema digitale traspare anche con riferimento ai nuovi diritti attribuiti all'interessato.

Il diritto all'oblio, di cui all'art. 17 del Regolamento, segna la definitiva collocazione normativa di una problematica, che, affermatasi con la diffusione dell'utilizzo dei motori di ricerca, era già stata oggetto dell'intervento della Corte di giustizia, con la menzionata sentenza *Google Spain*. In tale pronuncia, la Corte di giustizia, discostandosi, in parte, dalle relative conclusioni dell'Avvocato generale Jääskinen (Conclusioni dell'Avvocato generale Jääskinen del 25 giugno 2013 nella causa *Google Spain*, causa C-131/12, spec. punti 108-110), ha acconsentito a che ragioni connesse al «diritto ad essere dimenticati» potessero prevalere tanto su un generale interesse a un più rapido e agevole accesso alle informazioni, quanto sui diritti economici dei fornitori di servizi di comunicazione. Più precisamente, la Corte ha stabilito che «[l']attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificato come trattamento di dati personali, e che il gestore di detto motore di ricerca deve essere considerato come il responsabile del trattamento». Dunque, sulla base di questa considerazione e valorizzando alcune delle disposizioni contenute nella Direttiva 95/46/CE alla luce degli artt. 7 e 8 della Carta UE, i giudici di Lussemburgo hanno riconosciuto il diritto del singolo interessato, in presenza di determinate condizioni, a chiedere al gestore del motore di ricerca, prima, e alle autorità competenti, poi, l'eliminazione dall'elenco dei risultati che appare in seguito ad una ricerca effettuata a partire dal nome di tale soggetto dei *links* verso pagine *web* pubblicate da terzi (c.d. "deindicizzazione").

L'art. 17 del Regolamento, facendo propri i suddetti approdi giurisprudenziali ed estendendone l'ambito oltre l'attività dei motori di ricerca, ha sancito il «Diritto alla cancellazione (diritto all'oblio)» (F. DI CIOMMO, 2019, p. 353).

In particolare, l'art. 17, par. 1 stabilisce il diritto dell'interessato ad ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, nonché l'obbligo per quest'ultimo di cancellare senza ingiustificato ritardo i dati personali. Affinché l'interessato possa esercitare tale diritto, deve ricorrere almeno uno dei seguenti presupposti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato ha revocato il consenso su cui si basa il trattamento (è il caso, delineato dal considerando n. 65, in cui l'interessato che ha prestato il proprio consenso quando era minore e, quindi, non pienamente consapevole dei rischi derivanti dal trattamento, ritenga successivamente di eliminare tale tipo di dati personali); c) l'interessato si era precedentemente opposto al trattamento; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; infine, f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Inoltre, l'art. 17, par. 2 stabilisce che, al ricorrere dell'obbligo di cancellazione di cui al primo paragrafo, il titolare del trattamento vi provvede «tenendo conto della tecnologia disponibile», adottando, altresì, le misure ragionevoli, anche di natura tecnica, per informare gli altri eventuali titolari del trattamento che stanno trattando i dati personali, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. La scelta di ricorrere alla clausola generale della «tecnologia disponibile», allo stesso modo di quanto già osservato in merito alla re-identificazione, rappresenta l'intento del legislatore di sottrarre il Regolamento al rischio di obsolescenza normativa. Dalla disposizione in questione, si ricava altresì che l'obbligo di cancellazione deve essere ottemperato sia dal titolare del trattamento oggetto della richiesta di cancellazione dei dati personali, sia dagli altri soggetti che stiano trattando quegli stessi dati personali, che dal primo devono essere quindi debitamente informati dell'obbligo di cancellazione pendente.

Infine, il terzo paragrafo ha ripreso dalla sentenza *Google Spain* e dalle Linee Guida del Gruppo dell'art. 29 (Linee guida del 26 novembre 2014 – WP 225 in tema di diritto all'oblio) la necessità di sottoporre il diritto all'oblio al bilanciamento con interessi contrapposti.

A tal proposito, infatti, l'art. 17 sostiene la non applicabilità dei parr. 1 e 2, qualora la conservazione dei dati personali sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico inte-

resse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria (considerando n. 65).

Di recente, con la sentenza *Google 2* (Corte di giustizia UE, sentenza 24 settembre 2019, causa C-507/17, ECLI:EU:C:2019:772), la Corte di giustizia è stata chiamata, ai sensi dell'art. 267 TFUE, a chiarire la portata territoriale del diritto all'oblio. In tale pronuncia, la Corte ha affermato che dall'applicazione del diritto all'oblio consegue l'obbligo per il titolare del trattamento, ossia il gestore di un motore di ricerca, di effettuare la cancellazione dei *links* controversi nelle versioni del motore di ricerca relative ai domini dei vari Stati membri (ad esempio google.it, .de, .fr, ecc.). Secondo i giudici del Lussemburgo, nonostante Internet costituisca una rete globale senza frontiere, caratteristica accentuata dai motori di ricerca che conferiscono ubiquità alle informazioni e ai *link*s ricercati, la portata territoriale dell'obbligo di cancellazione deve ritenersi coincidente con il solo territorio dell'Unione, in quanto né l'art. 17, né le altre norme del Regolamento relative ai poteri attribuiti alle autorità di controllo nazionali, prevedono strumenti che possano estendere ulteriormente tale portata.

La sentenza non è stata esente da critiche. Parte della dottrina ha, infatti, sottolineato che il diritto all'oblio, così come interpretato dalla sentenza in analisi, non conferirebbe all'interessato una tutela effettiva e completa, in quanto lo stesso resterebbe esposto al concreto pericolo che, attraverso misure elusive, i suoi dati rimangano accessibili sulle versioni del motore di ricerca d'oltreoceano.

A fronte di tali critiche, è stato osservato come la sentenza della Corte risulti coerente con l'impostazione del Regolamento per una duplice ragione. Innanzitutto, essa appare in linea con la volontà del legislatore europeo di garantire, attraverso lo strumento del Regolamento, un livello di tutela dei dati personali omogeneo in tutti gli Stati membri, sicché, a fronte dell'accoglimento di una richiesta di cancellazione dei *links* controversi, il gestore del motore di ricerca può essere obbligato a rimuoverli da tutti i domini attivi negli Stati membri dell'Unione.

Inoltre, la sentenza, valorizzando il terzo paragrafo dell'art. 17, non esclude categoricamente che la portata del diritto all'oblio possa estendersi a livello globale. A giudizio della Corte, infatti, sebbene il diritto dell'Unione non imponga che la deindicizzazione accolta verta su tutte le versioni del motore di ricerca in questione, neppure lo vieta. Le autorità di controllo o giudiziarie di uno Stato membro, pertanto, sono competenti ad effettuare, conformemente agli standard nazionali, un bilanciamento tra il diritto alla protezione dei dati personali e il diritto alla libertà d'informazione e, al termine di tale bilanciamento, richiedere al gestore del motore di ricerca, se del caso, di effettuare la cancellazione dei *links* controversi su tutte le sue versioni, finanche a livello globale.

4.2.4. … e il diritto alla portabilità dei dati

Il Regolamento ha altresì introdotto, *ex* art. 20, il nuovo dritto alla c.d. "portabilità dei dati personali" (L. BIANCHI, 2019, p. 223). Tale diritto si caratterizza per una duplice accezione.

In prima battuta, l'art. 20, par. 1 delinea il diritto dell'interessato di «ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento». In altri termini, come specificato dalle Linee guida del Gruppo art. 29 (Linee guida del 5 aprile 2017 – WP 242 rev. 01 sul diritto alla portabilità dei dati), la portabilità dei dati si sostanzia nel diritto dell'interessato a ricevere un *dataset* contenente i suoi dati personali trattati da un titolare (quali ad esempio l'elenco dei brani musicali preferiti ascoltati tramite una piattaforme di musica in streaming, o la rubrica dei contatti di posta elettronica), al fine di conservarli per scopi ulteriori. In questo senso, il diritto alla portabilità costituisce uno strumento con cui gli interessati possono gestire e riutilizzare, in piena autonomia, i propri dati personali.

In seconda battuta, l'art. 20, par. 1 permette all'interessato di trasmettere i propri dati personali tra più titolari del trattamento, senza che questi possano opporgli impedimenti, a meno che non ricorrano specifici casi eccezionali. Sotto quest'ultimo profilo, infatti, come previsto dal secondo paragrafo, tale passaggio dei dati tra più titolari avviene direttamente, ma solo qualora ciò sia «tecnicamente possibile». In questo senso, il Regolamento intende promuovere lo sviluppo di formati interoperabili da parte dei titolari, così da agevolare la portabilità dei dati, senza, tuttavia, configurare un obbligo in capo agli stessi di introdurre o mantenere sistemi di trattamento tecnicamente compatibili (considerando 68).

La combinazione delle due accezioni del diritto alla portabilità dei dati personali contribuisce a ridurre i rischi di «cattura» (c.d. "*lock-in*") degli utenti all'interno di un determinato ecosistema online, posto che questi possono spostare facilmente i loro dati su più piattaforme online, e, contestualmente, ad incentivare la competizione tra gli operatori del mercato ad offrire servizi migliori, al fine di attrarre a sé la portabilità dei dati.

Oltre alla compatibilità tecnica, il diritto alla portabilità dei dati è subordinato a tre condizioni cumulative: i) il trattamento dei dati deve esse fondato sul consenso dell'interessato oppure su un contratto di cui è parte l'interessato; ii) il trattamento deve essere «effettuato con mezzi automatizzati», non trovando, dunque, applicazione relativamente ad archivi o registri cartacei; iii) il trattamento deve avere ad oggetto i dati personali forniti da un interessato consapevolmente e attivamente (le informazioni inserite in un modulo di regi-

strazione online), oppure derivati dall'osservazione delle sue attività svolte online (la cronologia della navigazione su un sito web o delle ricerche effettuate).

I parr. 3 e 4 dell'art. 20, invece, regolano i rapporti tra il diritto alla portabilità dei dati, il diritto all'oblio e altri diritti.

Nello specifico, il par. 3 definisce le interazioni tra la portabilità dei dati e il diritto all'oblio: la portabilità dei dati, non comportando la cancellazione automatica dei dati dai sistemi del titolare e non incidendo sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione, lascia del tutto impregiudicato l'esercizio del diritto all'oblio.

Diversamente, il par. 4 stabilisce che il diritto alla portabilità dei dati non deve ledere i diritti e le libertà altrui. La lesione si configurerebbe, in primo luogo, se la portabilità avesse ad oggetto un *dataset* composto non solo dai dati dell'interessato che esercita legittimamente il diritto, ma anche dai dati personali di altri interessati, che non hanno acconsentito espressamente a tale portabilità. Ne deriva che, per evitare di ledere i diritti dei terzi interessati, il «nuovo» titolare che ha ricevuto un *dataset* contenente dati riferibili a più interessati, non può utilizzare i dati riferiti a terzi per le proprie finalità. In caso contrario, è verosimile che il trattamento risulti illecito per violazione del principio di correttezza del trattamento, soprattutto qualora i terzi in questione non ricevano informativa e non siano in grado di esercitare i diritti loro riconosciuti in quanto interessati.

In secondo luogo, la lesione dei diritti e delle libertà altrui potrebbe ricorrere nel caso in cui la richiesta di portabilità riguardi dati soggetti a diritti di proprietà intellettuale o informazioni commerciali riservate, quali segreti industriali e aziendali. Tuttavia, come precisato dalle suddette Linee Guida, benché sia opportuno tenere conto dei diritti in questione prima di rispondere a una richiesta di portabilità, «tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni».

4.2.5. Brevi considerazioni sugli effetti delle novità introdotte dal Regolamento

L'analisi delle suddette novità mette in luce, oltre alla necessaria opera di adeguamento normativo al nuovo contesto digitale, l'elevato grado di dinamicità della tutela apprestata dal Regolamento, che è una caratteristica che le deriva dall'essere strettamente aderente, più che all'interessato, ai suoi dati personali. In altre parole, la tutela prevista dal Regolamento è dinamica in quanto idonea ad adeguarsi alle molteplici e differenti operazioni di trattamento a cui il dato personale stesso è sottoposto.

Orbene, siffatta tutela si pone quale strumento principale attraverso cui il Regolamento ha inteso realizzare il suo duplice obiettivo di garantire un quan-

to più elevato e coerente livello di protezione dei dati personali e un'ampia circolazione di tali dati. Sotto il primo aspetto, il carattere dinamico della tutela consente al Regolamento di trovare applicazione con riferimento, per esempio, alle operazioni di re-identificazione, che fanno oscillare il dato tra le categorie dell'anonimato e della riferibilità ad un soggetto determinato; oppure nel caso della portabilità dei dati, che incentiva uno scambio di dati multidirezionale, ossia formato da continui passaggi dei dati personali tra più titolari e responsabili del trattamento; oppure, ancora, nel caso della richiesta di cancellazione dei dati personali, che dispiega i propri effetti non solo nei confronti del titolare destinatario di tale richiesta, ma anche nei confronti di tutti gli altri titolari del trattamento che utilizzino i medesimi dati; o, infine, in occasione di trattamenti dei dati svolti al di fuori dei confini dell'UE, ossia in zone geografiche remote rispetto all'ubicazione dell'interessato.

Sotto il secondo aspetto, la tutela dinamica, proprio perché aderente ai dati personali, costituisce il giusto compromesso tra i diritti dell'interessato e l'interesse degli operatori economici a sottoporre tali dati a quante più numerose e varie operazioni di trattamento e di scambio.

In questo senso, il Regolamento rappresenta il più compiuto *trait d'union* tra la disciplina sulla protezione dei dati personali e il mercato unico digitale.

5. L'adeguamento della normativa nazionale al Regolamento

Il Regolamento, come già osservato, è direttamente applicabile negli ordinamenti degli Stati membri, non richiedendo (ma anzi vietando), da parte di questi ultimi, alcun tipo di intervento di recepimento. Ciò non significa, tuttavia, che gli Stati membri debbano rimanere inerti. Viceversa, essi devono dare effettiva attuazione al Regolamento, ed esercitare i poteri che quest'ultimo espressamente attribuisce loro.

Il legislatore italiano è intervenuto, in questo senso, con l'art. 13 della Legge n. 163/2017 (in *GURI* del 6 novembre 2017, n. 259), che ha demandato al Governo italiano l'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento. Nell'esercizio della delega così conferita, è stato adottato il D.Lgs. n. 101/2018 (in *GURI* del 4 aprile 2018, n. 205), che ha modificato il D.Lgs. n. 196/2003, recante il «Codice in materia di protezione dei dati personali» («Codice Privacy», in *GURI* 29 luglio 2003, n. 174).

Il D.Lgs. n. 101/2018 è suddiviso in sei Capi e si compone di 28 articoli, che, con tecnica novellistica, apportano al Codice Privacy le modifiche necessarie ad assicurarne la conformità al Regolamento, abrogando le disposizioni

incompatibili, modificandone altre e prevedendo in limitati casi nuove disposizioni in esecuzione delle riserve normative espressamente previste dal Regolamento stesso.

L'eterogeneità degli interventi cui è stato sottoposto il Codice Privacy ne rende impossibile l'individuazione di una comune struttura logica. Dunque, vale la pena limitare l'analisi ad alcuni aspetti principali della nuova disciplina nazionale, relativamente alla figura del Garante per la protezione dei dati personali, alle regole deontologiche ed al nuovo impianto sanzionatorio.

Per quanto riguarda il primo tema, il nuovo art. 2-*bis* del Codice Privacy specifica che l'Autorità pubblica indipendente richiesta dall'art. 51 del Regolamento è individuata nel Garante per la protezione dei dati personali. Il Garante per la protezione dei dati personali, istituito con la c.d. legge sulla privacy del 1995 (in *GURI* del 8 gennaio 1997, n. 5), è l'Autorità di controllo alla quale viene affidato, nell'ordinamento nazionale, il compito di attuare le disposizioni del Codice Privacy e del Regolamento, nonché di vigilare sulla loro corretta osservanza, disciplinandone le modalità di funzionamento, anche secondo i principi e in coerenza con le altre norme vigenti. Il Codice Privacy detta la disciplina di riferimento per il Garante della privacy, disciplinandone: i) l'organigramma e la struttura organizzativa (art. 153); ii) i requisiti e le procedure per la scelta del personale dipendente, così come i compiti e gli emolumenti loro spettanti (artt. 153, 155 e 156); iii) i compiti e i poteri (artt. 154 e 154-*bis*); iv) i provvedimenti che lo stesso può emanare, con l'espressa esclusione del suo intervento in relazione ai trattamenti di dati effettuati dalle autorità giudiziarie nell'esercizio delle proprie funzioni (artt. 157 e 158). Infine, il Garante è legittimato ad agire e stare in giudizio tramite i professionisti dell'Avvocatura dello Stato, oppure tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero avvocati del libero foro (art. 154-*ter*).

Inoltre, il Codice Privacy prevede il diritto dell'interessato di proporre reclamo (art. 141) e di rivolgere una segnalazione (art. 144) al Garante, il quale disciplina con propri regolamenti i rispettivi procedimenti (art. 142, comma 5).

Sul punto, deve altresì sottolinearsi che la figura del Garante non esaurisce la categoria delle autorità preposte alla tutela dei diritti dell'interessato. Infatti, il legislatore ha inserito nel Codice Privacy il nuovo Capo 0.1, che consta del solo art. 140-*bis*, rubricato «Forme alternative di tutela». Dal momento che gli artt. 77 e 79 del Regolamento lasciano impregiudicata la possibilità di avvalersi di ogni altro ricorso amministrativo o extragiudiziale disponibile, l'art. 140-*bis* assicura all'interessato, nel caso in cui lo stesso ritenga che i diritti attribuitigli dalla normativa in materia di protezione dei dati personali siano stati violati, la possibilità di scegliere alternativamente tra la proposta di reclamo al Garante

o il ricorso dinanzi all'Autorità giudiziaria. Tale alternatività tra la tutela giurisdizionale e quella innanzi al Garante mira ad evitare il rischio di duplicazione di procedimenti e, soprattutto, nel caso in cui i rispettivi procedimenti siano instaurati tra le stesse parti e per il medesimo oggetto, scongiura il potenziale conflitto di «giudicati» in caso di impugnazione, davanti al giudice, della decisione del Garante sul reclamo.

Per quanto attiene, invece, alle regole deontologiche, l'art. 2-*quater* del Codice attribuisce al Garante il compito di dare attuazione alla possibilità offerta dal Regolamento agli Stati membri di adottare disposizioni più stringenti per la disciplina del trattamento dei dati personali in determinati settori.

In particolare, l'art. 2-*quater* prevede che il Garante promuova l'adozione di regole deontologiche per le seguenti tipologie di trattamenti: *a*) per quelli connessi ad un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, *ex* art. 6, par. 1, lett. c) ed e) del Regolamento; per i trattamenti di dati genetici, dati biometrici o dati relativi alla salute, *ex* art. 9, par. 4 del Regolamento; *b*) per quelli connessi a specifici ambiti (libertà d'espressione e di informazione; accesso del pubblico ai documenti ufficiali; numero di identificazione nazionale; rapporti di lavoro; archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; dati vigenti presso chiese e associazioni religiose), *ex* artt. da 85 a 91 del Regolamento.

Le Regole deontologiche fino ad ora adottate, dopo essere state sottoposte dal Garante ad un esame di compatibilità con il Regolamento, sono state pubblicate nella Gazzetta Ufficiale della Repubblica italiana e riportate nell'allegato A del nuovo Codice Privacy. Il rispetto di tali regole costituisce requisito di liceità del relativo trattamento.

Infine, per quanto attiene al nuovo regime sanzionatorio, l'art. 83 del Regolamento attribuisce un ruolo fondamentale alle autorità di controllo nazionali, le quali, a fronte di una violazione del Regolamento, possono alternativamente (o cumulativamente) applicare una delle misure correttive di cui all'art. 58, par. 2, ovvero infliggere una sanzione amministrativa pecuniaria di cui al medesimo art. 83, par. 4.

Tale discrezionalità, tuttavia, non è assoluta. Il Regolamento, infatti, impone limiti specifici alla discrezionalità delle autorità di controllo nazionali e, a livello più generale, richiede loro di improntare il proprio potere afflittivo ai criteri dell'effettività, della proporzionalità e della dissuasività della sanzione. Quanto ai limiti normativi, l'art. 83, par. 2, ad esempio, detta una serie di parametri da tenere in considerazione nella valutazione degli illeciti, tra cui, il carattere doloso o colposo della violazione, le categorie di dati personali interessate dalla violazione, il grado di responsabilità del titolare e l'eventuale adozione di precedenti provvedimenti correttivi. Inoltre, l'art. 83, par. 4, stabilisce tre categorie di

violazioni e, per ciascuna di esse, ne individua le corrispondenti sanzioni amministrative pecuniarie, delle quali sono fissati i limiti massimi, per il vero, molto elevati (per le imprese, nei casi di violazioni più gravi, sono previste sanzioni fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente). Ancora, l'art. 83, comma 8, prevede che l'esercizio da parte dell'autorità di controllo dei poteri sanzionatori è soggetto a garanzie procedurali adeguate, in conformità al diritto dell'Unione e all'ordinamento di ciascuno Stato membro, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

Se tali limiti caratterizzano l'esercizio del potere sanzionatorio per i casi di violazione delle norme stabilite dal Regolamento, per i casi di violazioni di disposizioni diverse da quelle già sanzionate dal Regolamento, l'art. 84 lascia un ampio margine di autonomia agli Stati membri, riconoscendo loro il compito di stabilirne le relative norme. Pertanto, in virtù della facoltà prevista dall'art. 84 del Regolamento, l'art. 15 del D.Lgs. n. 101/2018 ha introdotto nel Codice Privacy il nuovo art. 166, il quale detta le fattispecie specifiche di violazione delle disposizioni del Codice stesso. È questo il caso della violazione, da parte del titolare del trattamento, dell'obbligo di cui all'art. 2-*quinquies*, comma 2, del Codice Privacy, che impone di redigere con linguaggio particolarmente chiaro e semplice, comprensibile e accessibile al minore, le informazioni e le comunicazioni relative al trattamento che lo riguardi; oppure, della violazione delle modalità di redazione e conservazione di cartelle cliniche, prescritte dall'art. 92, comma 1 del Codice Privacy; o, ancora, della violazione delle menzionate regole deontologiche.

Il suddetto ampio margine di autonomia si riscontra anche con riferimento alle sanzioni penali, interamente rimesse agli Stati membri. Sotto questo profilo, il Codice Privacy, così come modificato ed integrato dal D.Lgs. n. 101/2018, disciplina le fattispecie penalmente rilevanti relative: al trattamento illecito dei dati (art. 167); alla comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (art. 167-*bis*); all'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167-*ter*); alla falsità nelle dichiarazioni rese al Garante e l'interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri della stessa Autorità (art. 168); all'inosservanza dei provvedimenti emanati dal Garante (art. 170).

Bibliografia

BALDUCCI ROMANO F., *Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia*, in *Rivista italiana di diritto pubblico comunitario*, 2015, p. 1619.

BESTAGNO F., *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, in *Il diritto dell'Unione europea*, 2015, 1, p. 25.

BIANCHI L., *Il diritto alla portabilità dei dati*, in R. PANETTA (a cura di) *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 2019, p. 223.

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*, 2018, 2, p. 64.

CARTABIA M., *Convergenze e divergenze nell'interpretazione delle clausole finali della carta dei diritti fondamentali dell'Unione europea*, in *Rivista AIC*, 2018.

DE SALVIA M., *Dati personali e sfera privata nella giurisprudenza della Corte europea dei diritti dell'uomo: ricostruzione sommaria delle linee-guida*, in M. FUMAGALLI MERAVIGLIA (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica o scontro di civiltà?*, Editoriale Scientifica, Napoli, 2015.

DI CIOMMO F., *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, p. 353.

DOMINELLI S., GRECO G., *I mercati dei servizi tra regolazione e governance*, Giappichelli, Tonio, 2019.

DONATI F., *Art. 8*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti, Commento alla Carta dei diritti fondamentali dell'Unione europea*, Il Mulino, Bologna, 2001, p. 83.

FABBRINI F., *Privacy and National Security in the Digital Age*, in *Tilburg Law Review, Journal of International and European Law*, 2015, p. 8.

GRANGER F.M.P., IRION K., *The right to protection of personal data: the new posterchild of European Union citizenship?, Civil rights and EU citizenship*, Edward Elgar, Cheltenham, 2018.

KRANENBORG H.R., *Article 8, Protection of personal data, The EU Charter of Fundamental Rights: a commentary*, in S. PEERS, T. HERVEY, J. KENNER, A. WARD (a cura di), *The EU Charter of Fundamental Rights: A Commentary*, C.H. Beck, Munich, 2014, p. 223.

NASCIMBENE B., *Tutela dei diritti fondamentali e competenza della Corte di giustizia nel Trattato di Amsterdam*, in *Scritti in onore di Giuseppe Federico Mancini*, Giuffrè, Milano, 1998, p. 683.

OLIVER P., *The protection of privacy in the economic sphere before the European Court of Justice*, in *Common Market Law Review*, 2009, p. 113.

PISAPIA A., *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, Torino, 2018.

PIZZETTI F., *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA, M. D'AMICO (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, Milano, 2009, p. 83.

POLLICINO O., *Diritto all'oblio e conservazione di dati: la Corte di giustizia a piedi uniti: verso un digital right to privacy*, in *Giurisprudenza costituzionale*, 2014, p. 2949.

POLLICINO O., BASSINI M., *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Il diritto dell'informazione e dell'informatica*, 2015, p. 741.

PUGLIA M., *La protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'UE*, in AA.VV. (a cura di), *Liber amicorum Antonio Tizzano: de la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Giappichelli, Torino, 2018, p. 788.

ROSSI DAL POZZO F., *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*)*, in *Rivista di diritto internazionale*, 2016, p. 690.

TESAURO G., *I diritti fondamentali nella giurisprudenza della Corte di giustizia*, in *RIDU*, 1992, p. 426.

VIOLA R., *La riforma del quadro normativo dell'audiovisivo tra mercato unico digitale e valori fondamentali*, in G.B. ABBAMONTE, E. APA, O. POLLICINO (a cura di), *La riforma del mercato audiovisivo europeo*, Giappichelli, Torino, 2019, p. XI.

WARREN S., BRANDEIS D., *The Right to Privacy*, in *Harvard Law Review*, 1890, vol. IV, n. 5.

ZENO-ZENCOVICH V., *La "comunione" di dati personali: un contributo al sistema dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, 2009.

ZENO-ZENCOVICH V., *Art. 8*, in S. BARTOLE, G. CONFORTI, B. RAIMONDI (a cura di) *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, Cedam, Padova, 2001, p. 314.

III.

DIGITALIZZAZIONE E DIRITTO AD UNA BUONA AMMINISTRAZIONE (IL PROCEDIMENTO AMMINISTRATIVO, FRA DIRITTO UE E TECNOLOGIE ICT)

Diana-Urania Galetta

SOMMARIO: 1. Premessa. – 2. Digitalizzazione e responsabile del procedimento. – 3. Un esempio concreto: il responsabile del procedimento all'epoca delle ICT quale elemento chiave del percorso verso una trasparenza reale ed effettiva. – 4. Digitalizzazione e comunicazione di avvio del procedimento. – 5. Digitalizzazione e decisione imparziale ed equa. – 6. Digitalizzazione e decisione entro un termine ragionevole. – 7. *Segue*. Lo sportello unico telematico e l'istanza telematica. – 8. *Segue.* L'Unione Europea e il "portale digitale unico". – 9. Digitalizzazione e diritto di ogni persona di essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale che le rechi pregiudizio. – 10. Digitalizzazione e diritto di ogni persona di accedere al fascicolo che la riguarda. – 11. Digitalizzazione e obbligo per l'amministrazione di motivare le proprie decisioni. – 12. Il procedimento amministrativo oggi: fra diritto ad una buona amministrazione (e relativi "standard minimi" *ex* art. 41 CDUE) e conseguenze derivanti dall'utilizzo delle tecnologie ICT.

1. Premessa

Sin dall'adozione della Carta dei diritti fondamentali dell'Unione Europea (CDUE), nel contesto UE la buona amministrazione si caratterizza come un nuovo diritto fondamentale della persona: il diritto ad una buona amministrazione, così come esso è scritto e dettagliato nell'art. 41 di detta Carta (D.-U. GALETTA, 2018b, p. 320).

Si tratta di un diritto e non solamente di un principio guida dell'azione amministrativa (A. ZITO, 2002), la cui nozione giuridica coincide con quell'idea filosofica secondo cui una buona Amministrazione Pubblica è un'amministrazione che adempie alle funzioni che le sono proprie nel contesto di una democrazia; ed è un'amministrazione che è al servizio dei cittadini e che svolge il

proprio lavoro in maniera imparziale e razionale, giustificando le proprie azioni ed orientandosi continuamente all'interesse generale.

Quanto all'interesse generale a cui tale azione deve essere orientata, questo, «nello Stato di diritto sociale e democratico risiede nel miglioramento permanente e integrale delle condizioni di vita delle persone» (J. RODRÍGUEZ-ARANA, 2013, p. 26). Il che appare come un'affermazione del tutto condivisibile: quale che sia il concetto di "miglioramento delle condizioni di vita" al quale ci si intenda, di volta in volta, orientare, anche in ragione della diversa ideologia dominante al riguardo, in luoghi ed epoche storiche diverse.

In questo senso, come vedremo, nell'epoca attuale la rivoluzione legata all'utilizzo delle più moderne tecnologie dell'informazione e della comunicazione (ICT) e all'uso dell'Intelligenza Artificiale può aiutare, e molto, a realizzare l'obiettivo della buona amministrazione nel nostro Paese.

A quest'ultimo riguardo va peraltro precisato, già a titolo di premessa, come il contenuto del diritto ad una buona amministrazione non debba considerarsi come limitato a quanto espressamente descritto nell'art. 41 CDUE.

Occorre infatti osservare, anzitutto, come la dizione «tale diritto comprende in particolare» usata dal legislatore dell'art. 41 CDUE, evidenzi chiaramente come i diritti espressamente elencati al comma 2 (e di cui si dirà partitamente nei prossimi paragrafi) non siano da considerarsi come esaustivi di tutto quanto può essere ricompreso nel concetto di buona amministrazione.

Il concetto più generale di che cosa debba intendersi per diritto ad una buona amministrazione è infatti contenuto nell'art. 41, comma 1, CDUE che si riferisce al diritto di ogni persona «a che le questioni che lo riguardano siano trattate in modo imparziale, equo ed entro un termine ragionevole».

La corrispondenza con quanto previsto dall'art. 97 della nostra Costituzione, laddove esso dispone che «I pubblici uffici sono organizzati (…) in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione», appare evidente. Le due previsioni si completano, cioè, reciprocamente: poiché un'amministrazione i cui pubblici uffici siano organizzati, secondo quanto prevede l'art. 97, comma 1, Cost., in modo che sia assicurata l'imparzialità dell'amministrazione è anche la sola che possa garantire il trattamento imparziale ed equo delle questioni che riguardano gli amministrati. E, allo stesso modo, un'amministrazione i cui pubblici uffici siano organizzati in modo da assicurare il "buon andamento" dovrebbe essere la sola idonea a garantire il rispetto del un termine ragionevole, cui fa riferimento l'art. 41 CDUE.

Il principio di buon andamento, infatti, certamente racchiude in sé anche un'esigenza di efficienza della pubblica amministrativa: nella prospettiva, cioè, che "buon andamento" significa anzitutto "andamento". Esso identifica perciò, certamente, l'idea di un'amministrazione che assume le proprie decisioni entro uno spazio di tempo ragionevole.

La migliore estrinsecazione del principio del buon andamento è rappresentata dalla Legge n. 241/1990 sul procedimento amministrativo (Legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e diritto di accesso ai documenti amministrativi): in linea con l'idea espressa a suo tempo in dottrina (G. BERTI, 1968) di una necessità di "procedimentalizzazione del buon andamento".

A partire dagli anni Novanta ha iniziato peraltro ad affermarsi una lettura orientata dei principi di imparzialità e buon andamento, strettamente connessa alla più generale esigenza di rimodernare la "macchina amministrativa", anche allo scopo di operare una adeguata riorganizzazione dell'apparato amministrativo.

Anche in questa prospettiva appare evidente il ruolo fondamentale che possono svolgere, oggi, le ICT.

Sia, dunque, nell'ottica della previsione di cui all'art. 97 della nostra Costituzione, che nell'ottica di quel diritto ad una buona amministrazione enunciato all'art. 41 della Carta dei diritti dell'Unione Europea, appare perciò evidente il ruolo cruciale delle ICT. Si tratta di un ruolo che esse in parte già svolgono, ma che sempre di più saranno chiamate a svolgere negli anni a venire; ed il cui contenuto concreto (attuale e potenziale) si tenterà di identificare nei paragrafi qui di seguito, con riferimento ai vari aspetti connessi al diritto ad una buona amministrazione.

Prima di potere iniziare l'analisi dei singoli istituti occorre peraltro fare un ulteriore passaggio e/o precisazione. Data l'elencazione non esaustiva contenuta nella previsione di cui all'art. 41 CDUE – quanto ai contenuti specifici del diritto ad una buona amministrazione – per poterli meglio identificare occorre, innanzitutto, fare riferimento alla giurisprudenza delle Corti UE antecedente all'adozione della Carta di Nizza. Questo perché, come è ormai noto, sono le Corti UE che hanno contributo, attraverso la loro copiosa giurisprudenza in materia, ad identificarne i contenuti specifici che sono stati poi parzialmente trasfusi nella previsione dell'art. 41 CDUE. Ed è infatti lo stesso testo delle spiegazioni allegate alla Carta a fare rinvio, a tale proposito, alla preesistente giurisprudenza della Corte di giustizia (Spiegazioni relative alla Carta dei Diritti Fondamentali, doc. 2007/C 303/02, in *GUUE* C/303 del 14 dicembre 2007). Ivi si legge, infatti, che «L'articolo 41, è basato sull'esistenza di una comunità di diritto, le cui caratteristiche sono state sviluppate dalla giurisprudenza che ha sancito segnatamente il principio della buona amministrazione».

In secondo luogo, con riguardo ai contenuti ulteriori del diritto ad una buona amministrazione, occorre a mio parere fare riferimento anche a quegli "istituti" del procedimento amministrativo che risultano talmente consolidati all'interno del nostro ordinamento nazionale da non potere essere separati

dall'idea stessa di buona amministrazione, per come noi oramai la intendiamo. Tale è il caso, ad esempio, per la figura del responsabile del procedimento, che per di più è considerata come una c.d. *best practice* nel contesto dell'Unione Europea (G. DELLA CANANEA, D.-U. GALETTA, 2016, p. XXI ss.). Ma anche per la c.d. comunicazione di avvio del procedimento. Ed è infatti da questi due istituti che prenderà avvio l'analisi che segue, alla ricerca del nesso fra ICT e diritto ad una buona amministrazione.

2. Digitalizzazione e responsabile del procedimento

Anche se essa era prevista già da alcune norme speciali, la figura del responsabile del procedimento costituisce una delle novità principali e più rilevanti introdotte nel nostro ordinamento nazionale dalla Legge n. 241/1990 sul procedimento amministrativo. E senza dubbio, come vedremo, tale istituto rientra a pieno titolo fra quelli che costituiscono l'essenza del diritto ad una buona amministrazione, così come esso è declinato all'interno del nostro ordinamento.

In secondo luogo, come vedremo, tale figura rappresenta il punto di snodo essenziale del rapporto fra digitalizzazione della Pubblica Amministrazione e diritto ad una buona amministrazione: soltanto attraverso un'adeguata valorizzazione di tale figura sarà infatti possibile passare dall'uso delle ICT come strumento di miglioramento della relazione Pubblica Amministrazione-cittadino riservato solo ai pochi, alle ICT come strumento di efficientamento del rapporto Pubblica Amministrazione-cittadino in una prospettiva che possa corrispondere all'idea della buona amministrazione.

Prima di chiarire meglio questo passaggio è opportuno peraltro ricordare brevemente che cosa prevede il nostro ordinamento nazionale a proposito del responsabile del procedimento nella Legge n. 241/1990.

In particolare, la Legge n. 241/1990 prevede tre cose:

1. che sia identificata, per legge o per regolamento, l'unità organizzativa responsabile del procedimento (art. 4): ossia l'entità organizzativa, l'ufficio responsabile;
2. che all'interno di ciascuna unità organizzativa sia individuato, da parte del dirigente, il funzionario responsabile del procedimento: ossia la persona fisica responsabile. Con la precisazione che, sino a che tale soggetto non venga specificamente identificato, è considerato quale responsabile del singolo procedimento il funzionario preposto all'unità organizzativa (art. 5);
3. che l'unità organizzativa competente ed il nominativo del responsabile del procedimento siano comunicati ai soggetti di cui all'art. 7, comma 1;

4. a far data dalle modifiche introdotte col c.d. DL-semplificazioni, che anche il domicilio digitale sia comunicato ai soggetti di cui all'art. 7, comma 1 (così prevede il D.L. n. 76/2020 all'art. 12, comma 1, convertito con la Legge 11 settembre 2020, n. 120).

Le funzioni del responsabile del procedimento sono infatti molteplici.

Costui svolge, anzitutto, un'essenziale funzione di "governo del procedimento", per quel che concerne l'organizzazione e la gestione dello stesso.

In particolare egli:

a) valuta, ai fini istruttori, le condizioni di ammissibilità, i requisiti di legittimazione ed i presupposti che siano rilevanti per l'emanazione di un provvedimento;

b) accerta di ufficio i fatti, disponendo il compimento degli atti all'uopo necessari, e adotta ogni misura per l'adeguato e sollecito svolgimento dell'istruttoria. In particolare, può chiedere il rilascio di dichiarazioni e la rettifica di dichiarazioni o istanze erronee o incomplete e può esperire accertamenti tecnici ed ispezioni ed ordinare esibizioni documentali;

c) propone l'indizione o, avendone la competenza, indice le conferenze di servizi.

Il responsabile del procedimento ha quindi funzioni istruttorie vere e proprie (lett. a) e b). Ma anche funzioni di impulso del procedimento (lett. c).

In secondo luogo, il responsabile del procedimento svolge un'importante funzione come soggetto interlocutore dei soggetti interessati al procedimento. Difatti il suo nominativo – come vedremo – è espressamente indicato nella comunicazione di avvio del procedimento, in modo che i soggetti interessati possano individuarlo, sin da subito, come il loro punto di riferimento. Questa è la ragione per cui, pure in ipotesi di procedimenti complessi articolati in subprocedimenti, deve ritenersi che, rispetto all'esterno, il responsabile debba essere di regola uno solo; mentre i responsabili di eventuali fasi e sub-procedimenti sono responsabili solo di fronte al responsabile: che ha appunto il ruolo essenziale di referente unico dell'amministrazione verso i cittadini.

La diversa tesi emersa a suo tempo in dottrina – nel senso di dovere privilegiare il riferimento ad una realtà caratterizzata da una struttura organizzativa disarticolata dell'Amministrazione Pubblica come argomento a favore dell'esistenza, in concreto, di più responsabili "esterni" (CERULLI IRELLI, 2008) – oltre a scontrarsi con la *ratio* stessa della previsione è stata smentita a più riprese dalla legislazione speciale: che prevede un responsabile unico anche con riferimento a procedimenti assai complessi e che si articolano in subprocedimenti. Così, ad esempio, all'art. 6 del D.P.R. n. 327/2001 in materia di espropriazione per pubblica utilità (D.P.R. 8 giugno 2001, n. 327, Testo unico delle di-

sposizioni legislative e regolamentari in materia di espropriazione per pubblica utilità). O, più di recente, all'art. 31 del Codice sugli Appalti Pubblici, che prevede il responsabile unico del procedimento (RUP) per l'affidamento di appalto e concessioni, il quale è identificato come il vero *dominus* della procedura di gara essendo titolare di tutti i compiti prescritti, «salve specifiche competenze affidate ad altri soggetti» (art. 31, comma 3, del D.Lgs. 18 aprile 2016, n. 50, Codice dei contratti pubblici). Come è stato peraltro chiaramente ribadito anche dalla giurisprudenza (Cons. Stato, sez. III, sentenza 2017, n. 132).

Infine, il responsabile del procedimento ha importanti funzioni decisorie: specifica infatti l'art. 6, lett. e), che il responsabile del procedimento «adotta, ove ne abbia la competenza, il provvedimento finale, ovvero trasmette gli atti all'organo competente per l'adozione», e che «L'organo competente per l'adozione del provvedimento finale, ove diverso dal responsabile del procedimento, non può discostarsi dalle risultanze dell'istruttoria condotta dal responsabile del procedimento se non indicandone la motivazione nel provvedimento finale».

Quest'ultimo alinea, che è stato introdotto ad opera della Legge n. 15/2005, non fa in realtà che confermare quegli indirizzi già ampiamente emersi in dottrina e in giurisprudenza. Ed ha l'effetto, da un lato, di confermare la centralità della fase istruttoria come momento di formazione e preparazione della decisione finale. Dall'altro, di porre l'accento, ancora una volta, sulla centralità del responsabile del procedimento. Egli è infatti il soggetto che governa una fase istruttoria dalle cui risultanze non è possibile discostarsi, se non con apposita e specifica motivazione.

Dopo avere illustrato rapidamente il suo ruolo ed i suoi compiti come identificati nella legislazione vigente, occorre a questo punto precisare che, in un contesto di Pubblica Amministrazione che faccia uso delle ICT per erogare (migliori) servizi ai cittadini e superare anche le distanze fisiche che impediscono talora ai cittadini di accedere ai servizi erogati, il ruolo del funzionario responsabile del procedimento non viene in alcun modo sminuito. Al contrario, in un "ambiente amministrativo" che sia dominato dall'utilizzo delle ICT appare evidente come questa figura possa giocare un ruolo ancora più centrale, sotto diversi profili.

In primo luogo, perché il funzionario responsabile del procedimento potrebbe rappresentare la figura chiave per tentare di colmare quel nuovo *gap* fra cittadini, che nella letteratura di settore è stato battezzato come divario digitale (*digital divide*, su cui si veda anche al capitolo VII, S. D'ANCONA, P. PROVENZANO).

Si tratta di quel complesso di disuguaglianze significative nell'accesso alle tecnologie dell'informazione e nella partecipazione a nuove forme di comunicazione e informazione che riguarda una parte piuttosto ampia dei cittadini: i cittadini più poveri, ma anche quelli più anziani (D. DONATI, 2005; G. PESCE, 2018).

Questo fenomeno non riguarda, come si potrebbe pensare, solo i Paesi del Terzo Mondo o quelli in via di sviluppo. l'Italia ha, in verità, consistenti problemi a questo riguardo; e ciò emerge chiaramente anche dall'Indice DESI (Indice di digitalizzazione dell'economia e della società, in https://ecommaeuropa.eu/digital-single-market/en/desi).

Questo documento, che fornisce una panoramica dei progressi compiuti dagli Stati membri UE nella digitalizzazione e dettagli sulle risposte politiche degli Stati membri per affrontare le sfide specifiche che questa comporta, per il 2019 colloca l'Italia al ventiquattresimo posto: seguita soltanto da Polonia, Grecia, Romania e Bulgaria. Questo poiché, sebbene l'utilizzo delle tecnologie digitali da parte delle aziende e la fornitura di servizi pubblici *online* si collochi in realtà vicino alla media degli altri Stati membri UE, risultano invece scarse le competenze digitali dei cittadini; e, soprattutto, è il divario tecnologico fra le varie fasce della popolazione ad essere il vero problema. I dati ISTAT (aggiornati al 6 aprile 2020) registrano, infatti, che nel periodo 2018-2019, il 33,8% delle famiglie non aveva computer o tablet in casa. Quanto all'uso di ed accesso a internet tra le famiglie italiane, i dati a fine dicembre 2019 registravano la permanenza di un forte divario digitale, da ricondurre soprattutto a fattori generazionali e culturali (questi dati e i relativi rapporti annuali sono facilmente reperibili sul sito dell'Istat al link: https://www.istat.it/it/archivio/internet).

Sicché, oltre che investire nella struttura digitale della Pubblica Amministrazione – acquisendo quegli strumenti che sono indispensabili per rendere effettiva la c.d. digitalizzazione della Pubblica Amministrazione, (v. capitolo VI, G. CARULLO) –, occorrerà altresì fornire alla Pubblica Amministrazione gli strumenti necessari per affrontare le sfide che questo divario digitale necessariamente comporta.

In questo senso, dato che al momento siamo ancora lungi dal dare concreta applicazione alla disposizione programmatica dell'art. 8 del Codice dell'Amministrazione digitale (CAD – D.Lgs. 7 marzo 2005, n. 82) sulla «Alfabetizzazione informatica dei cittadini», incombe alle singole Pubbliche Amministrazioni mettere i cittadini in grado di fruire di quei servizi che sono (e saranno in futuro) erogati con modalità digitali. E deve dunque essere compito del funzionario responsabile del procedimento accertarsi che i cittadini destinatari dei provvedimenti che fanno oggetto della sua attività dispongano degli strumenti a ciò necessari. In caso contrario, dovrà infatti essere lui a fungere da "punto di contatto" del cittadino con la Pubblica Amministrazione, anche eventualmente a distanza ed in maniera tale da evitare che il divario digitale si traduca, in ultima analisi, in un'attività amministrativa del tutto contraria ai contenuti basilari del diritto ad una buona amministrazione.

Evidentemente, questo implicherà la necessità di investire sulla figura del responsabile del procedimento: anche in termini di adeguata formazione di queste figure, che vanno necessariamente potenziate ed adeguatamente valorizzate. Viceversa, in uno scenario di amministrazione digitalizzata che fornisce i suoi servizi anche e soprattutto *online*, il diritto ad una buona amministrazione rischia di tragicamente infrangersi contro l'ostacolo rappresentato dall'assenza di strumenti ed abilità digitali proprio da parte di quei cittadini che più necessitano dei servizi erogati da parte delle Pubbliche Amministrazioni e che più dipendono dal rapporto con essa in termini non solo di benessere (inteso come miglioramento delle proprie condizioni di vita, nella prospettiva di J. RODRÍGUEZ-ARANA, 2013) ma, sovente, anche di vera e propria sopravvivenza.

D'altronde, la centralità della figura del responsabile del procedimento in un contesto di "buona amministrazione" è evidenziata chiaramente dalla sua menzione espressa nel contesto della Risoluzione del Parlamento europeo del 9 giugno 2016 per un'amministrazione europea aperta, efficace e indipendente (doc. 2016/2610(RSP), in https://www.europarl.europa.eu/doceo/document/TA-8-2016-0279_IT.html), il cui obiettivo è di arrivare a stabilire «una serie di norme procedurali che l'amministrazione dell'Unione dovrebbe rispettare nello svolgimento delle sue attività amministrative» (14° considerando della Risoluzione). Tali norme procedurali, intese appunto a garantire un'adeguata applicazione del diritto a una buona amministrazione, menzionano espressamente la figura del responsabile del procedimento all'art. 4, quello dedicato alle "definizioni". La lett. e) definisce infatti come «autorità competente: l'istituzione, l'organo o l'organismo, l'ufficio all'interno di essa oppure il titolare di una posizione all'interno dell'amministrazione dell'Unione che, secondo la legge applicabile, è responsabile del procedimento amministrativo».

Il che non fa che ribadire la estrema centralità di questa figura non solo nel quadro normativo nazionale, come si è visto, ma anche in un più ampio contesto di diritto amministrativo europeo.

In questa prospettiva, si rivela ovviamente d'importanza centrale la previsione inserita all'art. 3-*bis* della Legge n. 241/1990 dalla Legge n. 15/2005 ed ai sensi della quale: «Per conseguire maggiore efficienza nella loro attività, le Amministrazioni Pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati» (F. CARDARELLI, 2017). Essa si rivolge infatti, in primo luogo, al responsabile del procedimento: che può e deve avvalersene in un'ottica di efficiente gestione della fase istruttoria del procedimento amministrativo.

La previsione dell'art. 3-*bis* è stata peraltro oggetto di recente modifica, ad opera del D.L. n. 76/2020 (c.d. DL-semplificazioni – D.L. 16 luglio 2020, n.

76, Misure urgenti per la semplificazione e l'innovazione digitale, convertito con la Legge n. 120/2020) che ha sostituito il verbo "incentivano" con il verbo "agiscono" («agiscono mediante strumenti informatici e telematici») rendendo così chiaro che non si tratta di una previsione meramente programmatica. Da essa deriva un vero e proprio obbligo, in capo alle Pubbliche Amministrazioni ed allo scopo di conseguire maggiore efficienza, di agire mediante strumenti informatici e telematici. Ovviamente, però, nella misura in cui e per quanto tali strumenti siano effettivamente disponibili.

3. Un esempio concreto: il responsabile del procedimento all'epoca delle ICT quale elemento chiave del percorso verso una trasparenza reale ed effettiva

Per fornire un esempio concreto di come la figura del responsabile del procedimento possa rivestire importanza centrale nel percorso verso una Pubblica Amministrazione 4.0 – e rinviando ad altra parte di questo volume per la trattazione del tema generale (v. capitolo VIII, S. ROSSA) – mi limito qui ad osservare come la trasparenza non possa certo dirsi realizzata per il semplice fatto che la Pubblica Amministrazione abbia messo documenti e dati in suo possesso a disposizione dei cittadini. A tale scopo è infatti necessario che la Pubblica Amministrazione medesima metta anche a disposizione dei cittadini uno strumento di supporto, onde consentire loro di elaborare efficacemente l'enorme quantità di dati e informazioni messi così potenzialmente a disposizione (così D.-U. GALETTA, 2018b, p. 369 ss.).

L'Intelligenza Artificiale si rivela essere uno strumento molto importante a tale scopo e che possiede un notevole potenziale applicativo in questo ambito, consentendo di adattare la figura del responsabile del procedimento a questo specifico contesto ed alle specifiche problematiche che lo contraddistinguono.

In particolare, si potrebbe pensare qui di utilizzare un sistema di dialogo (*dialogue system*), o c.d. agente conversazionale: un assistente digitale, cioè, che funzioni tramite un sistema di riconoscimento del linguaggio naturale simile a quello, ad es., del sistema Siri di Apple.

Tale agente conversazionale potrebbe interfacciarsi col cittadino, supportandolo nella sua ricerca di quelle informazioni in possesso della Pubblica Amministrazione e che non siano sottratte al libero accesso per esigenze connesse alla tutela della privacy o di altri diritti fondamentali.

Per chiarire meglio l'aspetto tecnico della questione (su cui v. per tutti M. MCTEAR, Z. CALLEJAS, D. GRIOL BARRES, 2016), si tratterebbe di utilizzare, nella relazione cittadino-Pubblica Amministrazione finalizzata alla soddisfazione

delle istanze di apertura e trasparenza, un sistema di interfaccia intelligente che affiancherebbe il responsabile del procedimento. Ovverosia, un'interfaccia in grado di simulare il funzionamento del cervello umano, apprendendo in base al *feedback* ottenuto dall'ambiente circostante – e quindi dai cittadini-utenti, nel caso di specie – e declinata magari come interfaccia vocale conversazionale.

Quanto alla fattibilità in concreto, già oggi, grazie all'uso di sistemi di Intelligenza Artificiale più avanzati ed all'uso di tecniche di Intelligenza Artificiale più sofisticate rispetto a quelle della prima fase, come ad. es. le reti neurali artificiali profonde, possono essere generati dialoghi aperti: poiché le reti neurali artificiali già oggi sono in grado di modellare le conversazioni attraverso una previsione della frase successiva o della possibile risposta basata sulla conversazione precedente (v. J-C. HEUDIN, 2016 e J-C. HEUDIN, 2017).

Per il futuro, invece, la più sofisticata forma di applicazione di questi agenti di conversazione prevede un modello di dialogo con questi agenti conversazionali che combinerebbe anche il riconoscimento di scene e sentimenti con un modello di linguaggio naturale, includendo informazioni visive nella conversazione (immagini, oggetti, scene ed espressioni facciali diverse); e con l'obiettivo di rendere lo strumento maggiormente fruibile, in quanto capace di esprimere vere e proprie "emozioni" (R.W. PICARD, 2007).

Sebbene dunque, al momento attuale, l'uso di agenti di conversazione sia ancora molto embrionale, le utilità che potrebbero fornire questi sistemi vanno ben oltre la semplice assistenza. Questi supporti digitali potrebbero, infatti, rivelarsi essenziali per affrontare gli scenari di sovraccarico di informazioni generati dall'aumento esponenziale di dati e informazioni nel mondo digitale e le problematiche che ne scaturiscono nel rapporto cittadino-Pubblica Amministrazione (D.-U. GALETTA, 2018b, p. 159 ss.).

In concreto, si potrebbero immaginare sistemi di "assistenza ibrida", in cui l'utilizzo dell'Intelligenza Artificiale sotto forma di agente conversazionale si aggiungerebbe all'assistenza umana da parte del funzionario amministrativo responsabile del procedimento, consentendo così una riduzione dei costi della trasparenza e, soprattutto, trasformando la trasparenza da mero slogan in realtà concreta della relazione Pubblica Amministrazione-cittadino all'epoca dell'Amministrazione 4.0.

Ciò va evidentemente ben al di là di quanto di recente previsto nel DL-semplificazioni: il quale si limita a prevedere (modificando in tal senso l'art. 8, comma 2, lett. d), Legge n. 241/1990) che debbono essere comunicate ai destinatari della comunicazione di avvio del procedimento «le modalità con le quali, attraverso il punto di accesso telematico di cui all'articolo 64-bis del decreto legislativo 7 marzo 2005, n. 82 o con altre modalità telematiche, è possibile prendere visione degli atti, accedere al fascicolo informatico di cui all'arti-

colo 41 dello stesso decreto legislativo n. 82 del 2005 ed esercitare in via telematica i diritti previsti dalla presente legge» (art. 12, comma 1, lett. d), D.L. n. 76/2020, convertito con Legge n. 120/2020). Previsione che è peraltro completata da una lett. d-*bis*), la quale prevede (assai significativamente) che debba essere comunicato anche «l'ufficio dove è possibile prendere visione degli atti che non sono disponibili o accessibili con le modalità di cui alla lettera d)». L'unica misura, infatti, che il DL-semplificazioni mette in atto «Per superare il *digital divide* e avvicinare i cittadini all'uso delle tecnologie digitali» (l'espressione è contenuta nella Relazione Illustrativa al D.L. n. 76/2020) è che ai destinatari privi di un domicilio digitale l'avviso di avvenuta ricezione sia notificato, in formato cartaceo, a mezzo posta direttamente dal gestore della piattaforma, secondo le ordinarie modalità prevista dalla Legge n. 890/1982 sulle notificazioni a mezzo posta (v. art. 26, comma 7, del D.L. n. 76/2020, convertito con Legge n. 120/2020).

4. Digitalizzazione e comunicazione di avvio del procedimento

Nel Codice dell'Amministrazione digitale l'unico riferimento al responsabile del procedimento si trova nell'art. 41, comma 2: dove è precisato che «La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati». La norma prosegue precisando che (la pubblica amministrazione titolare del procedimento) «all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241».

Prima di passare all'analisi delle questioni legale all'intreccio fra digitalizzazione e diritti *ex* art. 10 Legge n. 241/1990 occorre dunque soffermarsi sulla comunicazione d'avvio che, come noto, è prevista dall'art. 7 della Legge n. 241/1990 sul procedimento amministrativo «ai soggetti nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti ed a quelli che per legge debbono intervenirvi». Nonché «a soggetti individuati o facilmente individuabili, diversi dai suoi diretti destinatari» (i c.d. "terzi interessati").

L'art. 7 prevede, in effetti, due sole eccezioni all'obbligo di comunicazione di avvio del procedimento: in generale, con riferimento all'adozione di provvedimenti tipici cautelari o di urgenza (art. 7, comma 2). E, in particolare, nelle ipotesi in cui, in concreto, «sussistano ragioni di impedimento derivanti da particolari esigenze di celerità del procedimento» (art. 7, comma 1). A quest'ultimo proposito, la giurisprudenza del Consiglio di Stato ha peraltro chiarito come non sia

sufficiente una qualsiasi urgenza per potere escludere l'obbligo di comunicazione di avvio, ma sia necessaria la sussistenza di circostanze particolari (urgenza qualificata), tali per cui la comunicazione comporterebbe una inevitabile compromissione dell'interesse pubblico al quale il provvedimento finale è rivolto (*ex multis* Cons. Stato, sez. IV, 25 marzo 1996, n. 368, in *Cons. Stato*, 1996, I, 398).

Oltre a queste due ipotesi di deroga previste dall'art. 7, vi è poi la deroga generale prevista dall'art. 13 della Legge n. 241/1990: che, più in generale, prevede la non applicabilità di tutte le disposizioni contenute nel capo III della Legge n. 241/1990 sulla partecipazione all'attività dell'Amministrazione diretta all'emanazione di atti normativi, atti amministrativi generali, di pianificazione e di programmazione, nonché procedimenti tributari, per i quali restano ferme le regole particolari che ne regolano la formazione. Nonché le altre deroghe eventualmente previste da leggi speciali di settore.

Accanto alle ipotesi di deroga espressamente previste dal legislatore, la giurisprudenza, nel corso del tempo, aveva tuttavia identificato fattispecie ulteriori di esclusione dall'obbligo di comunicazione d'avvio, ispirandosi alla regola del raggiungimento dello scopo e ad una lettura in chiave sostanzialista delle prescrizioni formali relative alla comunicazione di avvio del procedimento. Come è ormai noto, con la Legge n. 15/2005 tale indirizzo giurisprudenziale è stato accolto da legislatore è fatto proprio nella previsione dell'art. 21-*octies* Legge n. 241, comma 2, alinea 2, ai sensi del quale «Il provvedimento amministrativo non è comunque annullabile per mancata comunicazione dell'avvio del procedimento qualora l'amministrazione dimostri in giudizio che il contenuto del provvedimento non avrebbe potuto essere diverso da quello in concreto adottato».

In modo niente affatto coerente, tuttavia, la stessa Legge n. 15/2005 ha parallelamente integrato la previsione dell'art. 8 Legge n. 241 relativa ai contenuti della comunicazione di avvio. Prevedendo che, oltre all'amministrazione competente, all'oggetto del procedimento promosso, all'ufficio e alla persona responsabile del procedimento, all'ufficio in cui si può prendere visione degli atti, debbano venire comunicati anche la data entro la quale, deve concludersi il procedimento e i rimedi esperibili in caso di inerzia dell'amministrazione; e, nei procedimenti ad iniziativa di parte, la data di presentazione della relativa istanza. Inoltre, il D.L. n. 76/2020 prevede ora che debba essere comunicato anche il domicilio digitale dell'amministrazione (art. 12, comma 1, lett. d) par. 1, D.L. n. 76/2020, convertito con Legge n. 120/2020, che integra l'art. 8, comma 2, della Legge n. 241/1990).

Si tratta di importanti integrazioni rispetto al contenuto della comunicazione d'avvio, che confermano la sua lettura in una logica di strumento finalizzato all'instaurazione del contraddittorio; e con la stessa funzione che è riconosciuta all'atto di citazione nel processo civile e all'informazione di garanzia in quello penale.

Il che nettamente contrasta, però, con quella visione sostanzialistica degli adempimenti procedurali accolta nell'art. 21-*octies* della stessa Legge n. 241/1990. Tale previsione si fa infatti essenzialmente carico delle difficoltà pratiche e dei costi lamentati dalle Pubbliche Amministrazioni rispetto ad una comunicazione di avvio operata in modo "tradizionale". È infatti noto che il comma 1 dell'art. 8 parla di «comunicazione personale» e prevede la possibilità di ricorso a «forme di pubblicità idonee di volta in volta stabilite dall'amministrazione medesima» solo quando il numero di destinatari sia tale che la comunicazione personale diventi impossibile o particolarmente gravosa.

Si ritiene, tuttavia, che in uno scenario di amministrazione digitalizzata molte delle problematiche pratiche tradizionalmente connesse alla comunicazione di avvio del procedimento potrebbero trovare una più facile soluzione.

In primo luogo, l'uso di tecnologie ICT potrebbe facilitare all'amministrazione l'individuazione di eventuali "terzi interessati".

In secondo luogo, e nella prospettiva dei principi di efficienza ed economicità dell'azione amministrativa, l'uso di tecnologie ICT potrebbe consentire, se non un vero e proprio azzeramento, certamente una riduzione consistente dei tempi e dei costi sinora connessi all'espletamento di questo adempimento (stampa, imbustamento, invio postale, ecc.). A fronte, ovviamente, di un investimento iniziale per acquisire ed impostare le tecnologie appropriate e formare i pubblici dipendenti al loro corretto utilizzo.

A questo proposito in dottrina è stato giustamente osservato (A. MASUCCI, 2011, p. 24) come l'obbligo di comunicare l'avvio del procedimento all'indirizzo di posta elettronica certificata sussista certamente con rispetto a coloro che abbiano usato quest'ultima per inviare un'istanza di avvio del procedimento. Si deve aggiungere qui che, indipendentemente da questo caso specifico, nel quale l'invio all'indirizzo di posta elettronica appare come una conseguenza evidente di quanto previsto negli artt. 6 ss. del CAD, sarebbe necessario (ed opportuno) prevedere modalità di automazione dell'invio della comunicazione di avvio del procedimento in tutti casi: con invio della stessa al domicilio digitale del destinatario della comunicazione (in argomento v. capitolo VII, S. D'ANCONA e P. PROVENZANO, spec. par. 3.). E ciò con riguardo sia ai diretti interessati, che agli intervenienti necessari in qualunque procedimento.

Questa pare peraltro essere la direzione imboccata dal recente D.L. n. 76/2020, che introduce rilevanti novità al riguardo. In particolare, l'art. 26 del D.L. definisce le modalità di funzionamento della piattaforma digitale tramite cui le pubbliche amministrazioni possono notificare i propri atti, provvedimenti, avvisi e comunicazioni a cittadini e imprese (su cui v. capitolo VI, S. D'ANCONA).

L'istituzione della piattaforma in questione (piattaforma per la notificazione digitale degli atti della Pubblica Amministrazione) era peraltro prevista già

dall'art. 1, comma 402, della Legge 27 dicembre 2019, n. 160, che affida il suo sviluppo, tramite Poste Italiane Spa e con il riutilizzo di infrastrutture tecnologiche esistenti, alla società PagoPA Spa.

A questo riguardo l'obiettivo del D.L. n. 76/2020 è infatti di semplificare, attraverso l'uso delle tecnologie e in coerenza con gli obiettivi dell'agenda digitale, l'attività dell'amministrazione di notificazione degli atti, provvedimenti, avvisi e comunicazioni, redendoli al contempo maggiormente accessibili ai destinatari. In questa prospettiva un ruolo importante dovrebbero svolgerlo strumenti informatici e telematici quale la AppIO e/o i c.d. "sistemi di avvisatura digitale" (a questo proposito si vedano le modifiche apportate dal D.L. n. 76/2020 all'art. 64-*bis* del CAD e tese a consolidare la natura dell'AppIO, quale punto di accesso telematico ai servizi pubblici).

Si ritiene, tuttavia, che pure in uno scenario quale quello ipotizzato dal DL-semplificazioni (e nel quale l'importanza del possesso di un indirizzo di posta elettronica certificata a fini della possibilità di eleggere un domicilio digitale verrebbe, in ipotesi, a ridursi) sarebbe senz'altro opportuno prevedere degli investimenti appositi finalizzati a ripristinare anche la possibilità di assegnazione gratuita di un indirizzo di posta elettronica certificata (eleggibile quale domicilio digitale) a tutti quei cittadini che lo richiedano. In linea con quanto era stato originariamente previsto dall'art. 16-*bis*, comma 5 ss., del D.L. n. 185/2008 (convertito in Legge 28 gennaio 2009, n. 2). All'art. 2 del decreto si statuiva infatti che «ai cittadini che ne fanno richiesta il Dipartimento per l'innovazione e le tecnologie [ora denominato Dipartimento per la digitalizzazione della Pubblica Amministrazione e l'innovazione tecnologica a norma del D.P.C.M. del 28 aprile 2009], direttamente o tramite l'affidatario del servizio, assegna un indirizzo di posta elettronica certificata». Il D.P.C.M. del 6 maggio 2009 aveva poi definito le modalità per il rilascio della casella PEC (CEC-PAC) ai cittadini, che poteva essere utilizzata solo per comunicazioni verso la PA. Tuttavia, a fronte degli alti costi legati all'erogazione di tale servizio e con la motivazione di un loro scarso utilizzo (v. https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2014/12/17/chiude-cec-pac-arrivo-solo-standard-posta-certificata), tale possibilità di ottenimento di un indirizzo gratuito di Postacertificat@ (CEC-PAC) è venuta meno a fine 2014 (dal 18 Dicembre 2014 il servizio non è più attivabile!). Sicché, attualmente il servizio di posta elettronica certificata (PEC) è disponibile solo a pagamento, presso i gestori PEC autorizzati dall'Agenzia per l'Italia Digitale (Agid). Con la sola eccezione, del tutto peculiare, del domicilio digitale «valido unicamente per il ricevimento di comunicazioni e notifiche» che, come misura accessoria rispetto all'erogazione della sanzione prevista all'art. 37 per la mancata attivazione del domicilio digitale o per la sua cancellazione, verrà assegnato gratui-

tamente all'imprenditore da parte dell'ufficio del registro delle imprese presso il cassetto digitale dell'imprenditore. Questo in base alla modifica introdotta all'art. 37 dalla legge di conversione del DL-semplificazioni

5. Digitalizzazione e decisione imparziale ed equa

Il primo comma dell'art. 41 CDUE statuisce che «Ogni persona ha diritto a che le questioni che la riguardano siano trattate in modo imparziale ed equo (…) dalle istituzioni, organi e organismi dell'Unione».

Sul primo aspetto, quello dell'imparzialità, si tratta di una giurisprudenza dei giudici comunitari del tutto (e ormai da tempo) consolidata; ed alla quale gli stessi redattori della Carta di Nizza fanno espresso riferimento nelle spiegazioni allegate alla Carta medesima (Testo delle spiegazioni relative al testo completo della Carta, pubblicate nella Gazzetta ufficiale dell'Unione Europea C-303/17 del 14.12.2007 e reperibili in http://www.europarl.europa.eu/charter/pdf/04473_it.pdf).

Questa giurisprudenza (v. per tutte Corte giust., sentenza 21 novembre 1991, in causa C-269/90, *Technische Universität München c. Hauptzollamt München-Mitte*, ECLI:EU:C:1991:438, punto 14) ha precisato che, presupposto di una decisione imparziale che sia espressione del principio di buona amministrazione, è che siano presi in considerazione «tutti gli elementi di fatto e di diritto disponibili al momento dell'adozione dell'atto», poiché sussiste l'obbligo di predisporre la decisione «con tutta la diligenza richiesta e di adottarla prendendo a fondamento tutti i dati idonei ad incidere sul risultato» (Tribunale UE, sentenza 19 marzo 1997, in causa T-73/95, *Oliveira c. Commissione*, ECLI:EU:T:1997:39, punto 32).

Quanto al termine equità, questo può assumere un duplice significato nel diritto amministrativo: quello di equità sostanziale e quello di equità procedurale. Ed è a questa seconda accezione del termine che si riferisce specificamente l'art. 41 CDUE, il quale sottende l'idea di una Pubblica Amministrazione in grado di offrire ai cittadini tutte quelle garanzie di contraddittorio, difesa, accesso ai documenti, motivazione delle decisioni, ecc., che sono elencate nel successivo comma 2 dell'art. 41 CDUE medesimo.

Ciò emerge chiaramente anche da una recente sentenza della Corte di giustizia, in cui si fa espresso riferimento alla necessità che, qualora la Commissione decida di utilizzare modelli econometrici nell'ambito di procedure di controllo delle operazioni di concentrazione, «le parti notificanti vengano messe in condizione di far conoscere le proprie osservazioni al riguardo», poiché «La divulgazione di questi modelli e delle scelte metodologiche sottese al-

la loro elaborazione (…) contribuisce (…) a conferire al procedimento il suo carattere equo, in conformità del principio di buona amministrazione enunciato all'articolo 41 della Carta dei diritti fondamentali dell'Unione europea» (Corte giust., sentenza 16 gennaio 2019, in causa C 265/17P, United Parcel Service, ECLI:EU:C:2019:23, punto 33 s.).

Questi arresti giurisprudenziali richiamano ovviamente l'attenzione sull'importanza di un'istruttoria adeguata del procedimento. Il che, ove si abbia riguardo ad uno scenario caratterizzato dalla disponibilità di tecnologie ICT, sposta l'attenzione sulla necessità di fare uso di tutti quegli strumenti che consentono, oggi, alle Pubbliche Amministrazioni, di acquisire facilmente non solo documenti (per il che si rinvia al tema delle Banche dati e della loro interconnessione, di cui al capitolo VI, G. CARULLO), ma anche informazioni tratte da sensori e strumenti di monitoraggio di vario tipo (sul che si rinvia invece al capitolo IV, R. CAVALLO PERIN e I. ALBERTI).

Quanto sin qui osservato vale, evidentemente, anche ove si abbia riguardo alla prima accezione di equità, quella di equità sostanziale: che è infatti connessa ai concetti di giustizia e proporzionalità dell'azione amministrativa. Con il che il diritto ad un trattamento equo delle proprie questioni da parte dell'Amministrazione trova un collegamento anche con il più generale divieto, posto dai Trattati UE, di operare trattamenti discriminatori. Il principio di uguaglianza, infatti, oltre a presupporre un dovere di imparzialità della Pubblica Amministrazione, presuppone altresì un dovere dell'Amministrazione di astenersi da comportamenti che risultino contrari al principio di giustizia e che, come tali, verrebbero senz'altro a rappresentare una violazione del dovere di garantire un equo trattamento.

A quest'ultimo proposito occorre fare riferimento ad un altro nesso, ed in questo caso non necessariamente positivo, fra Pubbliche Amministrazioni, ICT e decisione imparziale ed equa. Se non fosse infatti possibile giungere ad un'organizzazione dell'attività amministrativa che fa uso delle ICT tale da consentire il superamento del divario digitale di cui già si è detto (par. 2, *supra*), sarebbe infatti fortemente messo in discussione il rispetto di questi due importanti principi, che integrano il diritto ad una buona amministrazione, ma che sono anche oggetto di menzione espressa nell'art. 97 Cost.

Sotto questo profilo, come già si è detto, la soluzione primaria consiste nello sfruttare appieno tutte le potenzialità insite nella figura del responsabile del procedimento: il cui compito, in uno scenario digitale, assume un'importanza che va ovviamente bel al di là di quel che concerne l'obbligo, statuito dall'art. 41 CAD, di predisporre il c.d. "fascicolo informatico" (su cui si rinvia al capitolo V, S. D'ANCONA).

Il responsabile del procedimento dovrebbe infatti farsi "garante in concreto"

del rispetto dei principi di equità ed imparzialità nella fase istruttoria del procedimento in uno scenario di amministrazione digitalizzata. Da un lato, adottando soluzioni organizzative concrete che permettano di evitare discriminazioni fra cittadini in ragione del diverso livello di "alfabetizzazione informatica" e della diversa disponibilità di strumenti informatici (e di un collegamento alla rete). Dall'altro lato, evitando che, in particolare allorquando la Pubblica Amministrazione faccia ricorso all'uso di algoritmi di Intelligenza Artificiale nella fase istruttoria del procedimento, essa possa operare discriminazioni fra diverse categorie di cittadini nascondendosi dietro il paradigma della c.d. neutralità dell'algoritmo.

A quest'ultimo proposito occorre infatti precisare che, se deve senz'altro consentirsi alle Pubbliche Amministrazioni – nel quadro della loro potestà autorganizzatoria (A. MASUCCI, 1993; F. COSTANTINO, 2012; F. COSTANTINO, 2016) – di fare ricorso agli strumenti messi oggi a disposizione dalle ICT, ove questi si rivelino idonei allo scopo di garantire un'istruttoria più completa e maggiormente corrispondente ai principi di imparzialità e buon andamento, è altresì necessario che ciò avvenga nel rispetto del principio di trasparenza, inteso anzitutto nei termini di piena conoscibilità e dell'esistenza di eventuali processi decisionali automatizzati e dell'algoritmo (D.-U. GALETTA, 2020 – v. anche *infra* par. 11).

Questo è necessario a maggior ragione oggi dopo l'avvenuta introduzione – ad opera della Legge n. 120/2020 di conversione del DL-semplificazioni – di un comma 2-*bis* nell'art. 1 della Legge n. 241/1990 sul procedimento amministrativo, ai sensi del quale «I rapporti tra il cittadino e la pubblica amministrazione sono improntati ai principi della collaborazione e della buona fede».

6. Digitalizzazione e decisione entro un termine ragionevole

Il primo comma dell'art. 41 CDUE specifica che, oltre ad essere trattate in modo imparziale ed equo, «Ogni persona ha diritto a che le questioni che la riguardano siano trattate (…) entro un termine ragionevole».

La ragion d'essere di questa previsione era stata ben sottolineata dall'avvocato generale *Mischo*, in sue conclusioni del 2001, nelle quali aveva sottolineato che, «il fatto di esigere che l'amministrazione prenda posizione entro un termine ragionevole è già acquisito in diritto comunitario»; e la sua ragion d'essere va identificata nella «esigenza di tutelare gli operatori da un'incertezza giuridica protratta» (Conclusioni del 25 ottobre 2001, in causa C-244/99P, DSM, ECLI:EU:C:2001:575, punto 83 s.).

Già prima dell'adozione della Carta dei diritti la giurisprudenza comunitaria aveva infatti, da tempo, riconosciuto che quello della decisione entro un termine ragionevole era un principio generale del diritto comunitario, fondato

sul presupposto che «un'amministrazione lenta è una cattiva amministrazione» (così ricorda l'Avv. gen. Jacobs, nelle sue conclusioni del 22 marzo 2001, in causa C-270/99, Z, ECLI:EU:C:2001:180, punto 40. Nello stesso senso si veda ad es. la sentenza Corte Giust., 28 marzo 1997, in causa C-282/95P, Guerin, ECLI:EU:C:1997:159, punto 37).

Quanto a che cosa debba intendersi per termine ragionevole, nella giurisprudenza dei Tribunali UE di Lussemburgo è chiaramente messo in evidenza come la sua ragionevolezza vada valutata caso per caso e tenendo adeguatamente in conto le peculiarità di ogni singolo procedimento. Sicché, nella prospettiva del diritto ad una buona amministrazione *ex* art. 41 CDUE, è da respingersi l'idea del «termine unico di riferimento rispetto al quale andrebbe valutato qualunque procedimento, indipendentemente dalle sue caratteristiche»; poiché, si osserva, «solo un'impostazione casistica può consentire di applicare concretamente il principio del termine ragionevole» nella misura in cui, diversamente ragionando, l'amministrazione procedente «si vedrebbe costretta ad istruire i procedimenti entro termini che non le consentirebbero di pervenire ad una decisione finale corretta» (Conclusioni dell'Avv. gen. Mischo, in causa C-244/99P cit., punto 139 ss.).

Nella prospettiva di combattere la lentezza dell'azione amministrativa, pur garantendo che si addivenga ad una decisione finale il più possibile corretta, in quanto basata su una istruttoria adeguata, è evidente come il ricorso alle tecnologie ICT possa rivelarsi essenziale.

Questo risultato può infatti raggiungersi, da un lato attraverso l'efficientamento della fase istruttoria grazie all'istanza telematica (su cui si rinvia al capitolo IV, di R. CAVALLO PERIN, I. ALBERTI) e allo sportello unico telematico (di cui si dirà nel prossimo par. 7.).

Dall'altro lato, il risultato di una maggiore rapidità della fase istruttoria del procedimento, pur senza rinunciare all'adeguata estensione dell'attività istruttoria stessa, può raggiungersi tramite l'uso, in questo contesto, di sistemi di Intelligenza Artificiale. Molte delle attività di gestione di informazioni e dati compiute dalla Pubbliche Amministrazioni nella fase istruttoria del procedimento amministrativo possono infatti essere facilmente standardizzate e si prestano dunque a processi di automazione, posti in essere attraverso l'uso di sistemi di Intelligenza Artificiale, appunto (D.-U. GALETTA, J.G. CORVALÁN, 2019).

L'automazione tramite l'introduzione di sistemi di Intelligenza Artificiale di tipo debole (non predittiva) in quella parte della fase istruttoria del procedimento che consiste essenzialmente nella gestione dei dati e dei documenti in possesso delle Pubbliche Amministrazioni (che andrebbero ovviamente previamente digitalizzati e resi interoperabili – v. capitolo 6, G. CARULLO) consentirebbe dunque, già di per sé, un'evidente accelerazione complessiva del-

l'attività amministrativa ed un efficientamento della macchina burocratico-amministrativa. Se a questo si unisse, poi, la *Big Data Analysis* a fini di ulteriore accrescimento della capacità conoscitiva, la funzione conoscitiva della Pubblica Amministrazione (F. LEVI, 1967), pur se molto potenziata dall'analisi dei *Big Data*, diventerebbe di gran lunga più efficace ed efficiente, ma rimarrebbe sostanzialmente sempre la medesima. Essa cambierebbe, invece, radicalmente la sua natura nel momento in cui si introducesse, come è di certo possibile fare oggi, anche l'utilizzazione di strumenti di Intelligenza Artificiale predittiva (o forte che dir si voglia) nel contesto della fase istruttoria del procedimento (sul che si rinvia al capitolo IV, di R. CAVALLO PERIN, I. ALBERTI).

Tutto questo si affiancherebbe, ovviamente, a quanto già previsto dal nostro CAD: che, per accelerare i tempi delle interazioni fra le varie amministrazioni all'interno del procedimento già prevede che «Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa» (art. 47, comma 1, CAD).

7. *Segue.* Lo sportello unico telematico e l'istanza telematica

Come si è già anticipato, uno strumento di grande efficientamento della fase istruttoria grazie alle ICT è rappresentato dalla istanza telematica e dallo sportello unico telematico. A tale proposito, l'art. 10 del nostro CAD prevedeva infatti, al suo comma 1, che lo sportello unico per le attività produttive (c.d. SUAP), di cui all'art. 38, comma 3, del D.L. 25 giugno 2008, n. 112 (convertito, con modificazioni, dalla Legge 6 agosto 2008, n.133) «eroga i propri servizi verso l'utenza in via telematica». Tale previsione è stata successivamente abrogata dal D.Lgs. 26 agosto 2016, n. 179 (che ha anche introdotto lo Sportello unico amministrativo presso l'Autorità di sistema portuale – art. 18 del D.Lgs. n. 179/2016) e non compare dunque più nella versione del CAD attualmente in vigore. Tuttavia, ed in conformità con quanto previsto dal D.Lgs. 26 marzo 2010, n. 59 (emanato ai fini del recepimento della cosiddetta Direttiva Bolkestein, n. 2006/123/CE), l'istituzione dei SUAP telematici rimane, ed è di competenza dei Comuni, che possono crearli in forma singola o associata tra più Comuni.

Il servizio è attualmente disponibile presso gli oltre 3.500 comuni che si avvalgono del sistema telematico SUAP delle Camere di Commercio Italiane. Il D.P.R. del 7 settembre 2010, n. 160, con cui si è adottato il Regolamento per la semplificazione ed il riordino della disciplina sul SUAP, ha affidato infatti alle Camere di Commercio il compito di realizzare il portale impresainungiorno.gov.it, attraverso il quale è possibile accedere alla rete nazionale degli Sportelli SUAP.

La stessa norma ha anche previsto che, per i Comuni che non disponessero ancora della strumentazione informatica e telematica richiesta per il corretto funzionamento degli Sportelli, le Camere di commercio dovessero prestarsi a svolgere le funzioni di accettazione delle pratiche informatiche destinate al SUAP di tali Comuni.

Attualmente, dunque, il SUAP è l'unico soggetto pubblico di riferimento territoriale per tutti i procedimenti che abbiano ad oggetto l'esercizio di attività produttive e di prestazione di servizi, e per quelli relativi alle azioni di localizzazione, realizzazione, trasformazione, ristrutturazione o riconversione, ampliamento o trasferimento, nonché cessazione o riattivazione delle "attività produttive": cioè delle attività di produzione di beni e servizi, incluse le attività agricole, commerciali e artigianali, le attività turistiche e alberghiere, i servizi resi dalle banche e dagli intermediari finanziari e i servizi di telecomunicazioni (art. 2, comma 1, D.P.R. n. 160/2010).

È parimenti previsto che «Le domande, le dichiarazioni, le segnalazioni e le comunicazioni concernenti le attività di cui al comma 1 ed i relativi elaborati tecnici e allegati sono presentati *esclusivamente* in modalità telematica» (art. 2, comma 2, D.P.R. n. 160/2010). E che anche la trasmissione della documentazione alle altre amministrazioni che intervengono nel procedimento da parte del SUAP è attuata con modalità telematiche di ricevimento e di trasmissione (trasmissione telematica tra enti, art. 2, comma 3, D.P.R. n. 160/2010 – v. capitolo V, S. D'ANCONA).

Obiettivo dell'istituzione del SUAP è di garantire anche per l'ipotesi di procedimenti paralleli (in cui, cioè, lo svolgimento di una determinata attività sia subordinata all'ottenimento di diversi provvedimenti amministrativi) che vi sia unicità e univocità dell'interlocutore. A questo proposito, nel D.P.R. n. 160/2010 è infatti previsto che «Il SUAP assicura al richiedente una *risposta telematica unica e tempestiva* in luogo degli altri uffici comunali e di tutte le amministrazioni pubbliche comunque coinvolte nel procedimento, ivi comprese quelle preposte alla tutela ambientale, paesaggistico-territoriale, del patrimonio storico-artistico o alla tutela della salute e della pubblica incolumità» (art. 4, comma 1, D.P.R. n. 160/2010). Ed è parimenti previsto un "Divieto di gestioni alternative", consistente nel fatto che tutte le comunicazioni al richiedente debbono essere «trasmesse esclusivamente dal SUAP» (art. 4, comma 2, D.P.R. n. 160/2010).

Se le attività di cui all'art. 2, comma 1, D.P.R. n. 160/2010 sono soggette alla disciplina della Segnalazione Certificata di Inizio Attività (SCIA) è previsto che anche questa debba essere trasmessa al SUAP, il quale «verifica, con modalità informatica, la completezza formale della segnalazione e dei relativi allegati» e «Se la verifica è positiva, rilascia automaticamente la ricevuta e trasmet-

te immediatamente in via telematica la segnalazione e i relativi allegati alle amministrazioni e agli uffici competenti» (art. 5 D.P.R. n. 160/2010).

Lo schema qui sotto riportato è utile a riassumere le differenze, per l'ipotesi di presentazione di un'istanza di rilascio di autorizzazione che ricada nell'ambito di applicazione della disciplina SUAP, fra il precedente contesto (di classica amministrazione "cartacea") e l'attuale contesto, in cui l'amministrazione è tenuta a fare uso delle ICT.

AMMINISTRAZIONE TRADIZIONALE	**AMMINISTRAZIONE CHE FA USO DELLE ICT**
L'istanza e gli allegati erano compilati su moduli di carta.	L'istanza e gli allegati sono compilati su moduli digitali.
Allegati cartacei in una o più copie, a seconda della necessità di trasmettere l'istanza ad altri enti.	Allegati digitali, in copia unica.
Il richiedente e gli altri soggetti coinvolti apponevano ai documenti la propria firma autografa.	Il richiedente e gli altri soggetti coinvolti appongono ai documenti la propria firma digitale.
La documentazione veniva inviata al SUAP per raccomandata o presentata all'ufficio protocollo del Comune.	La documentazione viene trasmessa al SUAP via Applicazioni Web oppure via PEC.
Il SUAP inoltrava la documentazione agli enti interessati per raccomandata.	Il SUAP inoltra la documentazione agli enti interessati via PEC.
Il protocollo del SUAP protocolla in modo cartaceo l'istanza.	Il protocollo del SUAP protocolla digitalmente l'istanza.
Le comunicazioni erano firmate con firma autografa e spedite al richiedente per raccomandata.	Le comunicazioni sono firmate digitalmente e spedite al richiedente via PEC.

8. *Segue.* L'Unione Europea e il "portale digitale unico"

In Italia, come si è visto, per il momento, esistono sportelli unici solo nei comuni; oppure solo in taluni ambiti settoriali (ad es. lo Sportello unico do-

ganale e lo Sportello unico amministrativo presso l'Autorità di sistema portuale).

L'Unione Europea, per parte sua, si è mossa però chiaramente nella direzione del portale *digitale* unico quale elemento chiave della sua strategia per il mercato unico (v. la Strategia per il mercato unico digitale in Europa e la Comunicazione della Commissione del 28 ottobre 2015 intitolata «Migliorare il mercato unico: maggiori opportunità per i cittadini e le imprese»). Nel dicembre 2018 è stato infatti approvato il Regolamento 2018/1724/UE, che prevede la creazione di un portale digitale unico (*Single Digital Gateway*) a disposizione dei cittadini come portale unico di accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi, a partire dal dicembre 2020 (così prevede l'art. 39, entrata in vigore, del Regolamento 2018/1724/UE).

Questo portale digitale unico – a cui fa ora riferimento anche il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022 licenziato nel mese di luglio 2020 (v. in https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2020/08/12/il-piano-triennale-linformatica-nella-pa-2020-2022, p. 11 ss.) – dovrà fungere «da punto di ingresso unico mediante il quale i cittadini e le imprese possano accedere alle informazioni sulle norme e sui requisiti che devono soddisfare in virtù del diritto dell'Unione o nazionale», con l'obiettivo non solo di «semplificare il contatto di cittadini e imprese con i servizi assistenza e di risoluzione dei problemi istituiti a livello nazionale o di Unione, migliorandone l'efficacia», ma anche di «agevolare l'accesso e il completamento delle procedure in linea» (Considerando 12 del Regolamento 2018/1724/UE).

In quest'ultima prospettiva appare specialmente rilevante la previsione dell'art. 6 del Regolamento, che impone agli Stati membri di consentire l'espletamento di una serie di procedure «interamente in linea». L'obiettivo è rendere operativa, entro il 2023, la possibilità di gestire *online* più di 20 procedure amministrative, tra cui i certificati di nascita, le dichiarazioni dei redditi e le iscrizioni all'università.

Questa tendenza alla creazione in ogni ambito di portali/sportelli digitali unici, se da un lato favorisce l'efficienza e la maggior celerità dell'azione amministrativa, nella prospettiva anche del rispetto del termine ragionevole per l'adozione della decisione di cui all'art. 41 CDUE, dall'altro lato essa implica, però, anche l'esigenza di rivisitare nozioni e postulati che acquisiscono tutta un'altra dinamica in un contesto organizzativo dominato dalle ICT. Questo accade, ad esempio, con i principi di cooperazione, di collaborazione, di coordinamento e di decentramento. I principi del decentramento e del coordinamento nel campo dell'organizzazione amministrativa perdono, infatti, di rilevanza a fronte delle forme di organizzazione amministrativa che sono necessi-

tate dall'introduzione del modello del portale/sportello digitale unico. Mentre assumono, invece, rilevanza ancora maggiore i principi di cooperazione e di collaborazione.

9. Digitalizzazione e diritto di ogni persona di essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale che le rechi pregiudizio

Il comma 2 dell'art. 41 CDUE, nel concretizzare gli elementi essenziali di quel diritto ad un trattamento equo ed imparziale ed entro un termine ragionevole statuito dal primo comma, menziona, anzitutto, «il diritto di ogni persona ad essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale che le rechi pregiudizio».

Si tratta di una delle garanzie centrali connesse al diritto ad una buona amministrazione e che non rappresenta, tuttavia, affatto una novità per il diritto UE. Essa era infatti oggetto di menzione espressa già in diverse norme di diritto UE secondario antecedenti all'adozione della CDUE, da cui la giurisprudenza ha ricavato quel principio generale trasformato poi in diritto nell'art. 41 CDUE.

Quanto ai contenuti specifici di questo diritto, per la giurisprudenza UE occorre anzitutto che il destinatario del provvedimento sia «messo in condizione di far conoscere utilmente il proprio punto di vista sugli elementi presi in considerazione» (Corte giust., sentenza 29 giugno 1994, in causa C-135/92, *Fiskano c. Commissione*, ECLI:EU:C:1994:267, punto 40); e, nel concreto, si tratta del suo diritto ad esprimere la propria opinione su tutti gli elementi di fatto e di diritto rilevanti (ad es. Tribunale UE, sentenza 06 dicembre 1994, in causa T-450/93, Lisertal, ECLI:EU:T:1994:290, punto 42).

Quale presupposto essenziale per l'esercizio del diritto di essere ascoltati vi è naturalmente – al pari di quanto avviene nel nostro diritto amministrativo nazionale – il diritto di essere informati dell'avvio del procedimento, cui ovviamente corrisponde il dovere dell'Amministrazione di informare i soggetti interessati (su cui già *supra* par. 3): dovere che rappresenta una delle componenti essenziali anche del diritto di essere ascoltati *ex* art. 41 CDUE.

A conferma dell'importanza del diritto di essere ascoltati la giurisprudenza UE ha a più riprese sottolineato come, nell'adottare la sua decisione finale, l'Amministrazione potrà tenere conto soltanto di quegli elementi sui quali sia stato possibile per l'interessato esprimere la sua opinione (così già Corte giust., sentenza 15 luglio 1970, in causa 45/69, *Firma Böhringer Mannheim GmbH c. Commissione*, ECLI:EU:C:1970:73, punto 9).

L'ambito di applicazione del diritto di essere ascoltati non è, tuttavia, sem-

pre identico: esso può variare nei suoi contenuti concreti a seconda delle circostanze e, in taluni casi, può venire addirittura meno del tutto, essendo dipendente anche dalla natura del provvedimento che si vuole adottare. Maggiore è, infatti, il margine di apprezzamento discrezionale dell'Amministrazione procedente, maggiore sarà lo spazio da concedere alla partecipazione (Corte giust., sentenza 21 novembre 1991, in causa C-269/90 cit., punto 14). Ma è anche l'impatto concreto del provvedimento sulle posizioni giuridiche del destinatario a giocare un ruolo centrale rispetto all'estensione in concreto del diritto di essere ascoltati (Cfr., ad es., Corte giust., sentenza 28 maggio 1980, in cause riun. 33 e 75/79, *Kühner c. Commissione*, ECLI:EU:C:1980:139, punto 25).

In perfetta coerenza con quanto è normalmente previsto a tale riguardo anche dalle discipline normative nazionali, vi è peraltro un caso nel quale il diritto di essere ascoltati può venire meno del tutto secondo la giurisprudenza dei giudici UE: quando il suo esercizio comporti il rischio di successiva distruzione od occultamento di documenti che siano indispensabili ai fini dell'espletamento dell'attività istruttoria stessa (v. le conclusioni dell'Avv. gen. Warner del 30 aprile 1980, in causa 136/79, National Panasonic, ECLI:EU:C:1980:119, relativa ad un'indagine in materia di concorrenza).

Infine, nella giurisprudenza UE si è fatto talora riferimento anche ad esigenze di efficienza dell'Amministrazione quale ragione che potrebbe giustificare una restrizione (o, addirittura, una eliminazione) del diritto in questione. Si tratta, per il vero, di eccezioni. Ma, sebbene in dottrina si fossero espresse forti perplessità rispetto a quest'ultima categoria di possibili eccezioni (v. D.-U. GALETTA, 2020), la giurisprudenza più recente ha purtroppo confermato questo orientamento nella prospettiva di «un interesse di semplificazione amministrativa e di gestione efficace della procedura» (Corte giust., sentenza 3 luglio 2014, in causa C-129/13, Kamino International Logistics, ECLI:EU:C:2014:2041, punto 42 ss.).

Tuttavia, questa è proprio l'ipotesi in cui potrebbe esservi un decisivo apporto da parte delle ICT: perché se, come nel caso *Kamino*, l'esigenza primaria è quella di non compromettere l'effetto utile del codice doganale (così punto 77 sent. *Kamino International Logistics* cit.), resta pur sempre anche l'esigenza di garantire che l'istruttoria non sia un'attività riservata esclusivamente ad una Pubblica Amministrazione che agisce in modo autoreferenziale (A. MASUCCI, 2011, p. 43). Un'impostazione diversa si rivelerebbe in effetti, con riguardo al nostro ordinamento nazionale, oltre che antistorica, certamente contraria a quei principi di imparzialità e buon andamento dell'art. 97 Cost. che trovano riscontro nel diritto ad una decisione imparziale ed equa iscritto nell'art. 41 CDUE e di cui il diritto di essere sentiti non rappresenta che un corollario.

In questa prospettiva, la caratteristica del mondo digitale è che si tratta di

un «universo di immediatezza»: anche perché l'idea di spazio (e di luogo fisico) diventa irrilevante (D.-U. GALETTA, 2018b, p. 323). Il che, naturalmente, consente di ridurre le inefficienze connesse ai tempi di una partecipazione che è per sua natura "asincrona". Ma tale asincronismo, mentre è un elemento certamente negativo in termini di efficienza ed incide negativamente sulla ragionevole durata del procedimento nel caso della partecipazione con modalità cartacea, può invece diventare un elemento positivo in un contesto dominato dalle ICT: in cui colui che chiede di essere ascoltato lo potrebbe fare attraverso piattaforme digitali e strumenti analoghi.

In questo senso l'esperienza del bilancio partecipato del Comune di Milano (v. B. CAPPIELLO, G. CARULLO, M. PAGANI, M. ATTARDO, 2020) rappresenta un esempio certamente positivo di utilizzo di simili piattaforme di partecipazione asincrona che, dalla prospettiva degli strumenti tecnologici utilizzati, potrebbe certamente essere esteso anche all'ipotesi di partecipazione al procedimento di cui stiamo qui discutendo.

A questo proposito vale la pena di segnalare che il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022 «promuove l'avvio di nuove piattaforme che consentono di razionalizzare i servizi per le amministrazioni ed i cittadini» (v. in https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2020/08/12/il-piano-triennale-linformatica-nella-pa-2020-2022, p. 23).

10. Digitalizzazione e diritto di ogni persona di accedere al fascicolo che la riguarda

Il diritto di accesso al proprio fascicolo, da tempo previsto per singoli ambiti settoriali del diritto UE, è anche principio generale del diritto UE e trova perciò applicazione, come tale, con riguardo a tutti i procedimenti amministrativi. Secondo i giudici UE di Lussemburgo, infatti, «La consultazione del fascicolo rientra tra le garanzie procedurali miranti a tutelare i diritti della difesa e a garantire, in particolare, l'esercizio effettivo del diritto di contraddittorio». (Così ad es. Tribunale UE, sentenza 18 dicembre 1992, in cause riun. 10, 11, 12 e 15/92, *Cimenteries CBR SA c. Commissione*, ECLI:EU:T:1992:123, punto 38).

Quanto alla carta dei diritti, l'art. 41 CDUE si riferisce al «diritto di ogni persona di accedere al fascicolo che la riguarda» che va tenuto ben distinto dal più generale «diritto di accedere ai documenti delle istituzioni, organi o organismi dell'Unione», statuito dall'art. 42 CDUE (su cui v. nel capitolo VIII, S. ROSSA).

Nel diritto UE il diritto di accedere agli atti del proprio fascicolo è stretta-

mente connesso al diritto ad essere informati di cui si è detto al precedente paragrafo e corrisponde ad una visione della partecipazione del cittadino strumentale alla protezione delle sue posizioni giuridiche soggettive, diversamente dall'accesso *ex* art. 42 CDUE. Infatti, la Corte di giustizia UE sottolinea come l'accesso sia necessario allo scopo di stabilire, ad esempio, se le accuse mosse dalla Commissione siano fondate e da potere predisporre in modo adeguato i propri strumenti difensivi (Corte giust., sentenza 9 novembre 1983, in causa 322/81, *NV Nederlandsche Banden Industrie Michelin c. Commissione*, ECLI:EU:C:1983:313, punto 5 ss.; Tribunale UE, sentenza 17 dicembre 1991, in causa T-7/89, *SA Hercules Chemicals NV c. Commissione*, ECLI:EU:T:1991:75, punto 51). Con la conseguenza che la Commissione UE non potrà fondare la sua decisione su documenti e mezzi di prova ai quali l'interessato non abbia avuto previamente accesso (come ha espressamente statuito il Tribunale UE con la ben nota pronunzia *Solvay* del 1995.Tribunale UE, sentenza 29 giugno 1995, in causa T-30/91, *Solvay SA c. Commissione*, ECLI:EU:T:1995:115, punto 83).

La prospettiva è cioè quella di garantire, nell'ottica tipica del principio di parità delle armi, parità nel livello d'informazione delle parti.

Al pari del diritto di essere ascoltati, anche il diritto d'accesso al fascicolo subisce peraltro delle limitazioni che sono identificate già nel comma 2, lett. b) dell'art. 41 CDUE, come il «rispetto dei legittimi interessi della riservatezza e del segreto professionale». Dalla giurisprudenza dei giudici comunitari si evince tuttavia che, se da un lato le istituzioni UE sono tenute ad osservare il principio della riservatezza delle informazioni relative alle imprese, questo obbligo deve tuttavia essere interpretato in modo tale da non svuotare il diritto d'accesso «del suo contenuto essenziale» (Corte giust., sentenza 20 marzo 1985, in causa 264/82, *Timex Corporation c. Consiglio*, ECLI:EU:C:1985:119, punto 29); e «spetta alle autorità o agli organi giurisdizionali competenti ricercare, alla luce delle circostanze di ciascun caso di specie, un equilibrio tra tali interessi contrapposti» (così da ultimo Corte giust., sentenza 13 settembre 2018, in causa C 358/16, UBS, ECLI:EU:C:2018:715, punto 70).

Ciononostante, anche al diritto d'accesso al proprio fascicolo sono talora imposte dalle Amministrazioni procedenti limitazioni giustificate in relazione a presunte esigenze di efficienza. A questo proposito, tuttavia, il Tribunale UE, nella notissima sentenza Solvay, ha sottolineato come «il rispetto dei diritti della difesa non può urtarsi a difficoltà tecniche e giuridiche che un'amministrazione efficiente può e deve superare» (Tribunale UE, sentenza 29 giugno 1995, in causa T-30/91 cit., punto 102). Sicché, nell'opinione delle Corti UE sarà possibile negare l'accesso solo nell'ipotesi in cui questo rappresenti, ad esempio, un rischio per le stesse indagini in corso; ma non in altre ipotesi: pena l'impossibilità di utilizzare i documenti stessi quali «validi mezzi di prova» (tra le tante,

Tribunale UE, sentenza 10 marzo 1992, in causa T-9/89, *Hüels AG c. Commissione*, ECLI:EU:T:1992:3, punto 38; Corte giust., sentenza 03 luglio 1991, in causa C-62/86, *AKZO Chemie c. Commissione*, ECLI:EU:C:1991:286, punto 21).

Anche a questo proposito – e con specifico riferimento alla circostanza che nell'opinione dei giudici UE, come si è detto, il rispetto dei diritti della difesa non può urtarsi a difficoltà tecniche – appare evidente come le tecnologie ICT possano facilitare e rendere assai più rapido l'accesso (al proprio fascicolo). A questo riguardo infatti, già nel Piano d'azione per l'e-government presentato nel 2000 dall'allora ministro per la funzione pubblica Bassanini (e tuttora consultabile in http://www.interlex.it/testi/rappegov.htm) si precisava che «In coerenza con gli obiettivi definiti dalla Unione europea, i progetti per il breve periodo sono principalmente orientati a consentire l'accesso telematico alle informazioni (…) tramite la realizzazione di un insieme di portali» (par. 2 del Piano d'azione per l'e-government cit.). E l'art. 3, comma 1, CAD attualmente in vigore specifica che «Chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2, anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo».

11. Digitalizzazione e obbligo per l'amministrazione di motivare le proprie decisioni

Nel contesto del diritto UE l'obbligo di motivazione riveste un'importanza cruciale. Non a caso, infatti, già l'art. 15 del Trattato CECA statuiva che «Les décisions, recommandations et avis de la Haute Autorité sont motivés» (il testo ufficiale del Trattato istitutivo della Comunità europea del carbone e dell'acciaio fu firmato a Parigi il 18 aprile 1951 e redatto unicamente in lingua francese).

Parimenti, l'art. 190 dell'originario Trattato CEE del 1957 statuiva che «I regolamenti, le direttive e le decisioni del Consiglio e della Commissione sono motivati». E questo in un'epoca in cui negli ordinamenti nazionali la segretezza dell'attività amministrativa era, invece, la regola normale!

Attualmente la norma generale di riferimento nel diritto UE è l'art. 296, comma 2, TFUE che prevede che «gli atti giuridici sono motivati». Mentre la previsione contenuta nell'art. 41, comma 2, CDUE si riferisce, più specificamente, all'obbligo «per l'amministrazione di motivare le proprie decisioni».

Data l'estrema genericità delle previsioni richiamate, la giurisprudenza intesa a specificare i contenuti concreti dell'obbligo di motivazione è ovviamente assai abbondante. In particolare, sin dagli esordi della sua giurisprudenza la Corte di giustizia UE ha posto in evidenza come dalla motivazione debbano risultare tutti

gli elementi di fatto e di diritto «su cui le decisioni poggiano (…) in modo da consentire che su di esse si eserciti il controllo giurisdizionale» (così già Corte giust., sentenza 20 marzo 1957, in causa 2/56, *Die in der "Geitling" Ruhrkohlen-Verkaufsgesellschaft mbH zusammengeschlossenen Bergwerksgesellschaften c. Alta Autorità*, ECLI:EU:C:1957, p. 35 ss. V. anche Corte giust., sentenza 17 novembre 1987, in cause riun. 142 e 156/84, *British American Tobacco Co. Ltd c. Commissione*, ECLI:EU:C:1987:490, punto 72).

La motivazione deve esporre in modo plausibile le ragioni di fatto e di diritto che hanno condotto all'adozione dell'atto (v. da ultimo Tribunale UE, sentenza 28 giugno 2016, in causa T 216/13, *Telefónica*, ECLI:EU:T:2016:369, punto 275 ss.); e la sua ampiezza è strettamente legata alle peculiarità del singolo caso (V. Tribunale UE, sentenza 12 dicembre 1996, in causa T-16/91 RV, *Rendo NV e.a. c. Commissione*, ECLI:EU:T:1996:189, punto 44).

A questo proposito, dalla costante giurisprudenza della Corte di giustizia si desume che vi è l'esigenza di fornire una motivazione più dettagliata per l'ipotesi di decisioni individuali (Così, ad es., già Corte giust., sentenza 28 maggio 1980, in cause riun. 33/79 e 75/79 cit., punto 14). E che l'obbligo di motivazione è particolarmente ampio allorché la decisione in questione incida oltre una certa misura nella sfera giuridica del suo destinatario. Nell'opinione dei giudici di Lussemburgo, peraltro, la violazione dell'obbligo di motivazione sussiste non solo nell'ipotesi in cui manchi del tutto la motivazione, ma anche nell'ipotesi in cui questa appaia insufficiente sotto il profilo quantitativo o qualitativo (v. già Corte giust., sentenza 20 marzo 1959, in causa 18/57, *I. Nolde c. Alta Autorità*, ECLI:EU:C:1959:6, p. 115).

È a quest'ultimo proposito che entra in gioco il tema delle tecnologie ICT che rileva, in particolare, in relazione alla c.d. decisione amministrativa automatizzata (su cui v. il capitolo IV, R. CAVALLO PERIN e I. ALBERTI. V. anche il capitolo I, A. SIMONCINI).

A tale riguardo è sufficiente qui osservare, come il Consiglio di Stato abbia anzitutto chiarito che, allorché ci si trova di fronte a «procedure seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale (…), l'assenza di intervento umano (…) 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» (Cons. Stato, sez. VI, sentenza 8 aprile 2019, n. 2270, punto 8.1.). Tuttavia, a fronte della contestazione dei ricorrenti sul fatto che la procedura automatizzata «era sfociata in provvedimenti privi di alcuna motivazione, senza l'individuazione di un funzionario dell'amministrazione che abbia valutato le singole situazioni ed abbia correttamente esternato le relative

determinazioni provvedimentali» (sent. CdS 2019/2270 cit., punto 7), il Consiglio di Stato ha altresì precisato come «L'utilizzo di procedure "robotizzate"» non possa essere «motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa», quale quelli di «pubblicità e trasparenza» (sent. CdS 2019/2270, punto 8.2. V. sul punto anche il capitolo I, A. SIMONCINI).

Sicché, nell'opinione del nostro Consiglio di Stato, nel momento in cui si faccia (legittimamente) ricorso ad una automatizzazione del procedimento amministrativo, diventa ancora più importante assolvere all'obbligo di motivazione: poiché «la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo» (sent. CdS 2019/2270, punto 8.4.).

Può dunque concludersi che, se da un lato il nostro Consiglio di Stato ritiene che debba senz'altro consentirsi alla Pubblica Amministrazione di fare ricorso agli strumenti messi a disposizione dalle tecnologie ICT, nella misura in cui questi si rivelano idonei allo scopo di realizzare un'azione amministrativa maggiormente rispondente ai canoni di imparzialità e di buon andamento di cui all'art. 97 Cost., dall'altro lato, esso ne condiziona l'utilizzo all'osservanza del principio di trasparenza (su cui v. il capitolo VIII, S. ROSSA), che viene inteso anzitutto nei termini di piena conoscibilità e dell'esistenza di eventuali processi decisionali automatizzati e dell'algoritmo. Questo obbligo di trasparenza va assolto, anzitutto, attraverso il corretto assolvimento del dovere di motivazione del provvedimento finale adottato. Sicché – e per concludere – in uno scenario di decisioni amministrative adottate grazie a strumenti ICT quali gli algoritmi d'intelligenza artificiale (debole o forte che sia), l'obbligo di motivazione, lungi dal perdere significato, ne esce rafforzato.

Questa conclusione è perfettamente in linea con quanto di recente osservato in dottrina, da chi ha messo in evidenza come il fatto che vi possa essere una difficoltà legata alla complessità "tecnica" nello spiegare in che modo l'algoritmo sia giunto ad adottare una certa soluzione non equivalga affatto al *non potere fornire* una spiegazione (C. COGLIANESE, D. LEHR, 2019).

12. Il procedimento amministrativo oggi: fra diritto ad una buona amministrazione (e relativi "standard minimi" *ex* art. 41 CDUE) e conseguenze derivanti dall'utilizzo delle tecnologie ICT

Nel suo parere del 2005 sul CAD il nostro Consiglio di Stato aveva osservato che «come rilevato dalla migliore dottrina, la presenza di nuovi mezzi di svolgimento dell'attività amministrativa impone, quando le innovazioni lo

consentono, il compimento di operazioni di adattamento dei vecchi istituti alle nuove situazioni» (Consiglio di Stato, parere del 7 febbraio 2005 n. 11995, punto 7.). L'uso di tecnologie ICT a supporto della propria attività da parte delle Pubbliche Amministrazioni rappresenta infatti, certamente, un elemento importante nella prospettiva di implementare in concreto sia il dettato costituzionale dell'art. 97 (sotto il profilo e di una maggiore imparzialità e del buon andamento), sia – come si è visto – i vari corollari di quel diritto ad una buona amministrazione ora statuito all'art. 41 CDUE, ma che è frutto di una lunga evoluzione giurisprudenziale, avviatasi sin dai primi anni dell'esperienza comunitaria (D.-U. GALETTA, B. GRZESZICK, 2016).

Anche in questa prospettiva, dunque, il tema dell'automazione dell'attività amministrativa analizzato dal punto di vista della digitalizzazione del procedimento amministrativo rappresenta un oggetto di studio e ricerca di rilevanza centrale oggi (v. anche il capitolo IV, R. CAVALLO PERIN e I. ALBERTI).

In linea, dunque, con quella distinzione a suo tempo messa in luce in dottrina, tra atto a forma elettronica ed atto a elaborazione elettronica (A. MASUCCI, 1993, p. 13; D. MARONGIU, 2005, p. 17), e in linea con l'ormai ben noto principio del *digital first*, occorre dunque certamente che la Pubblica Amministrazione faccia quel famoso balzo in avanti che implica il passaggio alla c.d. Pubblica Amministrazione 4.0 (D.-U. GALETTA, J.G. CORVALÁN, 2019).

A tale scopo è necessario, anzitutto, che si consumi il passaggio da un modello di informatica c.d. documentaria, ossia l'utilizzo della telematica per la raccolta, l'organizzazione e la comunicazione in modalità digitale di dati e di informazioni precedentemente contenuti all'interno di un supporto cartaceo, ad un modello di vera e propria informatica meta-documentaria, nella quale l'utilizzo degli strumenti informatici consente la riproduzione automatica di certi processi logici tipici della mente umana (M. D'ANGELOSANTE, 2016). Si tratta del tema, complesso e centrale, dell'utilizzo di sistemi di intelligenza artificiale a supporto dell'attività amministrativa, di cui si è detto in vari capitoli di questo volume (si veda specialmente il capitolo VI, G. CARULLO).

In secondo luogo, occorre non solo procedere ad una vera e propria automazione del procedimento amministrativo grazie alle ICT, identificandone e sfruttandone appieno le relative potenzialità. Occorre anche essere in grado di identificare gli obiettivi che possono essere raggiunti tramite l'automazione dell'attività amministrativa e, più in generale, tramite l'uso delle ICT.

Perché si tratti realmente di un balzo in avanti anche nella prospettiva degli artt. 97 Cost. e 41 CDUE occorre tuttavia, anche, che vi sia consapevolezza di quelle regole che devono essere necessariamente rispettate affinché il sistema di garanzie su cui si fonda lo "Stato di diritto" (e, nel nostro caso, "di diritto amministrativo") resti intatto. E in questa prospettiva occorre avere in mente,

che le garanzie procedimentali sono in sé e per sé molto rilevanti; almeno tanto quanto lo sono gli interessi c.d. sostanziali che con l'attività amministrativa si mira a soddisfare (D.-U. GALETTA, 2003).

Sicché – e per concludere – dovendosi trattare di scelte non operate sulla spinta del momento, ma adeguatamente ponderate e soppesate anche nei loro effetti di medio-lungo periodo, non appare opportuno che la scelta sul se e sul come ricorrere all'automazione sia lasciata alla singola Pubblica Amministrazione, volta per volta, senza che l'automazione del procedimento venga magari neppure resa nota al destinatario dell'atto finale. Così facendo, infatti, se sarà forse possibile raggiungere un obiettivo di maggiore efficienza e celerità dell'azione amministrativa grazie all'uso delle ICT, non sarà invece possibile garantire il mantenimento di quel modello di "buona amministrazione" europeo rispetto al quale le garanzie riconosciute dall'art. 41 CDUE rappresentano peraltro solo degli "standard minimi".

Bibliografia

AVANZINI G., *Decisioni algoritmiche e algoritmi informatici: predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Editoriale Scientifica, Napoli, 2019.

BASSAN F., *Diritto delle comunicazioni elettroniche*, Giuffrè, Milano, 2010.

BERTI G., *La Pubblica Amministrazione come organizzazione*, Cedam, Padova, 1968.

CAPPIELLO B., CARULLO G., PAGANI M., ATTARDO M., *Il finanziamento delle opere pubbliche con la tecnologia blockchain: nuove forme di collaborazione pubblico-privato per una più efficace raccolta fondi bottom-up ed una più effettiva partecipazione della popolazione*, in *CERIDAP*, 2020, 2, https://ceridap.eu.

CARDARELLI F., *L'uso della telematica. Commento all'art. 3-bis della l. 241/90*, in M.A. SANDULLI (a cura di), *Codice dell'azione amministrativa*, Giuffrè, Milano, 2017.

CARULLO G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, Torino, 2017.

CERULLI IRELLI V., *Lineamenti del diritto amministrativo*, Giappichelli, Torino, 2008.

CIVITARESE MATTEUCCI S., L. TORCHIA, *La tecnificazione*, in L. FERRARA, D. SORACE (a cura di), *A 150 anni dall'unificazione amministrativa italiana: studi*, Firenze University Press, Firenze, 2016, vol. IV.

COGLIANESE C., LEHR D., *Transparency and Algorithmic Governance*, in *Administrative Law Review* e in University of Penn Law School, *Public Law Research Paper*, No. 18-38, in SSRN: https://ssrn.com/abstract=3293008.

COSTANTINO F., *Autonomia dell'Amministrazione e innovazione digitale*, Jovene, Napoli, 2012.

COSTANTINO F., *L'uso della telematica nella pubblica amministrazione*, in A. ROMANO (a cura di), *L'azione amministrativa. Saggi sul procedimento amministrativo*, Giappichelli, Torino, 2016, p. 246 ss.

D'ANGELOSANTE M., *La consistenza del modello dell'amministrazione 'invisibile' nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*, in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione* cit., p. 156 ss.

DELLA CANANEA G., GALETTA D.-U. e. a. (a cura di), *Codice ReNEUAL del procedimento amministrativo dell'Unione Europea*, Editoriale Scientifica, Napoli, 2016.

DONATI D., *Digital divide e promozione della diffusione delle ICT*, in F. MERLONI (a cura di), *Introduzione all'eGovernment: pubbliche amministrazioni e società dell'informazione*, Giappichelli, Torino, 2005, p. 209 ss.

DUNI G., *L'amministrazione digitale. Il diritto amministrativo nell'evoluzione telematica*, Giuffrè, Milano, 2008.

GAETANO S., *La digitalizzazione del procedimento amministrativo*, Clioedu, Lecce, 2018.

GALETTA D.-U., *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 2020, 3.

GALETTA D.-U., *Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens?*, in *European Public Law*, 2019, 25(2), p. 171 ss. [2019a].

GALETTA D.-U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in *Rivista italiana di diritto pubblico comunitario*, 2019, 2, p. 165 ss. [2019b].

GALETTA D.-U., *Digitalización y transparencia: ¿un "responsable de la trasparencia" y su "asistente digital" como herramientas del buen gobierno del futuro?*, in *Revista Jurídica de Buenos Aires*, 2018, 96, I, p. 159 ss. [2018a].

GALETTA D.-U., *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini?*, in *Ciberspazio e Diritto*, 2018, 3, p. 319 ss. [2018b].

GALETTA D.-U., *Riflessioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE sul diritto ad una buona amministrazione, anche alla luce di alcune recenti pronunce della Corte di giustizia*, in *Il Diritto dell'Unione europea*, 2013, 1, p. 133 ss.

GALETTA D.-U., *Diritto ad una buona amministrazione e ruolo del nostro giudice amministrativo dopo l'entrata in vigore del Trattato di Lisbona*, in *Diritto Amministrativo*, 2010, 3, p. 601 ss.

GALETTA D.-U., *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione*, in *Rivista italiana di diritto pubblico comunitario*, 2005, 3, p. 819 ss.

GALETTA D.-U., CORVALÁN J.G., *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in Federalismi.it, 2019, 3, 6 febbraio 2019, p. 1 ss.

GALETTA D.-U., GRZESZICK B., *Kommentar zu Art. 41 Grundrechtecharta*, K. STERN, M. SACHS (a cura di), *Europäische Grundrechtecharta. Kölner Gemeinschafts-Kommentar*, Köln, II ed., 2016, p. 618 ss.

HEUDIN J-C., *Intelligence Artificielle. Manuel de survie*, Science-eBook, 2017.
HEUDIN J-C., *Comprendre le deep learning: Une introduction aux réseaux de neurones*, Paris, 2016.
LEVI F., *L'attività conoscitiva della pubblica amministrazione*, Giappichelli, Torino, 1967.
MARONGIU D., *L'attività amministrativa automatizzata*, Maggioli, Rimini, 2005.
MASUCCI A., *L'atto amministrativo informatico: primi lineamenti di una ricostruzione*, Jovene, Napoli, 1993.
MASUCCI A., *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Giappichelli, Torino, 2011.
MCTEAR M., CALLEJAS Z., GRIOL BARRES D., *The conversational interface: Talking to smart devices*, Springer International Publishing, Switzerland, 2016.
MOSCARIELLO A., *El principio de la buena Administración*, in *El Derecho*, Serie Especial Administrativo, 28/02/2013.
PESCE G., *Amministrazione digitale: genesi, sviluppi, prospettive*, Editoriale Scientifica, Napoli, 2018.
PICARD R.W. *Toward Machines With Emotional Intelligence*, G. MATTHEWS, M. ZEIDNER, R.D. ROBERTS (a cura di), *The Science of Emotional Intelligence: Knowns and Unknowns*, Oxford University Press, Oxford, 2007.
PIOGGIA A., *Le risorse e gli strumenti*, in F. MERLONI (a cura di), *Introduzione all'eGovernment: pubbliche amministrazioni e società dell'informazione*, Giappichelli, Torino, 2005, p. 281 ss.
RODRÍGUEZ-ARANA J., *La buena administración como principio y como derecho fundamental in Europa*, in *Derecho y Ciencias Sociales*, 2013, 6, p. 23 ss. reperibile anche in https://dialnet.unirioja.es/descarga/articulo/5167578.pdf.
SPANO TARDIVO P., *El principio de transparencia de la gestión pública in el marco de la teoría del bueno gobierno y la buena administración*, in *Revista Digital de la Asociación Argentina de Derecho Administrativo*, 2016, 1, p. 226 ss.
SÖDERMAN J., *Speech of the European Omdundsaman-Public hearing on the draft of fundamental Rights of the European Union*, *Preliminary remarks*, 2000, in www.ombudsman.europa.eu.
TRIMARCHI BANFI F., *Il diritto ad una buona amministrazione*, in M.P. CHITI, G. GRECO (a cura di), *Trattato di diritto amministrativo europeo*, Giuffrè, Milano, 2007, p. 63 ss.
ZITO A., *Il «diritto ad una buona amministrazione» nella Carte dei diritti fondamentali dell'Unione europea e nell'ordinamento interno*, in *Rivista italiana di diritto pubblico comunitario*, 2002, p. 427 ss.

IV.

ATTI E PROCEDIMENTI AMMINISTRATIVI DIGITALI

Roberto Cavallo Perin e Isabella Alberti[*]

SOMMARIO: 1. L'atto amministrativo digitale: dall'informatizzazione all'automazione. – 1.1. Atto amministrativo e tecnologia. – 1.2. L'atto amministrativo informatico. – 1.3. L'atto amministrativo digitale. – 2. Le prime fasi del procedimento digitale. – 2.1. La comunicazione informale e i siti web: moduli e formulari. – 2.2. L'inizio *software* del procedimento. – 2.3. La comunicazione telematica dell'inizio del procedimento. – 2.4. L'istruttoria documentale su fatti, stati o qualità, tra *machine learning* e reti neurali. – 2.5. L'istruttoria non documentale: *Internet of Things*, rilevazioni aerofotogrammetriche o satellitari, *blockchain*, piattaforme, *Applications Programming Interfaces*. – 2.6. Le interconnessioni tra banche dati come strumento per ottenere nuova conoscenza (rinvio al capitolo VI). – 3. La validità della decisione automatica: tra norme, atti generali e precedenti. – 3.1. La natura giuridica dell'algoritmo. – 3.2. L'algoritmo nella definizione della validità degli atti amministrativi. – 3.3. L'algoritmo tra interpretazione e discrezionalità. – 4. La decisione automatizzata. – 4.1. Sull'opacità e sul difetto di motivazione dell'algoritmo. – 4.2. La base legale dell'atto digitale e la partecipazione degli interessati. – 4.3. Indirizzo politico, imparzialità e sistematicità delle decisioni. – 4.4. Il sindacato sull'algoritmo e la correzione casistica. – 4.5. Rapidità e conservazione negli algoritmi.

1. L'atto amministrativo digitale: dall'informatizzazione all'automazione

1.1. Atto amministrativo e tecnologia

L'atto amministrativo in forma elettronica (G. DUNI, 1978, p. 407 s.; A. MASUCCI, 1993, p. 83 s.) comincia a essere studiato sin dagli anni '70 quando

[*] La redazione dei paragrafi 1, 3 e 4 è di Roberto Cavallo Perin, l'intero paragrafo 2 è di Isabella Alberti.

gli strumenti informatici diventano parte dell'organizzazione della Pubblica Amministrazione.

Le prime applicazioni d'informatica pubblica (M.G. LOSANO, 1986, p. 1 s.; A. USAI, 1992, p. 2 s.; U. FANTIGROSSI, 1993, p. 33 s.) si sono sviluppate secondo due direttrici, tutt'ora presenti nel dibattito: l'una che relega la tecnica a strumenti d'ausilio (in sequenza storica: computer, internet, smartphone, ecc.), l'altra che pensa invece che l'innovazione investa essenzialmente la Pubblica Amministrazione e il procedimento decisionale pubblico, ridisegnandone la forma e la sostanza.

Anche se entrambe le applicazioni intendono favorire la transizione dalla dimensione analogica a quella digitale sia dell'attività, sia dell'organizzazione della Pubblica Amministrazione, la prima pensa che sia possibile un controllo esterno dell'innovazione ad opera del diritto o dell'etica, lasciando e riconoscendo che l'innovazione è essenzialmente posta da altri (informatici, neuroscienziati, ecc.); la seconda invece vuole accogliere l'innovazione scientifica ed esserne parte creativa determinante.

L'atto amministrativo *digitale* – esito ultimo dell'evoluzione segnata prima dall'atto elettronico, poi informatico o automatico – è in sé una sfida alle scienze giuridiche, in particolare al diritto amministrativo, poiché, in questo come in altri casi, l'innovazione tecnologica dell'attività dell'amministrazione pubblica obbliga i teorici a un'attenta rivisitazione delle tradizionali categorie giuridiche sul principio di legalità e sulla validità dell'atto amministrativo (par. 3), sul procedimento (par. 2) e sul provvedimento amministrativo (par. 4) e ancora prima sugli atti d'iniziativa (par. 2.1. e par. 2.2), sull'attività conoscitiva delle amministrazioni pubbliche posta a base delle scelte d'interesse generale (parr. 2.4, 2.5 e 2.6), in particolare per la programmazione e per le modalità di erogazione dei servizi pubblici.

1.2. L'atto amministrativo informatico

In una prima fase il processo di informatizzazione (M.G. LOSANO, 1979, p. 155 s.; E. ZAFFARONI, 1996, p. 2516 s.; A.G. OROFINO, 2003, p. 1371 s.) si è concentrato sull'inserimento nella Pubblica Amministrazione delle tecnologie gestionali già utilizzate dalle organizzazioni private, ivi compresa la gestione e l'archiviazione dei documenti, con un graduale ma inesorabile cambiamento dell'apparato amministrativo.

L'accelerazione del processo si è avuta con internet e la connessione a rete dei computer, poi quando ciascun individuo si è dotato di uno smartphone: un cambio d'infrastruttura che ha inaugurato il processo di telematizzazione dell'attività amministrativa e posto le basi per un sistema di *e-Government* (*supra* Introduzione).

Il provvedimento amministrativo ha dapprima subìto solo parzialmente l'innovazione tecnologica, poiché gli atti *amministrativi* restavano – nella tradizione millenaria– resi su carta: riprodotti in formato elettronico oppure in forma cartacea, a seconda della confezione originaria, rispettivamente su carta o su supporto digitale. L'introduzione degli strumenti informatici perciò non ha potuto sino a quel momento recare incertezze, poiché l'atto amministrativo era pur sempre offerto su carta.

L'atto amministrativo informatizzato ha avuto riconoscimento legislativo nella stagione delle grandi riforme della Pubblica Amministrazione degli anni '90, con il D.Lgs. 12 febbraio 1993, n. 39; un testo emanato pochi giorni dopo il D.Lgs. 3 febbraio 1993, n. 29, sulla privatizzazione del pubblico impiego e la disciplina dell'organizzazione delle pubbliche amministrazioni.

Gli «atti amministrativi adottati da tutte le pubbliche amministrazioni sono *di norma* predisposti tramite i sistemi informativi automatizzati» (art. 3, D.Lgs. 12 febbraio 1993, n. 39; ora art. 3-*bis*, Legge 7 agosto 1990, n. 241, mod. da Legge 11 settembre 2020, n. 120, di conversione del DL-semplificazioni n. 76/2020, art. 12, comma 1, lett. b), un enunciato legislativo che – già vent'otto anni or sono – ha qualificato giuridicamente la forma elettronica dell'atto amministrativo come soluzione ordinaria, ma ancor prima ha chiarito che sono direttamente il processo conoscitivo e il procedimento decisionale a venire affidati – di norma – a *sistemi informativi automatizzati*.

Quanto alla forma estrinseca dell'atto (A.G. OROFINO, 2016, p. 181 s.) nessun serio ostacolo poteva opporsi a un riconoscimento anche solo interpretativo della forma scritta come possibile sia su supporto informatico, sia su supporto cartaceo; un'interpretazione evolutiva che già l'arrivo del computer aveva largamente imposto all'attenzione dei teorici e dei pratici.

La vera portata innovativa dell'enunciato legislativo s'afferma invece con riferimento alla *predisposizione* dell'atto amministrativo, cioè alla definizione-organizzazione dei procedimenti amministrativi tramite *sistemi informativi automatizzati* e di ciascuna sua fase: dall'iniziativa, all'istruttoria, alla partecipazione e alla decisione, infine a quella c.d. integrativa dell'efficacia.

Una disciplina che ha aperto giuridicamente all'elaborazione elettronica del contenuto dell'atto amministrativo come conseguenza dell'applicazione di sistemi informativi automatizzati che oggi sono basati sempre più su algoritmi sofisticati che suscitano nuove questioni: dall'individuazione dell'esatto momento in cui si forma la volontà della Pubblica Amministrazione (I.M. DELGADO, 2019, p. 643 s.), se la stessa volontà sia da individuare nella programmazione dell'algoritmo o se invece sia riconducibile alla successiva automatica emanazione del provvedimento.

La logica binaria che è alla base dei sistemi informatici ha indotto dappri-

ma a ritenere ammissibile l'atto amministrativo digitale solo per l'attività vincolata dell'amministrazione pubblica, in tutta consonanza all'idea che in tali casi il sillogismo giudiziale sia una sorta d'automatismo, poiché è pur sempre condotto sulla base di criteri oggettivi ed univoci, comunque su assiomi logici del giudizio condizionale, sicché al verificarsi di predeterminate condizioni, si ricollegano all'atto determinati effetti giuridici (F. SAITTA, 2003, p. 10).

L'idea del pari risalente – che quasi mai un potere è da ritenersi del tutto vincolato – ha contribuito a marginalizzare l'equiparazione dell'automatismo all'attività vincolata dell'amministrazione, poiché più esattamente si può oggi soggiungere che nell'automazione è esclusa – e nell'atto vincolato è affermata – l'intermediazione umana del caso concreto, seppure nella forma particolare di quel pensiero umano che è l'interpretazione (M.S. GIANNINI, 1939, p. 209).

Si è invece ritenuto preferibile pensare che, anche in costanza di una predeterminazione legislativa del potere pubblico, l'accertamento del fatto richieda pur sempre un ruolo attivo dell'intelletto umano, prima della Pubblica Amministrazione e poi del giudice nella valutazione della realtà e degli interessi così come coinvolti dal caso concreto.

L'atto amministrativo digitale che è l'esito di un algoritmo deterministico si pone all'interprete come un atto che è il prodotto del seguente schema decisionale: a) individuazione degli elementi caratterizzanti la fattispecie definita dalla norma e loro introduzione nel programma informatico sotto forma di *input*; b) successiva definizione di regole procedurali di tipo deterministico che soddisfano la formula condizionale del "*if … then*"; c) conseguente elaborazione automatizzata dell'*output* di risposta, che rappresenta il contenuto del provvedimento.

La piena programmabilità *ex ante* dei passaggi logici del programma informatico rende prevedibili i risultati e comprensibile la logica decisionale, così rendendo compatibili tali strumenti informatici con i principi dell'attività amministrativa. Ciò non vale per gli algoritmi di apprendimento basati sia su tecniche di *machine learning* sia su quelle di *deep learning* (c.d. reti neurali) che di recente hanno reso noti e dato un particolare rilievo agli atti amministrativi digitali.

1.3. L'atto amministrativo digitale

L'atto amministrativo automatico è una realtà giuridica da molti anni, basti pensare al verbale di accertamento delle violazioni del codice della strada, ove si prevede che l'accertamento delle violazioni *ivi* contemplate possa compiersi in assenza della contestazione immediata, qualora sia stata accertata da un dispositivo omologato ovvero approvato per il funzionamento in modo completamente automatico e gestito dalla polizia stradale. La documentazione prodotta dal di-

spositivo ha valore di atto di accertamento, che costituisce pieno titolo ai fini dell'applicazione della sanzione amministrativa, nonché valore probatorio.

Del pari è la formazione delle liste dei sorteggiabili tra i professori universitari candidati alla commissione per l'Abilitazione Scientifica Nazionale o per la creazione delle graduatorie di mobilità aventi ad oggetto i trasferimenti dei funzionari dell'Arma dei carabinieri o la formazione della graduatoria finale di un concorso pubblico, elaborata sulla base della comparazione esclusivamente informatizzata dei titoli posseduti dai candidati.

Superate le ipotesi più semplici, con l'atto amministrativo digitale è possibile che una macchina impari dall'esperienza umana, ordinando e classificando migliaia di casi (*infra* parr. 3-4) che sono i precedenti applicativi di un enunciato normativo.

Attraverso l'analisi casistica si possono programmare gli algoritmi deterministici e i sistemi d'intelligenza artificiale basati su algoritmi di apprendimento (*machine learning e deep learning*) affinché indichino minuziosamente sino a che punto un semplice livellamento del terreno non costituisca abuso edilizio, poiché non integra l'ipotesi di sbancamento. Per far ciò ad esempio si devono estrapolare e classificare gli interventi che non modificano in modo stabile né la struttura, né la funzione dell'area e che pertanto non sono soggetti al titolo abilitativo edilizio, da quelli che, invece, apportano una trasformazione rilevante sotto il profilo urbanistico-edilizio del territorio.

In prospettiva, dunque, l'atto amministrativo digitale si pone come il risultato di una previa proposta di decisione avanzata dallo strumento d'intelligenza artificiale, poi confermata o negata dall'intervento umano. Sulla base della casistica inserita lo strumento sarà in grado di classificare il nuovo caso sottopostogli, confrontando il nuovo caso con quelli utilizzati per il proprio *training*. Disporrà, per esempio, per il previo permesso di costruire qualora l'intervento sia un'infissione stabile e durevole al suolo: distinguendo i muri di contenimento dalle recinzioni (Cons. Stato, sez. II, 9 gennaio 2020, n. 212), le piazzole di non ampia dimensione (es. mq 14,30) dal mero livellamento del terreno (Cons. Stato, sez. VI, 24 settembre 2019, n. 6380).

Il grado di conoscenza offerto dall'intelligenza artificiale, che trae dai precedenti applicativi nuove letture dei casi su cui interviene la Pubblica Amministrazione, permette di sostenere che *machine learning* e disciplina giuridica sulla struttura del procedimento e del provvedimento amministrativo si rivelano – reciprocamente – un utile complemento l'uno per la scienza dell'altro, corredando della potenza del diritto le innovative scoperte che provengono dalla scienza informatica, dalle neuroscienze, dalla matematica e così via.

2. Le prime fasi del procedimento digitale

2.1. La comunicazione informale e i siti web: moduli e formulari

Gli obblighi di comunicazione informale – un tempo sbrigati allo sportello, al telefono, con lettera, infine con e-mail – sono oggi assolti rinviando l'interessato alla consultazione del sito web dell'ente o dell'ufficio, che è diventato il canale privilegiato di comunicazione (D.Lgs. 14 marzo 2013, n. 33; artt. 53 e 54, D.Lgs. 7 marzo 2005, n. 82; M. PIETRANGELO, 2016, p. 102).

Il rinvio al sito web appare legittimo solo ove lo stesso risulti effettivo; in assenza di norme generali e astratte, linee guida o altre soft law, ciò si afferma solo ove il sito web sia stato costruito osservando quanto ritenuto necessario dalla scienza della comunicazione e cioè si presenti conforme ai principi di *accessibilità*, *usabilità*, *affidabilità*, *omogeneità* ed *interoperabilità* (D.Lgs. 14 marzo 2005, n. 82, art. 53).

Funzionale a garantire l'effettività dei principi di pubblicità e trasparenza è il monitoraggio del sito (cfr. art. 8, Direttiva 2016/2102/UE, del Parlamento Europeo e del Consiglio, 26 ottobre 2016, *Relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici)* che non può non assumere il punto di vista dell'utente di media diligenza, al fine di verificare periodicamente un'agevole fruizione dei contenuti (art. 54, D.Lgs. n. 82/2005), provvedendo ove necessario alle rettifiche o ai riposizionamenti delle informazioni.

Gli Stati membri assumono oneri di armonizzazione per l'accessibilità dei siti web e loro *app* mobili di modo che siano *percepibili*, *utilizzabili*, *comprensibili* e *inattaccabili* (art. 4, Direttiva 2016/2102/UE, cit.), garantendo *feedback* per la revisione del sito (art. 7, par. 1, lett. b), Direttiva 2016/2102/UE) rendendoli pienamente accessibili, anche alle persone con disabilità (art. 1, par. 1, Direttiva 2016/2102/UE).

A tal fine d'utilità è un sistema di raccolta e vaglio delle segnalazioni cui collegare sistemi di intelligenza artificiale come il *chatbot* che automaticamente risponde alle domande frequenti, aiutando l'interessato nella ricerca di informazioni, nell'assolvimento di oneri, reindirizzandoli su pagine web o aiutandone la lettura. Un algoritmo di apprendimento – non supervisionato – può definire la classificazione delle domande, rilevando che le informazioni si sono rivelate non facili per carenza di dettagli o scarsa chiarezza, oppure non intuitiva è stata la reperibilità di esse, infine per quali altri motivi disagevole ne è stata la consultazione.

Seppure le modalità di un'agevole fruizione di un sito web dipendano da molteplici fattori – caratteri degli utenti, intermediazione di professionisti o no, molteplicità dei procedimenti assegnati a quell'ufficio, ecc. – si tratta quasi

sempre di una verifica che è facilmente percepibile da un giudice che, al pari dell'utente, non riesca a reperire con immediatezza l'informazione.

Il sito web assolve ormai in via crescente ai principali doveri e obblighi generali di comunicazione e informazione sui servizi erogati dalle stesse, sulle relative prassi, sulla modulistica o formulari da utilizzare per i singoli procedimenti, nonché sugli uffici ai quali rivolgersi per informazioni, sugli orari e le modalità di accesso con indicazione degli indirizzi, dei recapiti telefonici e delle caselle di posta elettronica istituzionale, a cui presentare le istanze (D.Lgs. 14 marzo 2013, n. 33, art. 35, comma 1, lett. d).

Oltre il sito web, molta importanza è riconosciuta allo sportello unico digitale (*Single Digital Gateway*) come canale privilegiato di comunicazione e relazione tra le amministrazioni e cittadini e imprese (v. capitolo III, D.-U. GALETTA). Con la sua istituzione (art. 2, Regolamento 2018/1724/UE del Parlamento Europeo e del Consiglio del 2 ottobre 2018, *che stabilisce l'apertura di uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e modifica il regolamento (UE) n. 1024/2012*) e la definizione dei parametri obbligatori, che devono essere assicurati per garantire l'accesso alle informazioni di alta qualità, vengono assicurate le condizioni minime per l'esercizio dei diritti di cittadini e imprese alle procedure e ai servizi di assistenza.

A differenza dello sportello unico per le imprese, quello in esame offre tutte le informazioni sui servizi di cui è competente un'istituzione dell'Unione Europea, analogamente a quanto previsto nei documenti programmatici di alcuni Stati membri (cfr. Francia, Spagna) come l'italiano *Piano Triennale per l'informatica nella Pubblica Amministrazione*, che individua azioni di semplificazione e di potenziamento dei servizi digitali delle pubbliche amministrazioni come linee guida e kit di sviluppo.

2.2. L'inizio *software* del procedimento

L'evoluzione normativa che ha accompagnato l'informatizzazione della Pubblica Amministrazione ha riguardato in particolare la fase dell'iniziativa, affiancando alla millenaria versione cartacea prima la comunicazione via fax, poi via software, cui si è affiancata più di recente il superamento dell'onere di costituire presso l'ufficio competente la fisica formazione del fascicolo e il fisico deposito degli atti cartacei del procedimento.

Più esattamente le istanze, nonché le dichiarazioni sostitutive di atto di notorietà da produrre all'amministrazione pubblica, ai gestori o esercenti di pubblici servizi, sono presentate con sottoscrizione avanti al dipendente ad-

detto, oppure sono inviate, in modalità telematica, con la sottoscrizione unitamente a copia fotostatica, anche non autenticata, di un documento di identità del sottoscrittore, poi inserita nel fascicolo (art. 38, comma 3, D.P.R. 28 dicembre 2000, n. 445), anch'esso ora curato in modalità telematica (art. 41, D.Lgs. 7 marzo 2005, n. 82, su cui v. il capitolo III, D.-U. GALETTA). Norme speciali disciplinano i contratti pubblici prevedendo la modalità telematica sin dalle procedure ad evidenza pubblica (D.Lgs. 16 aprile 2016, n. 50, art. 58; rinvio al capitolo XI, G.M. RACCA).

Istanze o dichiarazioni sono validamente inviate per via telematica alle pubbliche amministrazioni, producendo un documento informatico:

a) se sono inviate con posta elettronica certificata (art. 1, comma 1, lett. n-*ter*) e art. 65, comma 1, lett. c-*bis*), D.Lgs. 7 marzo 2005, n. 82) *oppure*

b) se la sottoscrizione è accompagnata dalla *scannerizzazione* del documento di identità personale (art. 65, comma 1, lett. c), D.Lgs. 7 marzo 2005, n. 82), o sottoscrivendo (artt. 20 e 65, D.Lgs. 7 marzo 2005, n. 82) con firma digitale (art. 24, D.Lgs. 7 marzo 2005, n. 82; imposta per la sottoscrizione di accordi fra pubbliche amministrazioni, art. 15, comma 2-*bis*, Legge 7 agosto 1990, n. 241), oppure, in conformità alla disciplina europea, con la firma elettronica avanzata, o la firma elettronica qualificata.

La firma digitale (art. 24, D.Lgs. 7 marzo 2005, n. 82), così come la firma elettronica qualificata, si basa su una procedura informatica, chiamata validazione, che garantisce la provenienza, l'autenticità e l'integrità del documento informatico (v. capitolo V, S. D'ANCONA).

Istanze o dichiarazioni possono venire destinate alla Pubblica Amministrazione anche utilizzando i sistemi informativi delle amministrazioni stesse, previa l'elettronica identificazione tramite *Sistema Pubblico di Identità Digitale* (SPID), attraverso la *Carta nazionale dei servizi* o la *Carta d'identità elettronica* (art. 65, comma 1, lett. b); art. 64, comma 2-*novies*, D.Lgs. 7 marzo 2005, n. 82). Sono autenticazioni che non necessitano di alcuna firma autografa o altro equivalente (v. capitolo VII, S. D'ANCONA e P. PROVENZANO).

Sebbene differenti (così nel D.Lgs. 7 marzo 2005, n. 82) esse sono intercambiabili, perché la struttura tecnologica di riferimento garantisce l'identità del soggetto sottoscrittore, nonché l'integrità e l'immutabilità del documento, equiparando il loro valore giuridico a quello assegnato alla firma autografa (Regolamento 2014/910/UE, art. 25, par. 2).

Discorso analogo può svolgersi per la sottoscrizione autentica dell'istanza mediante la carta nazionale dei servizi (CNS), o la carta di identità elettronica (CIE) (art. 64, D.Lgs. 7 marzo 2005, n. 82) ove la garanzia dell'integrità del documento e della paternità del sottoscrittore dipende dal previo accertamen-

to dell'identità compiuto dall'Amministrazione che ha provveduto al rilascio del documento identificativo.

Una pluralità di strumenti normativi che assicurano il diritto a pretendere l'uso degli strumenti informatici nelle pubbliche amministrazioni (art. 3, D.Lgs. 7 marzo 2005, n. 82), che è stato variamente riconosciuto nell'ordinamento italiano.

Al malfunzionamento che – per una causa non imputabile all'istante – abbia impedito la ricezione della domanda è conseguita la riapertura di termini perentori del procedimento (T.A.R. Lombardia, sede Milano, sez. IV, 19 settembre 2018, n. 2109; T.A.R. Lombardia, Milano, sez. IV, 9 gennaio 2019, n. 40) per il riconoscimento di una responsabilità del gestore del sistema informatico, trattandosi di sistemi che sono in totale dominio dell'amministrazione e delle sue relazioni con i gestori medesimi (Cons. Stato, 25 gennaio 2013, n. 481), da cui il conseguente «onere di attivazione, volto a sanare, se del caso, le mere anomalie di invio» (T.A.R. Puglia, Bari, sez. I, 28 luglio 2015, n. 1094).

La *ratio decidendi* è che la responsabilità consegue alla scelta istituzionale dell'amministrazione di volere ricorrere a un determinato sistema informativo con una evidente agevolazione nella gestione digitale dei flussi documentali che deve essere «controbilanciata dalla capacità di rimediare alle occasionali possibili disfunzioni, in particolare attraverso lo strumento procedimentale del soccorso istruttorio» (Cons. Stato, 25 gennaio 2013, n. 481), affinché sia garantito a tutti gli interessati l'accesso ai servizi offerti.

Istanze, dichiarazioni spedite in via telematica e le copie informatiche di documenti analogici (art. 22, D.Lgs. 7 marzo 2005, n. 82) sono documenti informatici che soddisfano il requisito della forma scritta prevista dalla legge e hanno l'efficacia probatoria della scrittura privata, cioè dànno piena prova – sino a querela di falso – della provenienza delle dichiarazioni di chi l'ha sottoscritta (art. 20, comma 1 *bis*, D.Lgs. 7 marzo 2005, n. 82; art. 2702, c.c.).

2.3. La comunicazione telematica dell'inizio del procedimento

Il responsabile del procedimento (su cui v. il capitolo III, D.-U. GALETTA) è tenuto a comunicare l'avvio del procedimento ai possibili destinatari (coloro verso i quali il provvedimento è destinato a produrre effetti) e ai controinteressati (coloro che facilmente individuabili potrebbero subire un pregiudizio dal provvedimento), nonché a chi per legge debba intervenirvi (art. 7, Legge 7 agosto 1990, n. 241).

La comunicazione di avvio del procedimento deve tassativamente indicare: l'amministrazione competente (art. 8, lett. a), Legge 7 agosto 1990, n. 241),

l'ufficio, il domicilio digitale e la persona responsabile del procedimento (art. 8, lett. c), Legge 7 agosto 1990, n. 241, mod. da Legge n. 120/2020, art. 12, comma 1, lett. d), punto 1) e le modalità con le quali si può prendere visione degli atti, nonché accedere al fascicolo informatico (art. 41, comma 2, D.Lgs. 7 marzo 2005, n. 82, cfr. Legge n. 120/2020, art. 12, comma 1, lett. d), punto 2) e le modalità d'esercizio in via telematica dei diritti di partecipazione al procedimento (art. 8, lett. d), Legge 7 agosto 1990, n. 241; art. 10, Legge 7 agosto 1990, n. 241; art. 41, comma 2, D.Lgs. 7 marzo 2005, n. 82; cfr. Legge n. 120/2020, art. 12, comma 1, lett. d), punto 2), oppure l'ufficio ove è possibile accedere a quegli atti che non sono accessibili o disponibili in via telematica (art. 8, lett. d-*bis*), Legge 7 agosto 1990, n. 241, mod. da Legge n. 120/2020, art. 12, comma 1, lett. d), punto 3) la data di presentazione dell'istanza (art. 8, lett. c-*ter*), Legge 7 agosto 1990, n. 241), l'oggetto (art. 8, lett. b), Legge 7 agosto 1990, n. 241).

La comunicazione personale del *termine di conclusione del procedimento* (art. 8, comma 2, lett. c-*bis*), Legge 7 agosto 1990, n. 241) implica il significato giuridico del suo compimento, chiarendo – oltre i casi in cui l'istanza valga dichiarazione sostitutiva (art. 35, lett. g), D.Lgs. 14 marzo 2013, n. 33; art. 19, Legge 7 agosto 1990, n. 241) – se il suo superamento valga silenzio assenso (art. 35, lett. g), D.Lgs. 14 marzo 2013, n. 33; art. 20, Legge 7 agosto 1990, n. 241) o silenzio rigetto.

Unitamente al termine di conclusione del procedimento l'amministrazione deve indicare i *rimedi* amministrativi e giurisdizionali sia avverso il provvedimento finale (art. 35, comma 1, lett. h), D.Lgs. 14 marzo 2013, n. 33), sia contro la violazione del termine di conclusione del procedimento (art. 35, comma 1, lett. h), D.Lgs. 14 marzo 2013, n. 33), sia contro il silenzio dell'amministrazione (art. 8, comma 2, lett. c-*bis*), Legge 7 agosto 1990, n. 241), comprese le modalità per attivare il potere sostitutivo, con nome, recapiti telefonici e casella di posta elettronica istituzionale (art. 35, comma 1, lett. m), D.Lgs. 14 marzo 2013, n. 33).

L'amministrazione è obbligata all'immediato rilascio – anche telematico – della ricevuta del deposito di ogni istanza, segnalazione o comunicazione (art. 18-*bis*, Legge 7 agosto 1990, n. 241), che vale comunicazione di avvio del procedimento ove contenga le informazioni per essa prescritte (artt. 8 e 18-*bis*, Legge 7 agosto 1990, n. 241; art. 41, comma 2, D.Lgs. 7 marzo 2005, n. 82).

L'obbligo dell'amministrazione si correla con il *diritto soggettivo del partecipe* a «usare soluzioni e strumenti» telematici, tra cui presentare istanze e ricevere documenti per via digitale (art. 3, comma 1, D.Lgs. 7 marzo 2005, n. 82; art. 18 *bis*, Legge 7 agosto 1990, n. 241).

La modalità telematica è necessaria nella comunicazione tra pubbliche amministrazioni (artt. 47, 6-*ter*, D.Lgs. 7 marzo 2005, n. 82) e con chi svolge pro-

fessionalmente una attività – siano essi imprenditori (artt. 5-*bis*, comma 1 e 6-*bis*, D.Lgs. 7 marzo 2005, n. 82) o professionisti (art. 6-*bis*, D.Lgs. 7 marzo 2005, n. 82) – e con chiunque abbia un *domicilio digitale* (artt. 3-*bis*, 6, 6-*quater*, D.Lgs. 7 marzo 2005, n. 82) (sulla nozione di domicilio digitale v. capitolo VII, S. D'ANCONA e P. PROVENZANO).

La comunicazione telematica personale (art. 18-*bis*, Legge 7 agosto 1990, n. 241) deve contenere il nome, i relativi recapiti telefonici, la casella di posta elettronica istituzionale (art. 35, comma 1, lett. b) e c), D.Lgs. 14 marzo 2013, n. 33), sia *dell'ufficio-organo competente* all'adozione del *provvedimento finale* (art. 8, comma 2, lett. a), Legge 7 agosto 1990, n. 241; art. 35, comma 1, lett. c), D.Lgs. 14 marzo 2013, n. 33), sia *dell'ufficio e della persona responsabile del procedimento* (art. 8, comma 2, lett. c), Legge 7 agosto 1990, n. 241; art. 35, comma 1, lett. b), D.Lgs. 14 marzo 2013, n. 33) *sia dell'ufficio in cui prendere visione degli atti* (art. 8, comma 2, lett. d), Legge 7 agosto 1990, n. 241).

Anche la *data di presentazione dell'istanza* (art. 8, lett. c-*ter*), Legge 7 agosto 1990, n. 241), con il chiarimento se valga dichiarazione sostitutiva (art. 35, lett. g), D.Lgs. 14 marzo 2013, n. 33; art. 19, Legge 7 agosto 1990, n. 241), nonché l'*oggetto del procedimento* comprensivo del *tipo di procedimento* (art. 8, lett. b), Legge 7 agosto 1990, n. 241) e dei riferimenti normativi (art. 35, lett. a), D.Lgs. 14 marzo 2013, n. 33), vanno indicati nella comunicazione personale telematica dando il *link* di accesso al procedimento amministrativo digitale (art. 35, lett. i), D.Lgs. 14 marzo 2013, n. 33) e la *login e password* di consultazione del fascicolo informatico (art. 41, comma 2, D.Lgs. 7 marzo 2005, n. 82).

Al fine di favorire un controllo sul perseguimento delle proprie funzioni istituzionali la Pubblica Amministrazione ha verso chiunque un obbligo generale d'informazione su dati e documenti (art. 5, comma 2, D.Lgs. 14 marzo 2013, n. 33) che può assolvere pubblicando sul proprio sito web, non solo le informazioni sulle tipologie di procedimenti (artt. 2 e 4, Legge 7 agosto 1990, n. 241; art. 35, D.Lgs. 14 marzo 2013, n. 33), ma anche ulteriori e più precise informazioni sui procedimenti amministrativi che la stessa sta curando, estendendo *erga omnes* molto di ciò nella comunicazione personale dell'avvio del procedimento è rivolto a soggetti determinati. (v. nel capitolo VIII, S. ROSSA).

I diritti degli interessati alla partecipazione al procedimento – e non solo di coloro che sono notiziati dalla comunicazione telematica di avvio del procedimento – trovano infatti effettività nell'adempimento dell'obbligo dell'amministrazione di procedere a formare il fascicolo informatico (art. 41, comma 2, D.Lgs. 7 marzo 2005, n. 82) sempreché la stessa dia notizia *erga omnes* dell'informazione essenziale sull'esistenza dei procedimenti *in corso*, a mezzo di una pubblicazione sul sito web istituzionale conforme ai principi di *accessibilità*, *usabilità*, *affidabilità*, *omogeneità* ed *interoperabilità* (art. 53, D.Lgs. 14 marzo

2005, n. 82), di trasparenza e pubblicità dell'azione amministrativa (art. 1, Legge 7 agosto 1990, n. 241).

La notizia sull'esistenza dei procedimenti va corredata dal *link di accesso* a ogni *servizio on line* e delle modalità telematiche indispensabili per intervenire nel procedimento (artt. 7, 9 e 10, Legge 7 agosto 1990, n. 241), intervento che una volta legittimato dall'amministrazione dà l'accesso al fascicolo informatico con tutte le informazioni utili a individuare lo stato del procedimento, consultarne gli atti e procedere al deposito di memorie e documenti (art. 10, Legge 7 agosto 1990, n. 241; art. 35, D.Lgs. 14 marzo 2013, n. 33; su cui v. il capitolo III, D.-U. GALETTA).

Con l'accesso al fascicolo informatico si ottiene la conoscenza di tutte le informazioni sull'andamento del procedimento (art. 10, Legge 7 agosto 1990, n. 241; art. 35, comma 1, lett. e), D.Lgs. 14 marzo 2013, n. 33) in particolare dei termini infraprocedimentali (art. 35, comma 1, lett. f), D.Lgs. 14 marzo 2013, n. 33), d'esercizio dei diritti di partecipazione (art. 10, Legge 7 agosto 1990, n. 241; art. 41, comma 2, D.Lgs. 7 marzo 2005, n. 82), sui relativi oneri e obblighi, ivi compresi i pagamenti dei diritti di segreteria o d'altri connessi al procedimento (art. 35, comma 1, lett. l), D.Lgs. 14 marzo 2013, n. 33).

2.4. L'istruttoria documentale su fatti, stati o qualità, tra *machine learning* e reti neurali

Come si è già avuto modo di sottolineare, la riorganizzazione strutturale e gestionale delle pubbliche amministrazioni è stata possibile con l'ingresso delle nuove tecnologie (art. 15, D.Lgs. 7 marzo 2005, n. 82) con la successiva messa in connessione dei sistemi informativi pel tramite di una specifica infrastruttura pubblica (art. 75, D.Lgs. 7 marzo 2005, n. 82), con il riconoscimento della validità dei documenti informatici (art. 20, D.Lgs. 7 marzo 2005, n. 82) e con l'obbligo della loro raccolta in un fascicolo informatico (art. 41, D.Lgs. 7 marzo 2005, n. 82), così ridefinendo l'essenza stessa dell'attività conoscitiva della Pubblica Amministrazione (F. LEVI, 1967, p. 237 s.) e in particolare, per ciò che qui interessa, della fase istruttoria del procedimento amministrativo.

Anzitutto l'amministrazione rende conoscibile il *fascicolo informatico* alle altre amministrazioni coinvolte nel procedimento e verso gli interessati, attraverso un *identificativo* (art. 41, comma 2-*ter*, D.Lgs. 7 marzo 2005, n. 82) che ne consenta l'indicizzazione utile a reperirlo con il *Sistema pubblico di ricerca documentale* (art. 40-*ter*, D.Lgs. 7 marzo 2005, n. 82).

Assolvendo all'obbligo di conoscenza del fascicolo informatico, l'amministrazione non solo rende noti gli elementi essenziali di forma che debbono es-

sere resi pubblici per assolvere al principio di pubblicità e trasparenza dell'azione della Pubblica Amministrazione, ma rende altresì consultabili tutti gli atti, i documenti e i dati da chiunque formati per il procedimento (art. 41, comma 2-*ter*, D.Lgs. 7 marzo 2005, n. 82), assicurando l'accesso civico generalizzato (art. 5, comma 2, D.Lgs. 14 marzo 2013, n. 33; art. 41, comma 2-*quater*, D.Lgs. 7 marzo 2005, n. 82) e l'esercizio dei diritti dei partecipi (art. 10, Legge 7 agosto 1990, n. 241; art. 41, comma 2-*quater*, D.Lgs. 7 marzo 2005, n. 82) mediante autenticazione con proprie credenziali di identificazione elettronica.

L'affermazione in via generale della validità dell'uso della telematica nell'azione amministrativa (Legge 7 agosto 1990, n. 241, art. 3-*bis*, mod. da Legge n. 120/2020, art. 12, comma 1, lett. b) involge anche le attività endoprocedimentali, anzitutto l'accertamento di fatti, di stati e di qualità personali, raffinando la precedente e ancor più forte innovazione apportata con le autocertificazioni di cinquant'anni or sono (Legge 4 gennaio 1968, n. 15).

Sono acquisite d'ufficio dall'amministrazione procedente o dai gestori di pubblici servizi (art. 43, D.P.R. 28 dicembre 2000, n. 445) tutte le informazioni (fatti, qualità e stati soggettivi) necessarie all'istruttoria del procedimento a disposizione dell'amministrazione procedente (art. 18, comma 2, Legge 7 agosto 1990, n. 241), mentre, per quelle detenute istituzionalmente da qualsiasi altra Pubblica Amministrazione o altro gestore di servizio pubblico, l'amministrazione procedente può richiedere agli interessati l'autodichiarazione con l'indicazione degli elementi necessari alla ricerca dei documenti (combinato disposto: art. 18, comma 2, Legge 7 agosto 1990, n. 241; art. 43, commi 1 e 2, D.P.R. 28 dicembre 2000, n. 445).

Se le certificazioni e gli atti di notorietà su stati, qualità personali e fatti restano valide nei rapporti tra privati, occorre sottolineare che nei confronti delle pubbliche amministrazioni e dei gestori di servizi pubblici sono sostituite da «dichiarazioni sottoscritte dall'interessato» (artt. 40, 46 e 47, D.P.R. 28 dicembre 2000, n. 445). Dette dichiarazioni, o l'acquisizione d'ufficio di dati di cui si è detto, sostituiscono ogni altro tipo di documento amministrativo che comprovi i requisiti soggettivi ed oggettivi richiesti (art. 18, comma 3-*bis*, Legge 7 agosto 1990, n. 241, mod. da Legge n. 120/2020, art. 12, comma 1, lett. h), punto 2).

Qualora l'amministrazione procedente intenda contestare le informazioni oggetto di dichiarazioni sottoscritte dall'interessato e diversamente verificarne l'esattezza o la certezza, deve esercitare il potere di accertamento d'ufficio (art. 43, commi 1 e 2, D.P.R. 28 dicembre 2000, n. 445) nei limiti di quanto ivi indicato e contestato (artt. 46 e 47, D.P.R. 28 dicembre 2000, n. 445). A tal fine l'accertamento d'ufficio presso altre pubbliche amministrazioni o presso altri gestori di servizio pubblico è qualificato come attività di *rilevante interesse pubblico*.

Tale qualificazione giuridica consente un'attività di consultazione degli archivi *dell'amministrazione certificante* – quella che detiene le informazioni og-

getto di autocertificazione e ora soggetta a verifica – esentando dai limiti posti per l'accesso l'amministrazione procedente (art. 43, comma 3, D.P.R. 28 dicembre 2000, n. 445), anche ove la stessa riguardi dati sensibili (art. 2-*sexies*, comma 2, D.Lgs. n. 196/2003).

L'affermazione di un generale vincolo di legge di effettuare accertamenti d'ufficio di fatti, qualità e stati che sono nella disponibilità dell'amministrazione procedente assume un significato particolare non appena lo si consideri una norma d'attuazione del principio generale di non aggravamento del procedimento (art. 1, comma 2, Legge 7 agosto 1990, n. 241) e di buon andamento dell'azione amministrativa (art. 97, comma 2, Cost.).

Dell'accertamento d'ufficio, sia sui dati in possesso dell'amministrazione procedente sia su quelli detenuti da altre pubbliche amministrazioni o su altri gestori di servizio pubblico, se ne può offrire un'interpretazione che legittimi al tempo stesso un'attività automatica di verifica della certificazione ad opera dell'intelligenza artificiale.

Il vantaggio di quest'ultima è che permette una rielaborazione dei dati secondo una logica e in vista delle future scelte d'amministrazione, ove l'algoritmo – potendo contare sulla rielaborazione di una grande massa di dati (*big data*) (v. capitolo VI, G. CARULLO) – definisce correlazioni tra informazioni che si ritrovano in elevata probabilità, cui la cultura giuridica può assegnare la qualità di presunzioni (*juris tantum* oppure ex lege *juris et de jure*), da cui si possa derivare la conoscenza di fatti ulteriori (art. 2727, c.c.), essendo comprovati da ricorrenze gravi, precise e concordanti (art. 2729 c.c.).

I sistemi di intelligenza artificiale di gestione dei documenti offrono molte utilità: sono in grado di analizzare un testo scritto o parlato per offrire un supporto nella redazione di nuovi documenti, sia nel senso di organizzare quelli ritenuti utili alla redazione di un testo, sia nel senso di arrivare addirittura a proporre un documento nuovo con soluzioni predittive (*infra* par. 3.2).

A partire dall'analisi dei documenti stessi, l'algoritmo può essere allenato per comprenderne la semantica e proporre una frase oppure può rilevare parole chiave o informazioni rilevanti, disponendo l'archiviazione automatica in banche dati o altri sistemi d'archiviazione.

2.5. L'istruttoria non documentale: *Internet of Things*, rilevazioni aerofotogrammetriche o satellitari, *blockchain*, piattaforme, *Applications Programming Interfaces*

Oltre ai documenti informatici, assumono sempre maggiore rilevanza istruttoria i dati da qualunque fonte raccolti, che trovano negli *standard* euro-

pei l'imposizione di *format* comuni che ne assicurano la fruibilità verso l'esterno dell'organizzazione, la leggibilità meccanica nonché la qualità per il tramite del rispetto di standard ISO.

Tutte le istituzioni europee e le amministrazioni degli Stati membri sono così chiamate a raggiungere quella convergenza d'organizzazione che valorizzi: sia il dato in sé – che in forma aggregata (*big data)* – come elemento rilevante per il procedimento decisionale; sia il dato e la sua accessibilità come trasparenza dell'azione amministrativa (*Open Government*, Direttiva Ue n. 1024/2019 del Parlamento e del Consiglio del 20 giugno 2019) (v. capitolo VIII, S. ROSSA).

Così di recente è stato previsto che con decreto del Presidente della Repubblica venga adottata una *Strategia nazionale dati* che identifichi le tipologie, i limiti e le modalità per la condivisione dei dati aggregati (D.Lgs. 7 marzo 2005, n. 82, art. 50-*ter*, comma 4, mod. da Legge n. 120/2020, art. 34, comma 1).

La digitalizzazione dei documenti e dei procedimenti ha valorizzato il dato come unità informativa e ciò ha avviato un percorso di ridefinizione dei processi decisionali verso una logica che fruisce del calcolo probabilistico, elaborati su una base di dati che è la raccolta e la selezione di una considerevole esperienza pregressa.

Il cartaceo non è solo un modo di dare una rappresentazione di un supporto agli atti, che in sequenza costituiscono un procedimento amministrativo, ma indica una logica e un processo decisionale fondati sulla sintesi dei dati rilevanti per una determinata scelta dell'amministrazione sia essa discrezionale o vincolata.

L'operare dell'algoritmo – oltre ogni capacità di calcolo umano – aumenta la precisione e supera la precedente rappresentazione largamente superficiale e soggettiva della realtà, grazie alle molte interconnessioni e alla capacità di rilevare, quando non anche prevedere *in nuce*, l'emergere di nuove dinamiche o tendenze.

L'apporto di rilevatori diretti – come i sensori *dell'Internet of Things* o gli apparecchi satellitari – consentono di raggiungere un grado elevato di rappresentazione della realtà e di precisione nella conoscenza, delle relative evoluzioni o involuzioni, sia per qualità sia per quantità. Essi captano dati da molti punti di vista della realtà esterna, dei *possibili* rapporti causa-effetto, delle interconnessioni tra una scelta e l'altra, offrendo all'amministrazione più di un dettaglio della realtà.

I sensori *dell'Internet of Things* – con la loro reciproca connessione in rete – sono utilizzati dall'amministrazione per rilevare i dati che restituiscono le informazioni rilevanti, per esempio nella gestione del trasporto pubblico o della raccolta rifiuti solidi, ma anche per il monitoraggio ambientale e territoriale,

oppure a fini di sicurezza o inclusione sociale, su cui però ad oggi la sperimentazione è ancora locale e non assurge neppure come linee guida a un progetto nazionale.

Nella raccolta rifiuti solidi urbani, ad esempio, è stato sufficiente inserire dei sensori che rilevassero lo stato di riempimento dei cassonetti per ottenere le informazioni utili a pianificare una raccolta definita – non in modo omogeneo su tutto il territorio e in modo eguale nei diversi giorni della settimana o mesi dell'anno – ma meglio calibrata sulle variazioni di consumo effettivi.

L'*Internet of Things* è stata essenziale anche per la pianificazione dei servizi pubblici locali: nei trasporti, ad esempio, ciò si è concretizzato monitorando i flussi di spostamento della popolazione attraverso l'acquisto dagli operatori di telefonia mobile dei flussi periodici di entrata in metropoli, utili alla definizione dei tempi di fruizione della città (art. 54, comma 6, D.Lgs. 18 agosto 2000, n. 267).

Tenuto conto dei flussi, anche come capacità di autorganizzazione istituzionale delle persone, tali sistemi di rilevazione consentono di integrare il servizio pubblico di trasporto, soprattutto extrametropolitano, con l'uso di un'*app* cittadina di *car sharing* e secondo un modello che mette in crisi la netta contrapposizione tra gestore e consumatore, più che quella tra pubblico e privato.

La raccolta all'interno della città dei dati geo spaziali dei singoli mezzi di trasporto permette di restituire all'utenza le informazioni in tempo reale sul percorso che questi compiono in funzione del traffico orario o di imprevisti che incidono sulla definizione del servizio.

Vi sono poi tecnologie che rilevano dati sulla conformazione del territorio e ne monitorano l'andamento, che può essere ricostruito con riferimento ad un determinato periodo: oggi, un anno o dieci anni or sono. Così le rilevazioni aerofotogrammetriche, il sorvolo di droni, le immagini satellitari, le telecamere fisse poste sulle vie pubbliche, che restituiscono caratteristiche, dettagli o panoramiche del territorio.

L'impiego congiunto di strumenti di rilevazione delle immagini può ad esempio costituire un utile strumento di prevenzione o di rilevazione degli abusi edilizi, come nelle ristrutturazioni che comportino la demolizione e la successiva ricostruzione di edifici, al fine di verificare che siano rispettate le distanze legali, la volumetria, l'altezza e l'area di sedime della precedente struttura (art. 2-*bis*, comma 1-*ter*, D.P.R. 6 giugno 2001, n. 380).

Anche attraverso i sistemi di *Internet of Things* l'intelligenza artificiale consente di creare banche dati che possono venire alimentate da una archiviazione automatica, con la riorganizzazione delle informazioni sulla base delle caratteristiche ricorrenti che vengono classificate per gruppi omogenei (*cluster*).

La tecnologia *blockchain* – di recente rinominata tecnologia «*basata su regi-*

stri distribuiti» (art. 8-*ter*, Legge 11 febbraio 2019, n. 12; Legge n. 120/2020, art. 26, comma 3) – permette invece il tracciamento univoco e immutabile di sequenze di dati (ad es. transazioni) (v. capitolo VI, G. CARULLO). Nella fase istruttoria l'utilizzo della *blockchain* può quindi consentire ad esempio il controllo dei requisiti di legittimazione, delle condizioni di ammissibilità e dei presupposti rilevanti per l'emanazione del provvedimento (art. 6, Legge 7 agosto 1990, n. 241).

Così l'identificazione di colui che ha la disponibilità dell'immobile o di altro bene iscritto a pubblici registri (es. pubblico registro automobilistico), ove è dalla legge assunto come fatto di legittimazione a compiere un determinato atto giuridico (es. permesso di costruire; es. tassa automobilistica; sanzione amministrativa), può essere accertato grazie alla verifica dei dati registrati su di un registro distribuito (ad es. verificando l'*hash* associato ad un determinato documento). Come meglio si vedrà nel capitolo VI, il particolare procedimento che un algoritmo segue per generare un *hash* permette di identificare univocamente il documento cui è associato. La *blockchain* è da ultimo (Legge n. 120/2020, art. 26, comma 3) individuata come tecnica per assicurare l'autenticità, l'integrità, l'immodificabilità, la leggibilità e la reperibilità di documenti informatici resi disponibili dall'amministrazione.

Le piattaforme di *process service* consentono poi l'accertamento dei requisiti di legittimazione per la scelta del contraente, come nel caso degli acquisti su piattaforma MePA. Quelle di *task service* consentono invece l'autenticazione dei soggetti per qualsiasi procedimento amministrativo, come il *Sistema Pubblico per l'Identità Digitale* (SPID) (v. ancora il capitolo VII, S. D'ANCONA e P. PROVENZANO). Quelle di *data service* permettono infine l'accesso a fonti di dati raccolti nel perseguimento delle finalità istituzionali pubbliche, come i dati anagrafici raccolti dai singoli Comuni e che oggi sono quasi totalmente fruibili sulla piattaforma nazionale di *Anagrafe Nazionale della Popolazione Residente* (ANPR) grazie all'attribuzione ad ogni cittadino di un codice identificativo univoco che garantisce sia la circolarità anagrafica, sia l'interoperabilità con altre banche dati pubbliche (art. 62, comma 3, D.Lgs. 7 marzo 2005, n. 82, mod. da Legge n. 120/2020, art. 30, comma 1, lett. a), punto 3).

Sono utili allo *scarico massimo dei dati* le *Application Programming Interfaces* – APIs (art. 50 *ter*, comma 2, D.Lgs. 7 marzo 2005, n. 82, mod. da Legge n. 120/2020, art. 34, comma 1) che permettono l'accesso automatizzato ai sistemi informativi delle amministrazioni per lo sviluppo di nuovi servizi (v. capitolo VI, G. CARULLO). L'utilizzo delle *Application Programming Interfaces* agevola perciò uno "scarico massivo" e aggiornato dei dati, coadiuvando il processo di raccolta ed elaborazione degli stessi da parte delle amministrazioni ai fini dell'istruttoria procedimentale.

La carenza di istruttoria è un vizio degli atti amministrativi – d'eccesso di potere, quando non addirittura una violazione di legge (R. CAVALLO PERIN, 2011, p. 659 s.) – sicché assume una particolare rilevanza l'adeguatezza degli strumenti conoscitivi messi a disposizione della Pubblica Amministrazione, secondo gli standard tecnici utili a ciascun procedimento.

2.6. Le interconnessioni tra banche dati come strumento per ottenere nuova conoscenza (rinvio al capitolo VI)

Già agli inizi degli anni duemila, si iniziava a intuire il valore conoscitivo sia delle banche dati singolarmente analizzate, sia del valore derivante dalla loro interconnessione (V. BUSCEMA, 2003, p. 2443 s.).

Gli algoritmi predittivi che oggi possono essere utilizzati anche dalla Pubblica Amministrazione permettono di sfruttare la capacità conoscitiva tratta dalle banche dati documentali o da quelle che giornalmente solo alimentate dai sensori *Internet of Things,* secondo una logica del tutto nuova (M. FALCONE, 2017, p. 423). L'analisi dei dati può essere svolta attraverso l'individuazione di correlazioni e modelli ricorrenti selezionati – manualmente o automaticamente da un algoritmo – attraverso l'incrocio di differenti basi di dati e secondo una logica inferenziale.

La Pubblica Amministrazione, grazie all'utilizzazione di algoritmi predittivi, valorizza il proprio vasto patrimonio di beni immateriali, sviluppando una conoscenza che – a partire dagli elementi informativi sui fatti rilevanti che essa ha avuto sinora a disposizione – apre alla comprensione della complessità. Gli algoritmi consentono all'amministrazione pubblica di raggiungere livelli di conoscenza di maggiore potenza, di grande precisione e intima attenzione ai fatti, ma soprattutto al modo di percepirli degli individui e delle loro formazioni sociali in cui si svolge la loro personalità, una capacità che permette – come vedremo – di dare attuazione al principio di buona amministrazione.

Nei sistemi complessi vi è un ordine spontaneo che tali strumenti consentono di evidenziare e di capire nelle dinamiche evolutive che lo caratterizza, di cui l'amministrazione pubblica deve essere a conoscenza per effettuare scelte ad un tempo rilevanti ed effettive, cioè capaci di essere coessenziali alla realtà su cui intendono operare.

Quando si osservano le reti – in particolare quelle più eterogenee e interconnesse – si nota che le stesse cominciano a comportarsi come un tutto organizzato, secondo modalità sorprendenti, ove l'emergere spontaneo dell'ordine è rivelato dai flussi di comportamento di una pluralità di individui.

Algoritmi predittivi che partono dall'analisi delle informazioni contenute in

una banca dati li si trovano sempre più frequentemente nella Pubblica Amministrazione; così ad esempio l'Agenzia delle Entrate che dal 2019 svolge i controlli sulla situazione reddituale e le posizioni contributive utilizzando gli indicatori risultanti dalle percentuali di rischio di evasione che l'algoritmo ha associato ad ogni singolo contribuente.

Lo stesso dicasi per le applicazioni di tecniche di *data mining* al fine dell'attività di vigilanza ispettiva messe in atto da parte dell'Istituto Nazionale per la Previdenza Sociale (INPS) per l'individuazione degli evasori degli obblighi contributivi. Ciò è reso possibile grazie ad una gestione integrata dei flussi informativi che provengono da banche dati su dati assicurativi, contributivi, nonché su quelli relativi ai conti individuali e aziendali. Ne consegue che, in caso di anomalie riscontrate, l'INPS può decidere di attivare quei poteri di verifica che le sono propri per accertare il rischio di evasione avanzato dall'algoritmo.

Le banche dati nella fase istruttoria sono dunque essenziali perché in esse sono contenuti tutti gli atti infraprocedimentali volti ad accertare i fatti giuridicamente rilevanti, ma anche gli atti che di tali fatti offrono una valutazione tecnica o veri e propri pareri.

È a partire da questo presupposto che si possono immaginare le nuove applicazioni dell'intelligenza artificiale sulle banche dati: un algoritmo supervisionato può individuare una nuova conoscenza, dopo avere ricevuto le istruzioni di correlare determinati comportamenti noti ad altri fatti di non diretto accertamento, che al pari delle *presunzioni iuris tantum* (art. 2729, c.c.) si caratterizzano per una capacità predittiva che può essere smentita (prova contraria), ma che nel caso dell'algoritmo è misurata anche quantitativamente in ragione di percentuali d'errore, che col tempo assumono valori decrescenti (*infra* par. 3.2).

Analogamente l'algoritmo non supervisionato può, grazie alle interconnessioni tra molteplici banche dati pubbliche (G. CARULLO, 2018, p. 27 s.), indicare nuove classificazioni (*clusterizzazioni*) che il responsabile del procedimento valuta per considerare nuove prospettive istruttorie, mai ipotizzate prima su quel determinato tipo di procedimento.

Potenzialità conoscitive che, per esempio, emergono anche nelle funzioni di polizia di prevenzione dei reati (*XLaw* alla Questura di Napoli) e che sono d'interesse anche per la polizia amministrativa nell'attività di vigilanza (urbanistica, ispettorato del lavoro, ecc.) o di controllo (Corte dei Conti), ove l'analisi delle variabili può essere collegato anzitutto ad un determinato contesto sociale, d'impresa, o burocratico, poiché l'algoritmo consente alla polizia di vedere le connessioni ricorrenti tra la consumazione di alcuni illeciti, le modalità esecutive utilizzate, le vittime o i danni arrecati, permettendo di antici-

pare la propria attività di prevenzione e controllo in un particolare settore che per un certo tempo è considerato a rischio.

Nel campo della "*manutenzione preventiva*" l'installazione di sensori in punti sensibili delle infrastrutture per monitorare la raccolta dati su parametri significativi (ambientali, fisici, chimici, meccanici), soprattutto ove coniugati con l'applicazione di modelli matematici, offrono all'amministrazione informazioni determinanti sui rischi e garantiscono interventi mirati e anticipatori del danno (ANAS, S.p.A. 2019).

La capacità delle tecniche di *machine learning* di classificare i dati messi a disposizione dell'algoritmo consente di individuare caratteristiche simili e di suddividere i dati in classi, raffinando la capacità di decisione futura, poiché la base conoscitiva (storico) offre rappresentazioni significative della realtà che servono alla macchina per elaborare decisioni future.

Il punto di maggiore interesse è il carattere predittivo degli algoritmi che – oltre a dare rilievo a strumenti sempre più sofisticati di rilevazione della realtà – coglie quest'ultima non solo più come fatto in sé considerato, cui giustapporre una scelta d'interesse pubblico, ma come fatti istituzionali compiuti, conosciuti dall'amministrazione pubblica anzitutto come dato organizzato di soggetti che sono portatori di interessi (pubblici, privati o diffusi). Fatti che nel procedimento si affacciano per esempio come requisiti di legittimazione al procedimento (art. 9, Legge 7 agosto 1990, n. 241), di cui il responsabile deve offrire una valutazione preliminare (art. 6, comma 1, lett. a), Legge 7 agosto 1990, n. 241), utile a consentire la partecipazione sin dalla fase istruttoria.

Quanto detto per la fase conoscitiva dei procedimenti amministrativi volti all'emanazione di provvedimenti vale a maggior ragione per i procedimenti di piani, di programmi, o di atti generali, o normativi, per i quali – seppure valgono le particolari norme che ne regolano la formazione (art. 13, Legge 7 agosto 1990, n. 241) – non appare più possibile ipotizzarne l'emanazione a prescindere da una esatta attività istruttoria che dell'amministrare sappia anticipare gli *standard* indispensabili per quel periodo e in quel territorio: come limiti astratti, o anche solo da atto generale.

Il riferimento frequente è anzitutto in sede locale alla pianificazione territoriale o ai programmi di servizio pubblico di trasporto, ove i dati in tempo reale sui flussi di passeggeri e sui livelli del traffico, del meteo o nelle stagioni, consentono all'Amministrazione la definizione di standard e l'aggiustamento repentino di questi per incidere sensibilmente non solo sull'offerta di quel servizio ma, in un'ottica di sistema, sui tempi di fruizione (art. 50, comma 5, D.Lgs. 18 agosto 2000, n. 267) e sulla stessa architettura ed infrastruttura della città.

3. La validità della decisione automatica: tra norme, atti generali e precedenti

3.1. La natura giuridica dell'algoritmo

Opinioni autorevoli ritengono valido l'utilizzo dell'algoritmo nell'adozione di atti amministrativi (da ultimo: Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472), espressione di attività amministrativa (tra le prime T.A.R. Lazio, sez. III-*bis*, 27 marzo 2016, n. 3769), mentre permangono diverse considerazioni sulla natura giuridica dell'algoritmo.

Se alcuni ritengono che le variabili e regole poste nell'algoritmo rappresentino un potere d'organizzazione interno, altri vi ritrovano un autolimite all'esercizio delle funzioni, sicché nella prima ipotesi l'algoritmo avrebbe valore di atto interno (A. USAI, 1993, p. 164) o di "atto strumentale" (A. MASUCCI, 1993, p. 57), al pari di una circolare o di un ordine di servizio, mentre nel secondo si pensa che spieghi effetti verso i terzi come atto generale o come regolamento.

È stato altresì affermato che l'algoritmo – più correttamente il software che lo esegue – rientri nella nozione di documento amministrativo, che include in tale categoria «ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale» (art. 22, lett. d.), Legge n. 241/1990).

La rilevanza pubblicistica dell'utilizzo dell'algoritmo nel procedimento amministrativo, la sua riconducibilità alla nozione di documento amministrativo, garantiscono che anche verso l'atto amministrativo siano riconosciute le posizioni soggettive date nei confronti degli atti autoritativi della Pubblica Amministrazione; per quanto è qui di interesse i diritti di partecipazione e di accesso anche al codice sorgente del software che esegue l'algoritmo (T.A.R. Lazio, sez. III-*bis*, 27 marzo 2016, n. 3769).

Non condivisibile è l'idea che l'algoritmo – al di là della natura giuridica che si voglia assegnare – sia *ex ante* conclusivo del procedimento, poiché un atto generale – *a fortiori* se normativo – non può non avere almeno un ulteriore momento d'accertamento dei fatti che sono rilevanti per ogni singolo caso concreto, il cui fondamento ultimo risiede nell'idea che l'amministrare pubblico sia una funzione costituzionale ineludibile, al pari di quella giurisdizionale e legislativa, anche ove compiuta da una macchina che ha appreso un operare umano, seppure depurato dagli errori e dai pregiudizi.

Ciò chiarito – e in via di prima approssimazione – all'algoritmo si assegna la natura giuridica di atto generale (U. FANTIGROSSI, 1993, p. 56) o di norma a seconda degli effetti giuridici che ad esso si vuole ricondurre, tra cui il più noto è la possibilità di consentire deroghe allo standard d'amministrazione. Del pari nessun dubbio sulla circostanza che l'algoritmo possa materialmente produrre la soluzione che l'amministrazione pubblica intende volere come atto provvedimento.

3.2. L'algoritmo nella definizione della validità degli atti amministrativi

L'accuratezza richiesta nel definire l'algoritmo (supervisionato o non) sono operazioni essenziali poiché influenza il contenuto del provvedimento. Così le regole logico-informatiche, la scelta delle variabili (dette anche parametri), come ad esempio l'età, la residenza, il titolo di studio, le esperienze lavorative, ecc., nonché la selezione e l'inserimento dei dati che permettono di prevedere l'atto digitale.

Oltre a tali operazioni prettamente materiali, la definizione dell'algoritmo è spesso anche il prodotto dell'interpretazione che è data degli enunciati normativi o istituzionali ed è tradotta in variabili e in regole informatiche.

Tali operazioni (materiali e interpretative) assumono una rilevanza centrale, poiché definiscono i passaggi che l'algoritmo deve compiere, siccome esso corrisponde ad una sequenza ordinata di passaggi logici finiti, di operazioni di calcolo che, sulla base di quelle regole informatiche, valuta e gradua autonomamente gli *input* (in entrata) – cioè le variabili, i presupposti di fatto – ed elabora un *output* (in uscita), che è la decisione algoritmica.

Come vedremo, nell'attività vincolata le variabili – che identificano classi di *input* – sono rappresentate dall'interpretazione delle disposizioni (costituzionali, di legge, di regolamento, ecc.) e dai criteri che in quelle disposizioni sono indicati come, ad esempio, età, residenza, titolo di studio, esperienze lavorative, ecc., che definiscono l'emanazione del provvedimento amministrativo in senso sia procedimentale sia sostanziale.

Nell'attività discrezionale, invece, le variabili sono individuate come classi di *input*, ricavate dall'analisi delle casistiche pregresse affinché l'algoritmo possa assumere una decisione nel merito.

Superando le iniziali resistenze, che non immaginavano l'uso degli algoritmi nell'attività discrezionale, si può ora affermare che anche gli algoritmi possono essere utilizzati: sia nella fase istruttoria, sia nella fase integrativa dell'efficacia, in modo non molto diverso da come si verifica per l'attività vincolata.

Nondimeno nella fase decisionale, l'apporto algoritmico si può sostanziare

in una proposta del contenuto discrezionale del provvedimento elaborata sulla base della combinazione dei precedenti applicativi e dei presupposti che ricorrono in concreto, nonché tra il contenuto discrezionale del provvedimento che l'amministrazione intende adottare e il fine di interesse pubblico concreto che l'amministrazione intende soddisfare con quella misura.

L'apporto algoritmico – sulla base dei precedenti casi – verifica l'osservanza del principio di proporzionalità tra presupposti in concreto e contenuto discrezionale che intende assumere l'amministrazione, ivi compresi i limiti che il giudice ha dichiarato nel caso d'impugnazione del provvedimento.

Tuttavia, in entrambe le ipotesi, la precisione del modello è influenzata dalla quantità e dalla varietà della casistica messa a disposizione dello stesso, ossia in base alla rilevanza e alla rappresentatività della banca dati e del *data lake* di riferimento (sul concetto di *data lake* v. capitolo VI, G. CARULLO), più che a seguito di un giudizio di validità sul provvedimento in sé considerato.

L'algoritmo a fini decisionali deve quindi poggiare sulla scelta accurata delle variabili che derivano dalla casistica settoriale di riferimento e quindi, ad esempio, per il settore degli appalti si tratterà di individuare tutte le ipotesi in cui il soccorso istruttorio è stato correttamente esercitato per individuare le ipotesi in cui la domanda del concorrente, che è stata oggetto del potere del soccorso istruttorio, va ammessa alla gara.

Dall'analisi casistica ne deriverà una classificazione dei casi utili in cui il soccorso istruttorio è stato correttamente esercitato perché finalizzato a sopperire a *mere inesattezze*, come la mancata allegazione di documenti quando il contenuto era comunque ricavabile da altri (Cons. Stato, sez. V, 27 marzo 2020, n. 2146; Cons. Stato, sez. V, 16 marzo 2020, n. 1881) o per l'inosservanza delle formalità di firma digitale quando cui sopperisce il sistema d'autenticazione delle persone al portale (Cons. Stato, sez. III, 19 marzo 2020, n. 1963).

Del pari l'analisi della casistica permetterà di individuare i casi in cui, a contrario, il soccorso istruttorio è stato esercitato in assenza dei presupposti e la domanda resta inammissibile quando si ha una *modifica sostanziale della domanda* per mancanza anche parziale dei requisiti di partecipazione (Cons. Stato, sez. V, 9 marzo 2020, n. 1671) o con un'inammissibile presentazione – postuma – del certificato di esecuzione di lavori (Cons. Stato, sez. V, 28 dicembre 2017, n. 6135).

Il supporto algoritmico assume un'indubbia importanza dunque anche per l'attività discrezionale della Pubblica Amministrazione, in ragione dell'opera di classificazione dei fatti rilevanti secondo le differenti qualificazioni normative, da cui l'algoritmo apprende le differenti conseguenze normative che ne derivano ed elabora il provvedimento. Il modello attribuisce al nuovo caso l'etichetta (*label*) corrispondente alla qualificazione normativa che esso ha ap-

preso dalla casistica e quindi qualifichi come abuso edilizio quel caso che presenta le caratteristiche della categoria *sbancamento* o di *nuova costruzione* o che, a contrario, non rilevi un'ipotesi di abuso edilizio se il caso rientra nell'ipotesi di *livellamento* oppure di *opera facilmente rimovibile* (*supra* par. 1.3).

Ogni nuovo caso (es. livellamento o sbancamento; mere inesattezze documentali o modifica sostanziale della domanda) è dall'algoritmo classificato – secondo un'approssimazione probabilistica – in una delle qualificazioni normative (abuso edilizio o non; ammissione od esclusione della domanda di partecipazione alla gara) ed in ragione di tale calcolo probabilistico scaturisce il provvedimento digitale (ordine di ripristino oppure fiscalizzazione; ammissione od esclusione del concorrente alla gara).

La proposta algoritmica – come vedremo (par. 4) – e l'eventuale margine d'errore nella qualificazione normativa che, nel tempo e per effetto della nuova casistica inserita, assume carattere decrescente (20%; 10%), può essere oggetto di un contraddittorio tra i partecipi al procedimento, con risultati che possono portare ad assumere come definitiva la proposta di provvedimento scaturita dall'algoritmo (inteso perciò come atto generale), oppure al contrario come provvedimento d'eccezione di cui si deve offrire una congrua motivazione, infine disponendo la correzione dell'algoritmo nel caso di risultati aberranti.

L'algoritmo assume anzitutto come variabili (casi) della classificazione tutto ciò che si è individuato come limiti al potere a protezione delle libertà o dei diritti fondamentali, che è prescritto dall'ordinamento come nullità dell'atto amministrativo (art. 21-*septies*, Legge 7 agosto 1990, n. 241). Nondimeno l'algoritmo deve assumere come variabili ciò che il diritto ha individuato come casi d'annullabilità per incompetenza, violazione di legge o eccesso di potere dell'atto amministrativo, con l'avvertenza che non è eguale il modo di operare dell'algoritmo nelle ultime due ipotesi d'annullabilità.

L'algoritmo deve essere programmato considerando la casistica creatasi attorno alla violazione di uno standard d'amministrazione che ad un tempo è chiamato ad osservare e – per così dire – ad applicare nel caso concreto.

Affinché la decisione algoritmica non presenti profili di annullabilità per eccesso di potere, l'algoritmo dovrà assumere la logicità e la comprensibilità dell'amministrare come parametro di validità, procedendo poi a compiere – con imparzialità (art. 97, comma 2, Cost.), disciplina e onore (art. 54, comma 2, Cost.) – il concreto atto – di gestione in attuazione dell'indirizzo politico-amministrativo degli organi di governo (art. 4, D.Lgs. 30 marzo 2001, n. 165).

Ogniqualvolta la proposta algoritmica assolva all'esercizio di un'attività vincolata, la validità del provvedimento è predicabile in attuazione degli standard rilevanti per il caso sopposto al suo vaglio, la cui interpretazione è data

dalla classificazione dei casi che definiscono nel tempo l'enunciato generale e astratto.

Nel caso in cui l'algoritmo sia funzionale all'esercizio dell'attività discrezionale, ogni decisione può dirsi legittima sempreché l'amministrazione persegua l'interesse pubblico – così come definito dagli atti d'indirizzo politico – con scelte logiche e comprensibili per i destinatari e i terzi.

3.3. L'algoritmo tra interpretazione e discrezionalità

L'interpretazione per la violazione di legge è l'operazione intellettiva indispensabile per passare da una norma generale ed astratta al caso concreto, poiché la prima rappresenta pur sempre una sintesi della molteplicità dei casi, sicché la definizione delle variabili può non aver tenuto conto di casi meno frequenti o lo stesso enunciato normativo può, in tempi differenti, imporre di ridefinire il peso tra le varie classi.

Il controllo giurisdizionale – come vedremo (par. 4.4.) – si svolge dunque come sindacato sull'esito ottenuto dall'algoritmo, in ragione delle variabili che l'amministrazione ha selezionato, fermo restando che l'attività di selezione e di inserimento delle stesse può essere letterale, come nel caso di numeri indicati direttamente dalla norma, oppure un'interpretazione più complessa che richiede di valutare le variabili e i pesi ad esse assegnati.

Del pari è il ragionamento per l'incompetenza, che non configura una diversa formalizzazione algoritmica, trattandosi pur sempre di una speciale violazione di legge.

Quanto al vizio di eccesso di potere – al di là dell'ipotesi infrequente dello sviamento – lo stesso s'afferma normalmente pel tramite delle figure sintomatiche che limitano le scelte dell'amministrazione pubblica che perciò debbono essere in sé logiche e comprensibili.

Il controllo giurisdizionale – come vedremo (par. 4.4) – si svolge dunque come sindacato sull'esito ottenuto dall'algoritmo, in ragione delle figure sintomatiche che sono tratte dalla casistica in materia (di concessione di servizi pubblici, di incarichi dirigenziali, di procedure concorsuali, ecc.), che l'algoritmo del giudice ha selezionato dalla sua più che centenaria giurisprudenza.

Ciò che si è detto sinora per la violazione di legge, vale *a fortiori* quasi sempre per le ipotesi di nullità, ove la fa da padrona l'interpretazione degli enunciati di legge che definiscono il potere autoritativo. Più di rado si afferma anche l'argomentare per principi, come legittimazione del giudice al bilanciamento tra posizioni soggettive ugualmente tutelate in astratto.

L'argomentare per principi può essere formalizzato dall'algoritmo ricavan-

do dalla casistica – che ha già definito nel tempo conflitti analoghi o opposti – il peso da assegnare a ogni variabile (interessi e posizioni soggettive alla salute, all'istruzione, alla circolazione, ecc.) lasciando all'intermediazione umana del giudice la scelta tra diverse soluzioni ritenute di bilanciamento ritenute tutte ragionevoli.

Quanto alla scelta discrezionale si può affermare in generale che la stessa è annullabile ove sia illogico o incomprensibile il modo con cui l'amministrazione abbia deciso di perseguire l'interesse pubblico nel caso concreto e a tal fine nella nostra cultura giuridico amministrativa sono state individuate alcune figure sintomatiche – tra cui, ingiustizia manifesta, contraddittorietà intrinseca o estrinseca, disparità di trattamento di situazioni eguali, violazione della prassi, incompletezza dell'istruttoria, travisamento dei fatti, inosservanza dei parametri di riferimento per lo svolgimento dell'azione – che ben possono costituire *variabili* casistiche rilevanti per ciascun settore di azione dell'amministrazione.

In particolare la scelta discrezionale dell'amministrazione pubblica è frequentemente espressa dall'algoritmo configurato come atto generale (standard derogabile), oppure come scelta d'intelligenza – da intendersi come unica per quel caso concreto – che l'algoritmo assume in ragione degli atti d'indirizzo ma soprattutto delle precedenti scelte sino a quel momento effettuate dall'amministrazione pubblica. Ciò avviene considerando in rapporto diretto le scelte d'intelligenza che si considerano analoghe; argomentando invece a contrario per quelle che all'algoritmo sono state presentate come opposte.

In quest'ultimo caso dell'*intelligere* per "quel" caso concreto, sono segnati dalla casistica anche i limiti insuperabili entro i quali l'amministrazione pubblica compie – con imparzialità (art. 97, comma 2, Cost.), disciplina e onore (art. 54, comma 2, Cost.) – i concreti atti di gestione in attuazione dell'indirizzo politico-amministrativo degli organi di governo (art. 4, D.Lgs. 30 marzo 2001, n. 165), limiti che l'algoritmo giudiziale attraverso i precedenti indica come parametri di logicità e comprensibilità dell'amministrare nell'interesse pubblico (vizio d'eccesso di potere).

4. La decisione automatizzata

4.1. Sull'opacità e sul difetto di motivazione dell'algoritmo

Le riflessioni sviluppatesi intorno al tema della decisione amministrativa automatizzata (E. CARLONI, 2020, p. 2 s.; S. CIVITARESE MATTEUCCI, 2019, p. 8 s.; R. FERRARA, 2019, p. 775 s.; D.-U. GALETTA, J.G. CORVALÁN, 2019, p. 10 s.; G. AVANZINI, 2019, p. 35 s.) sono state accomunate dalla generale

perplessità verso l'opacità dei meccanismi decisionali sottesi alla logica algoritmica, caratterizzata da una prudenza verso l'ammissibilità della digitalizzazione dei procedimenti amministrativi.

Chiarita la legittimazione o base legale dell'atto informatico (par. 1; par. 4.2), la questione che emerge come particolarmente rilevante – talora confusa con la precedente – è quale cultura debba disciplinare la decisione amministrativa assunta con l'algoritmo e le conseguenti controversie: il diritto o l'informatica, aprendo uno scenario noto di opzioni del rapporto scienza e diritto, di cui la consulenza tecnica d'ufficio, o la perizia in sede penale, sono ipotesi più note di assegnazione di taluni aspetti, talora molto rilevanti, delle decisioni giurisdizionali alle scienze diverse dal diritto, poiché sezioni specializzate o giudici speciali conoscono da tempo l'inserimento di tecnici tra i giudici amministrativi (per esempio, nel caso del Tribunale Superiore delle Acque Pubbliche).

Del pari, le decisioni algoritmiche, siano esse amministrative oppure giudiziali, aprono – per vie differenti – alle *scienze non giuridiche* al fine di garantire quei diritti che il legislatore europeo ha enucleato a garanzia del destinatario di una decisione automatizzata. In particolare, si afferma che è comunque indispensabile poter ricostruire l'*iter* logico utilizzato nel processo decisionale automatizzato (art. 13, par. 2, lett. f); art. 14, par. 2, lett. g); art. 15, par. 2, lett. h), Regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016), affinché sia conoscibile la ragione della decisione, espressa unicamente in linguaggio informatico.

L'irragionevolezza di una decisione algoritmica assunta per errore di programmazione della procedura di trasferimento di posti di pubblico impiego (docenti di scuola secondaria) ha offerto l'occasione per statuire la piena accessibilità ai codici sorgente dell'algoritmo, ribadendo l'immancabilità dell'attività conoscitiva e decisionale umana, relegando le scienze informatiche a rango servente (T.A.R. Lazio, sez. III-*bis*, 22 marzo 2017, n. 3769).

Altre decisioni digitali hanno offerto la possibilità di esprimersi sulla natura delle stesse, riconoscendo che l'attività amministrativa – svolta dall'algoritmo – è «esercizio di attività amministrativa sostanziale» e come tale va assoggettata alla relativa disciplina, non ultima la Legge 7 agosto 1990, n. 241 (T.A.R. Puglia, sez. I, 27 giugno 2016, n 806).

Sennonché la forte riaffermazione di un primato della decisione umana rischia di non valorizzare le peculiarità della nostra cultura giuridica, ove l'analisi critica dei casi giurisprudenziali ha da tempo forgiato quella cultura capace di rivelare la *ratio decidendi* che – a prescindere dagli *obiter dicta* – fonda la relazione tra fatto e dispositivo, secondo un procedimento logico che è molto vicino al modo di operare degli algoritmi.

Se il diritto ha da tempo consentito di ricavare dal fatto e dalla decisione su quello, la vera ragione di quest'ultima, *a fortiori* ciò è possibile ove si rendano noti: sia i casi (*input*) conferiti all'algoritmo e selezionati come propria base per le decisioni (*data lake*), sia le regole informatiche sottese al suo funzionamento (*rectius*: l'*iter* logico).

In relazione a fattispecie in cui vengono trattati dati personali (v. capitolo II, F. ROSSI DAL POZZO), l'accesso alla casistica usata dall'algoritmo quale base di conoscenza (arg. *ex* art. 15, Regolamento 2016/679/UE) va assicurata a tutela di chi possa subire gli effetti di quella decisione che, conoscendo i dati (*data lake*), potrà valutare l'opportunità di esercitare il diritto di rettifica (arg. *ex* art. 16, Regolamento 2016/679/UE), con diritto di integrare la casistica con ulteriori e "significativi", o di cancellazione dei dati erronei o inattuali (arg. *ex* art. 17, Regolamento 2016/679/UE).

L'opacità dell'algoritmo può essere mitigata fortemente dall'esercizio dei diritti poc'anzi citati, poiché questi – al netto di errori di fatto o di programmazione – garantiscono sia l'accantonamento o incremento dei casi, sia la correzione dei pesi assegnati alle singole variabili e della logica algoritmica, a causa dei quali si sono prodotte soluzioni aberranti – prendendo talora atto della scarsa intellegibilità delle decisioni a suo tempo assunte dall'uomo.

Contrariamente a quanto si pensa l'algoritmo può rivelare la discriminazione contenuta nelle pregresse scelte umane date come *input* al medesimo in determinati settori o periodi (esempio paradigmatico è *Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis*, Case no. 2015AP157-CR, 5 April-13 July 2016, sulla concessione della libertà vigilata, assunta sulla base della decisione elaborata dal software *Compas* e dimostratasi discriminatoria; A. SIMONCINI, 2019b, p. 71).

Quanto al difetto di motivazione (su cui v. il capitolo III, D.-U. GALETTA) lo stesso può essere riferito all'algoritmo come atto amministrativo o all'atto applicativo (decisione amministrativa automatizzata) che ne scaturisce in *automatico*. L'algoritmo come atto amministrativo è stato considerato atto normativo, o quanto meno atto generale, sicché è sufficiente ricordare che è propria della nostra tradizione giuridica che questi non si debbano motivare, anche se eccezioni si sono affacciate negli ultimi anni, con particolare riferimento alle fonti dell'Unione Europea (l'esempio è offerto dai *considerando* che precedono – con funzione di motivazione – il testo di un regolamento o di una direttiva).

Per l'atto applicativo, invece, è possibile ipotizzare che se l'algoritmo è capace di elaborare il dispositivo sulla base della casistica pregressa, lo stesso possa essere programmato affinché ne ponga anche la relativa motivazione per ogni relativo caso concreto.

4.2. La base legale dell'atto digitale e la partecipazione degli interessati

Il significato essenziale del principio di legalità o, nel lessico del diritto dell'Unione Europea la *base legale,* impone che i poteri dell'autorità amministrativa trovino legittimazione in un atto legislativo variamente definito dai relativi ordinamenti (costituzione, legge, trattati, regolamenti, direttive) e ciò è considerato patrimonio della cultura costituzionale comune agli Stati membri, che sono accolti come principi generali dello stesso ordinamento dell'Unione Europea.

La disciplina dell'atto amministrativo informatico non apporta alcuna deroga all'indicato principio, al contrario pone un esplicito rafforzamento dell'ormai coessenziale principio di partecipazione degli interessati al procedimento amministrativo che conduce all'emanazione di un provvedimento.

La disciplina dell'Unione Europea infatti – seppure con riferimento al trattamento dei dati – legittima decisioni automatizzate, purché ricorrano talune condizioni, quali il consenso dell'interessato (art. 6, par. 1, lett. a), Regolamento 2016/679/UE), la necessità di eseguire un contratto (art. 6, par. 1, lett. b), Regolamento 2016/679/UE), l'adempimento da parte del titolare del trattamento di un obbligo legale (art. 6, par. 1, lett. c), Regolamento 2016/679/UE), la salvaguardia di interessi vitali che riguardano l'interessato o altra persona fisica (art. 6, par. 1, lett. d), Regolamento 2016/679/UE), l'esecuzione di un compito per ragioni di interesse pubblico o che sia connesso all'esercizio di pubblici poteri ad esso assegnati (art. 6, par. 1, lett. e), Regolamento 2016/679/UE) o il perseguimento di un legittimo interesse del titolare stesso (art. 6, par. 1, lett. f), Regolamento 2016/679/UE).

Il generale divieto di ricorrere a decisioni *esclusivamente* automatizzate – ossia che non prevedono alcun intervento umano – è superato da una norma di non facile lettura. Si stabilisce dapprima che le decisioni esclusivamente automatizzate sono consentite solo ove ciò sia autorizzato da una norma speciale del diritto dell'Unione o di uno Stato membro oppure qualora vi sia stato il previo *esplicito consenso dell'interessato o per la conclusione o esecuzione di un contratto*, ma per questi due ultimi è salvo il diritto dell'interessato di: *richiedere l'intervento umano*, *di far valere le proprie ragioni, di contestare la decisione* (art. 22, par. 3, Regolamento 2016/679/UE).

Le decisioni esclusivamente automatizzate possono essere autorizzate da una specifica norma dell'Unione o di uno Stato membro se poste a salvaguardia di interessi pubblici come la difesa, la sicurezza nazionale e quella pubblica, l'esercizio della funzione di prevenzione dei reati o per l'esecuzione di sanzioni, il controllo e l'ispezione connessi all'esercizio di pubblici poteri (art. 23, par. 1, Regolamento 2016/679/UE), sia essa dell'Unione Europea oppure dello Stato membro cui è soggetto il titolare del trattamento (art. 22, par. 2, lett.

b), Regolamento 2016/679/UE). Trattasi di autorizzazioni normative che non debbono menomare la tutela «dei diritti, delle libertà e dei legittimi interessi dell'interessato» (art. 22, par. 2, lett. b), Regolamento 2016/679/UE).

L'assenso dell'interessato – l'esplicito consenso o quello necessario alla conclusione o all'esecuzione di contratti tra l'interessato e il titolare del trattamento (art. 22, par. 2, lett. a) e c), Regolamento 2016/679/UE) – non vale acquiescenza alla decisione esclusivamente automatizzata, poiché l'interessato può sempre chiedere l'intervento umano (art. 22, par. 3, Regolamento 2016/679/UE).

Il diritto di contestare la decisione e ancora prima *di far valere le proprie ragioni* sono garanzie già presenti nell'ordinamento italiano da lungo tempo: il primo con i ricorsi amministrativi (D.P.R. n. 1199/1971) e la tutela giurisdizionale contro gli atti della Pubblica Amministrazione (artt. 113 e 24 Cost.); il secondo, già enunciato sin dalle leggi di unificazione amministrativa (art. 3, Legge n. 2248/1865, all. E), ha trovato specificazione con la disciplina sulla partecipazione al procedimento (art. 7 e s., Legge 7 agosto 1990, n. 241), che proprio con riferimento alla fase costitutiva della decisione riconosce ai partecipi l'accesso agli atti, di presentare memorie e documenti (art. 10, Legge 7 agosto 1990, n. 241), infine di presentare osservazioni al manifestato preavviso di rigetto dell'istanza (art. 10-*bis*, Legge 7 agosto 1990, n. 241).

La disciplina europea sul trattamento dei dati rafforza dunque i diritti di partecipazione al procedimento, un procedimento che – esaltato dal progresso tecnologico – può finalmente restituire effettività all'amministrazione pubblica (sul che vedi nel capitolo III, D.-U. GALETTA).

Una partecipazione a ragion veduta, cioè presa visione degli atti del procedimento, che vale altresì come apporto di conoscenza al procedimento (Cons. Stato, sez. VI, 11 aprile 2006, n. 2007) dei destinatari, dei controinteressati, o intervenuti al procedimento; poiché i partecipi sono *ex lege* (art. 10, Legge 7 agosto 1990, n. 241) i legittimi esponenti e gli unici interpreti dei propri interessi, ben inteso dopo la messa a loro disposizione degli esiti della potenza istruttoria dell'amministrazione digitale.

La legge sul procedimento ha così qualificato ogni partecipe (artt. 7 e 10, Legge 7 agosto 1990, n. 241) come unico e insostituibile valutatore dei propri interessi di cui è esponente, a definirli e rappresentarli all'amministrazione procedente, una rappresentazione che l'amministrazione procedente non può sostituire con altra, propria o altrui, anche ove la stessa sia una migliore definizione dell'interesse del partecipe, poiché la legge sulla partecipazione ha negato in radice ogni residua forma "paternalistica" d'amministrazione della cosa pubblica.

Riconosciuta in via di principio la validità di un atto amministrativo come

prodotto esclusivo dell'algoritmo, qualificato come atto amministrativo (T.A.R. Lazio, sez. III-*bis*, 22 marzo 2017, n. 3769), sicché anche all'atto amministrativo digitale s'applica integralmente la disciplina sulla partecipazione per essi prevista.

Più esattamente se la disciplina generale sull'attività amministrativa s'applica all'atto amministrativo digitale – che è stato prodotto dall'algoritmo e vagliato in contraddittorio dai partecipi – ne deriva sul piano logico la legittimazione giuridica dello stesso procedimento digitale che ne precede la definizione.

L'algoritmo all'esito della sua prima programmazione è legittimato dal "*notice and comment*" noto a talune discipline di settore (Autorità Indipendenti), che prevede la previa consultazione degli interessati sull'elaborazione dell'algoritmo.

Una partecipazione iniziale e poi sugli esiti cui è pervenuto l'algoritmo, su cui s'afferma il contraddittorio tra i partecipi al procedimento, che obbliga l'Amministrazione all'interposizione umana ove richiesta dagli interessati, il cui esito è una deroga motivata, oppure una correzione dello standard algoritmico, infine all'opposto motivando il mancato accoglimento delle osservazioni offerte in contraddittorio, assumendo quelle avverse ed a conferma di quanto prodotto dall'algoritmo, esprimendo l'interposizione umana richiesta dalle parti.

Il contraddittorio sulla proposta di provvedimento – caratterizzandosi come momento di partecipazione – non è *ex jure* un aggravio del procedimento (art. 2, Legge 7 agosto 1990, n. 241), favorendo *ex facto:* una integrazione d'eccezione dell'algoritmo, o una sua correzione come atto generale o normativo, individuando quell'attività istruttoria, valutativa, o casistica, che era mancata.

Il procedimento algoritmico e l'atto automatizzato che ne consegue trovano base legale e una generale legittimazione interpretando la disciplina nazionale sulla comunicazione di singoli atti procedimentali (artt. 7, 8, 10-*bis*, Legge 7 agosto 1990, n. 241) in combinato disposto e come disciplina generale di effettività del diritto degli interessati a ottenere un intervento umano (art. 22, par. 3, Regolamento 2016/679/UE), salvo – come si è detto – che norme speciali europee o nazionali autorizzino una decisione esclusivamente algoritmica per le ragioni d'interesse pubblico ivi previste (art. 22, par. 2, lett. b), Regolamento 2016/679/UE; cfr. art. 3-*bis*, mod. da Legge n. 120/2020, art. 12, comma 1, lett. b).

4.3. Indirizzo politico, imparzialità e sistematicità delle decisioni

Il principio di imparzialità (art. 97, comma 2, Cost.) è riferito sia (letteralmente) ai pubblici uffici, dunque all'organizzazione pubblica, sia come specificazione del principio di uguaglianza sostanziale dell'attività amministrativa.

Quest'ultimo assume un significato specifico e simmetrico rispetto al primo ove lo si interpreti come definizione di una natura giuridica (imparziale) degli atti d'istruttoria, degli atti di gestione ed esecuzione delle decisioni degli organi di governo, una natura giuridica che è costituzionalmente contrapposta agli atti di indirizzo politico-amministrativo degli organi di governo (artt. 49 e 114 Cost.; art. 4, D.Lgs. 30 marzo 2001, n. 165).

Atti d'indirizzo politico che sono provvedimenti, atti generali, o regolamenti sull'esercizio delle funzioni o sull'organizzazione a tal fine necessaria (artt. 117, comma 6, 87 comma 5, Cost.), segnando *standard* dell'atto generale che sono validamente derogabili purché motivato ne sia lo scostamento, oppure *standard* inderogabili a cagione dell'astrattezza della norma che impedisce al decisore di accondiscendere al caso concreto (*dura lex sed lex*).

Da qui l'utilità del procedimento algoritmico sopra delineato, che al tempo stesso sia cura d'interessi del caso concreto con conferma, revisione, o deroga degli *standard* d'amministrazione sino a quel momento assunti. Trattasi in definitiva di *standard* di gestione che – in quanto tali – sono sottoposti ad un logorio, di cui occorre avere il monitoraggio, disponendo ove occorra: per l'aggiornamento o per una consapevole conferma.

Il procedimento algoritmico e l'atto amministrativo digitale impongono dunque all'amministrare pubblico di provvedere in modo sistemico, cioè monitorando gli *standard* sino a quel momento definiti, sino al punto di addivenire alla ridefinizione di atti generali o normativi, in ragione del persistente scostamento dai primi, o di ineffettività dei secondi per generale inosservanza delle stesse.

Atti amministrativi digitali che, per tale capacità di monitorare gli standard, possono conformare l'esercizio futuro del potere, ridefinendo i parametri cui l'amministrazione è sottoposta nelle scelte a venire, sottraendo così l'attività a elementi d'incertezza (Cons. Stato, sez. VI, 14 luglio 1978, n. 97) o evidenziando esiti che nel tempo si sono dimostrati discriminatori e sproporzionati. Ne deriva che l'intelligenza artificiale, le reti neurali, in sintesi l'amministrazione digitale, consentono non solo di conoscere ciò che un'amministrazione pubblica è, ma soprattutto come la stessa può ed è capace di divenire con le sue decisioni, i suoi servizi pubblici, la fruizione delle sue banche dati, cioè con la messa a sistema del suo andamento come istituzione (art. 97, comma 2, Cost.), che è elemento costitutivo, essenza, del riconoscimento costituzionale dei pubblici uffici.

Analogamente e con riferimento alla partecipazione dei destinatari – diretti ed indiretti – dell'azione amministrativa, gli algoritmi consentono all'amministrazione pubblica di raggiungere una conoscenza che in assenza di essi non ha mai avuto l'amministrare pubblico, che in sintesi può dirsi di grande preci-

sione sui fatti e d'imparzialità nell'acquisizione degli stessi (per *Internet of Things* vedi *supra* parr. 2.5, 2.6).

Una "attività conoscitiva" che assume una particolare configurazione ove rivolta ad apprendere i fatti-interessi di coloro che sono i possibili destinatari dell'azione amministrativa (Legge 7 agosto 1990, n. 241, art. 7 e s.), poiché in tal caso assume rilevanza giuridica la rappresentazione che di tali interessi hanno i loro titolari. È essenziale perciò che l'algoritmo sappia intendere (*machine learning*, reti neurali, ecc.) quei fatti che sono interessi, così come sono percepiti e intesi dai loro esponenti, poiché la legge ha negato che l'amministrazione possa sostituire tale rappresentazione, anche adducendo che vi siano buone ragioni per una differente e migliore rappresentazione di quanto dagli stessi definito.

In ciò e per ciò vi è attuazione dei principi costituzionali che riguardano la pubblica amministrazione; sia del principio di imparzialità per ciò che attiene all'acquisizione di fatti che non appartengono ad una istruttoria finalizzata all'emanazione di un determinato atto amministrativo; sia di buon andamento dell'azione amministrativa con riferimento alla rappresentazione degli interessi ad opera dei partecipi al procedimento amministrativo.

Dal punto di vista dell'organizzazione pubblica l'effetto di sistema è la maggior capacità d'azione amministrativa, perché agevole è il controllo degli scostamenti dagli *standard*, che può addirittura essere dato a un algoritmo di controllo a ciò opportunamente allenato.

L'opera di sistematizzazione della complessità della realtà di cui è capace l'algoritmo potenzia senz'altro l'analisi conoscitiva dell'amministrazione pubblica e garantisce sia la prevedibilità delle decisioni, sia l'agevole identificazione di «ingiustizie gravi e manifeste».

4.4. Il sindacato sull'algoritmo e la correzione casistica

È di particolare interesse considerare gli strumenti che sono a disposizione dell'interessato per valutare la validità del procedimento algoritmico, con riferimento sia alle regole logiche sottese allo stesso, sia alla qualità degli *input* inseriti.

Il diritto a contestare la soluzione assunta esclusivamente dall'algoritmo apre al sindacato anche di merito dell'amministrazione pubblica proposto con i ricorsi amministrativi (D.P.R. 24 novembre 1971, n. 1199) o alla tutela del giudice ordinario o amministrativo (Legge 20 marzo 1865, n. 2248, all. E; D.Lgs. 2 luglio 2010, n. 104).

La programmazione algoritmica, si è detto, può dare esiti abnormi, oppure irragionevoli o illogici, con necessità di una correzione della base casistica (*data lake*) o delle variabili o delle regole assunte con l'algoritmo.

Il mancato far valere i propri diritti e interessi legittimi nella fase della partecipazione procedimentale non fa decadere il titolare dal diritto di agire in giudizio per la tutela dei medesimi (artt. 24, 113, 102 e 103 Cost.), poiché contrappeso costituzionale dei poteri unilaterali che il medesimo ordine riconosce alla Pubblica Amministrazione (artt. 13 e s., Cost.).

La correzione della casistica contenuta nella banca dati (*data lake*) – a differenza delle variabili e delle regole logiche – è importante per mantenere nel tempo la qualità dei dati (*data quality*) inseriti nell'algoritmo, qualità che è crescente in ragione del livello di complessità che si vuole raggiungere in quel ramo d'amministrazione, o per quel tipo di procedimento amministrativo, che è variamente definito e protetto (verso il basso) dalle norme generali astratte che delimitano le scelte discrezionali dell'amministrazione pubblica.

Il potere di correzione della qualità dei dati, al pari della revisione di variabili e di regole, può essere disposto anche a partire da un procedimento, sia perché l'amministrazione se ne avvede d'ufficio leggendo la soluzione definita dall'algoritmo, sia a seguito della partecipazione degli interessati, sia in ottemperanza della decisione assunta dal giudice ordinario o amministrativo. Il sindacato giudiziale sull'atto amministrativo digitale è differente – si è detto (par. 3.3) – se operato su un'attività vincolata o discrezionale, poiché è condotto nel primo sull'interpretazione che l'amministrazione ha dato nel selezionare le variabili, nel secondo, solo nei limiti del giudizio di logicità e ragionevolezza della decisione assunta.

L'atto amministrativo digitale è annullato qualora l'algoritmo giudiziale abbia offerto una soluzione differente rispetto a quella a suo tempo assunta dall'amministrazione con un proprio algoritmo e sulla base della propria casistica elaborata sulla medesima fattispecie oggetto del sindacato giurisdizionale. Una soluzione che l'algoritmo giudiziale ha avanzato sulla base della precedente casistica elaborata dalla giurisprudenza proprio sulla fattispecie oggetto del giudicato, soluzione che ha messo in rilievo come l'interpretazione delle variabili che l'amministrazione ha condotto si pone in contrasto con le decisioni giudiziali precedentemente assunte, quindi con il peso e con l'interpretazione che su quelle variabili, il giudice ha avuto l'ultima parola.

Qualora l'atto amministrativo digitale – oggetto del sindacato – sia espressione di discrezionalità, l'algoritmo giudiziale si sostanzi in una revisione che tiene conto dei parametri di logicità e di comprensibilità della scelta, in ragione dell'analisi della casistica (che in tal caso sarà data dalle sentenze pregresse) su cui è stato allenato l'algoritmo giudiziale, individuando le figure sintomatiche dell'eccesso di potere (*cluster*) di ogni procedimento, segnalando in via particolare il contrasto con le migliori prassi istituzionali di quell'amministrazione pubblica o perché non abbia assecondato l'indirizzo politico espresso per quel procedimento dagli organi di governo.

4.5. Rapidità e conservazione negli algoritmi

Connessa alla ripetitività dell'algoritmo è la rapidità delle decisioni dell'amministrazione pubblica che ne conseguono, sia ove un unico algoritmo consenta di mantenere decentrata l'istruttoria e l'esecuzione di una decisione (valersi degli uffici), sia al contrario quando più algoritmi sia posti al servizio dell'autonomia di ciascun ente (comune, provincia, città metropolitana o regione), del decentramento burocratico (es. di un ministero o di altro ente nazionale o regionale).

Seppure con differente rilievo costituzionale l'algoritmo rende possibile una minuta comparazione dell'esercizio delle funzioni nello spazio e nel tempo, offrendo una verifica dell'evoluzione di una pluralità dei centri d'indirizzo politico o delle migliori pratiche innovative create da taluni e poi estese ad altri, infine dà conto della effettiva autonomia di ciascun ente.

Oltre ai già decritti effetti sui procedimenti e sugli atti amministrativi, la digitalizzazione attribuisce un'elevata capacità alla Pubblica Amministrazione nella rapidità delle decisioni grazie alla conoscenza e valutazione dei casi pregressi, alla riorganizzazione a sistema e alla conseguente possibilità di anticipare tendenze rilevanti e ripetitive, facilitando l'emersione di modelli o ricorrenze non individuabili a "occhio nudo".

Una rapidità che certo dipende dal pregresso e non indifferente lavoro di selezione e normalizzazione dei dati, dalla minuta classificazione, dallo sviluppo e dall'allenamento dell'algoritmo su quello specifico *dataset*. Un procedimento di allenamento e progressivo perfezionamento dell'algoritmo che dà all'amministrazione una capacità di analisi della realtà superiore rispetto a quanto è stato sinora possibile.

Rapidità e progressiva attenzione all'esercizio delle funzioni e ai nuovi *particulari* che l'incedere dell'intelligenza artificiale consente di mettere a sistema sotto diversi profili. Anzitutto nell'attività amministrativa l'intelligenza artificiale consente un salto nella complessità dell'amministrare pubblico, mantenendo i suoi riti e procedimenti di cura dell'interesse pubblico, ma rafforzando l'effettività della partecipazione degli interessati.

Dal punto di vista dell'organizzazione pubblica l'intelligenza artificiale consente di dare attuazione scientifica al principio di adeguatezza, differenziazione e sussidiarietà, misurando quantità e qualità delle ricorrenze e ridisegnando l'attribuzione a enti e organi costitutivi della Repubblica italiana (artt. 114, 118, Cost.) delle funzioni in ragione della capacità organizzativa degli stessi di soddisfare il livello d'interessi sovranazionale, nazionale, regionale o ulteriormente locale, imposto in un dato periodo storico e in una data materia (G. ORSONI-E. D'ORLANDO, 2019, p. 600 s.).

Come ci ha ricordato Alan Turing: nessun cibernetico ha mai detto che le valvole pensano, proprio come nessuno ha mai detto che i neuroni pensano. È qui la confusione: a pensare è il sistema nel suo insieme … è la struttura logica di quel sistema, non già la sua particolare forma fisica. (A. HODGES, *Alan Turing. Storia di un enigma*, Bollati Boringhieri, 2014, p. 527, segnalato da L. Cavallo Perin).

Una messa a sistema che l'intelligenza artificiale, così come sinora delineata e diversamente da ciò che si crede generalmente, è da un certo punto di vista essenzialmente incapace d'innovazione; nel senso di quel *revirement* o di quella diversa opinione che il cambiamento dei costumi, il declino di idee un tempo dominanti, lo sviluppo delle tecnologie o della concezione delle cose hanno portato a maturazione.

Per quanto sinora detto l'algoritmo è conservazione, perché razionalizzazione delle pregresse scelte d'amministrazione, essenzialmente tratta dalle stesse che lascia l'innovazione all'intervento umano, ivi compresa alla sua capacità di *intelligere* la definizione degli algoritmi (*data lake*, variabili, regole), innovando radicalmente, sorprendentemente, le scelte preesistenti, con quella prudenza e al tempo stesso creatività che non è sostituibile dall'intelligenza artificiale, poiché quest'ultima dell'intelligenza umana è pur sempre un derivato.

Perciò l'algoritmo è capace di scelta discrezionale in continuità logica con le pregresse, poiché di ciò è capace la predittività, al pari di quanto l'algoritmo, al contrario, non è capace di interpretazione innovativa, essendo la discontinuità – discrezionale o d'interpretazione – una caratteristica propria dell'*intelligere* umano.

Bibliografia

AA.VV., *Smart cities e amministrazione intelligente*, in *Istituzioni del Federalismo*, 2015, p. 4.

AUBY J.B., *Il diritto amministrativo di fronte alle sfide digitali*, in *Istituzioni del Federalismo*, 2019, 3, pp. 619-641.

AVANZINI G., *Decisioni amministrative e algoritmi informatici*, Edizioni Scientifiche Italiane, Napoli, 2019.

BARBARO C., *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?*, in *Questione giustizia,* 2018, 4, pp. 189-195.

BENETAZZO C., *Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazione*, in Federalismi.it, 2020, 16, pp. 1-13.

BERLINGÒ V., *Il fenomeno della datafication e la sua giuridicizzazione*, in *Riv. trim. dir. pubb.*, 2017, 3, pp. 641-675.

BICHI R., *Intelligenza Artificiale tra "calcolabilita" del diritto e tutela dei diritti,* in E.

GABRIELLI e U. RUFFOLO (a cura di), *Intelligenza Artificiale e Diritto*, in *Giur. it.*, numero monografico, luglio 2019, pp. 1772-1778.

BUSCEMA V., *«Data base», sql e reti neurali: un felice connubio*, in *Foro amm. CDS*, 2003, 7-8, p. 2443 ss.

BUSCEMA V., *Discrezionalità amministrativa e reti neurali artificiali*, in *Foro amm.,* 1993, p. 620 ss.

CARLONI E., *AI, algoritmi e pubblica amministrazione in Italia*, in *Revista de los Estudios de Derecho y Ciencia Política*, 2020, 30, pp. 1-12.

CARLONI E., *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni,* in *Dir. pubb.*, 2019, 2, pp. 363-391.

CARULLO G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, Torino, 2018.

CASONATO C., *Intelligenza artificiale e diritto costituzionale: prime considerazioni,* in *Dir. pubb. comp. eu.*, 2019, n. speciale, pp. 101-130.

CASSESE S., *La partecipazione dei privati alle decisioni pubbliche. Saggio di diritto comparato*, in *Riv. trim. dir. pubbl.*, 2007, pp. 3-42.

CAVALLARO M.C., SMORTO G., *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in Federalismi.it, 2019, 16, pp. 1-22.

CAVALLO PERIN R., *Ragionando come se la digitalizzazione fosse* data, in *Diritto amministrativo,* 2020, 2, pp. 305-328.

CAVALLO PERIN R., voce *Violazione di legge*, in *Digesto delle discipline pubblicistiche*, agg. 2011.

CELOTTO A., *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giuridica dell'economia*, 2019, 1, pp. 1-10.

CERULLI IRELLI V., *La tecnificazione*, in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione*, vol. IV, in L. FERRARA e D. SORACE (a cura di), *A 150 anni dall'unificazione amministrativa italiana. Studi*, Firenze University Press, Firenze, 2016, pp. 279-284.

CIVITARESE MATTEUCCI S., *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubb.*, 2019, 1, pp. 5-42.

COGLIANESE C., LEHR D., *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, in *The Georgetown Law Review*, vol. 105, 2017, pp. 1147-1223.

COSTANTINO F., *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data, in Dir. pubb.*, 2019, 1,pp. 43-70.

D'ANGELOSANTE M., *La consistenza del modello dell'amministrazione "invisibile" nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*, in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione*, vol. IV, in L. FERRARA e D. SORACE (a cura di), *A 150 anni dall'unificazione amministrativa italiana. Studi*, Firenze University Press, Firenze, 2016, pp. 155-180.

D'ORLANDO E., *Algoritmi e organizzazione dell'amministrazione locale: come declinare il principio di adeguatezza affrontando la complessità,* in G.F. FERRARI (a cura di), *Smart city. L'evoluzione di un'idea*, Mimesis, Milano-Udine, 2020, pp. 529-552.

DE MINICO G., *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria,* in *Dir. pubb.*, 2019, 1, pp. 89-115.

DELGADO I.M., *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Istituzioni del Federalismo*, 2019, pp. 643-662.

DELGADO I.M., *La riforma dell'amministrazione digitale: un'opportunità per ripensare la pubblica amministrazione,* in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione*, vol. IV, in L. FERRARA e D. SORACE (a cura di), *A 150 anni dall'unificazione amministrativa italiana. Studi*, Firenze University Press, Firenze, 2016, pp. 133-154.

DUNI G., *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato nella forma elettronica*, in *Riv. amm. Repubbl. It.*, 1978, p. 407 ss.

FALCONE M., *Big data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica,* in *Riv. trim. dir. pubb.*, 2017, 3, pp. 601-640.

FALCONE M., *Le potenzialità conoscitive dei dati amministrativi nell'era della "rivoluzione dei dati": il caso delle politiche di eradicazione dell'epatite C*, in *Istituzioni del Federalismo*, 2017, 2, pp. 421-446.

FANTIGROSSI U., *Automazione e pubblica amministrazione. Profili giuridici*, Il Mulino, Bologna, 1993.

FASANO G., *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica,* in *MediaLaws*, 2019, 3, pp. 234-241.

FERRARA R., *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in *Diritto amministrativo*, 2019, p. 4.

FERRARI G.F., *L'idea di Smart City*, in G.F. FERRARI (a cura di), *La prossima città*, Mimesis, Milano-Udine, 2017, pp. 9-48.

GALETTA D.-U., *Open government, Open Data e azione amministrativa*, in *Istituzioni del Federalismo*, 2019, 3, pp. 663-683.

GALETTA D.-U., CORVALÁN J.G., *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?*, in *Federalismi.it*, 2019, 3, pp. 1-23.

GALETTA D.-U., *La pubblica amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?,* in *Ciberspazio e diritto*, 2018, 3, pp. 319-336.

GIANNINI M.S., *L'interpretazione dell'atto amministrativo*, Giuffrè, Milano, 1939.

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

LOSANO M.G., *Il diritto pubblico dell'informatica*, Einaudi, Torino, 1986.

LOSANO M.G., *L'automazione delle procedure gestionali e le banche di dati*, in *L'elaborazione elettronica. Principi di calcolo automatico*, Mondadori – The Open University, Milano, 1979.

Marongiu D., *I dati aperti come strumento di partecipazione al procedimento amministrativo*, in S. Civitarese Matteucci, L. Torchia (a cura di), *La tecnificazione*, vol. IV, in L. Ferrara e D. Sorace (a cura di), *A 150 anni dall'unificazione amministrativa italiana.* Studi, Firenze University Press, Firenze, 2016, pp. 77-94.

MARTINES F., *La digitalizzazione della pubblica amministrazione,* in *Medialaws*, 2018, 2, pp. 146-157.

MASUCCI A., *Digitalizzazione dell'amministrazione e servizi pubblici on line. Lineamenti del disegno normativo*, in *Dir. pubb.*, 2019, 1, pp. 117-151.
MASUCCI A., *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Giappichelli, Torino, 2011.
MASUCCI A., *L'atto amministrativo informatico: primi lineamenti di una ricostruzione*, Jovene, Napoli, 1993.
MORO P., *Algoritmo e pensiero giuridico. Antinomie e interazioni*, in *Medialaws*, 2019, 3, pp. 11-22.
MOROLLO F., *Documento elettronico fra e-government e artificial intelligence (AI)*, in Federalismi.it, 2015, 2, 1-30.
MUSSELLI L., *La decisione amministrativa nell'età degli algoritmi: primi spunti*, in *Medialaws*, 2020, 1, pp. 18-28.
NATALE A., *Introduzione. Una giustizia (im)prevedibile?*, in *Questione giustizia*, 2018, 4, pp. 7-16.
NOTARMUZI C., *Il procedimento amministrativo informatico*, in www.astrid-online.it, 2006.
OROFINO A.G., *L'esternazione informatica degli atti amministrativi*, in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione*, vol. IV, in L. FERRARA e D. SORACE (a cura di), *A 150 anni dall'unificazione amministrativa italiana. Studi*, Firenze University Press, Firenze, 2016, pp. 181-200.
OROFINO A.G., *L'informatizzazione dell'attività amministrativa nella giurisprudenza e nella prassi,* in *Giorn. dir. amm.*, 2003, p. 1371 ss.
OROFINO A.G., *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in *Foro amministrativo* CDS, 2002, 9, p. 2256 ss.
ORSI BATTAGLINI A., *Attività vincolata e situazioni giuridiche soggettive,* in *Id., Scritti giuridici*, Giuffrè, Milano, 2007, p. 1249 ss.
ORSONI G., D'ORLANDO E., *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Istituzioni del Federalismo*, 2019, 3, pp. 593-617.
OTRANTO P., *Decisione amministrativa e digitalizzazione della p.a.*, in *Federalismi*, 2018, 2, pp. 1-27.
PATRONI GRIFFI F., *La decisione robotica e il giudice amministrativo*, in A. CARLEO (a cura di), *Calcolabilità giuridica*, Il Mulino, Bologna, 2017.
PESCE G., *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, in www.giustizia-amministrativa.it, 2020.
PESCE G., *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, ESI, Napoli, 2018.
PICOZZA E., *Politica, diritto amministrativo and artificial intelligence*, in E. GABRIELLI e U. RUFFOLO (a cura di), *Intelligenza Artificiale e Diritto*, in *Giur. it.*, numero monografico, luglio 2019, pp. 1761-1771.
PIETRANGELO M., *Le pubbliche amministrazioni sul web tra comunicazione, consultazione e partecipazione*, in S. CIVITARESE MATTEUCCI, L. TORCHIA (a cura di), *La tecnificazione*, vol. IV, in L. FERRARA e D. SORACE (a cura di), *A 150 anni dall'unificazione amministrativa italiana. Studi*, Firenze University Press, Firenze, 2016, pp. 95-111.

QUATTROCOLO S., *Equità del processo penale e automated-evidence alla luce della convenzione europea dei diritti dell'uomo,* in *Revista Ítalo-Española de Derecho Procesal*, 2019, 2, pp. 1-17.

RANELLETTI O., *Principii di diritto amministrativo*, Luigi Pierro Editore, Napoli, 1902.

RESTA G., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del Diritto*, 2019, 2, pp. 199-236.

SAITTA F., *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo,* in *Riv. dir. amm. elettr.*, 2003, pp. 1-28.

SIMONCINI A., SUWEIS S. [a], *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale,* in *Rivista di filosofia del diritto*, fasc. 1, 2019, pp. 87-106.

SIMONCINI A., SUWEIS S. [b] *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 1, pp. 63-89.

SIMONCINI A., SUWEIS S. [c] *Profili costituzionali dell'amministrazione algoritmica*, in *Riv. trim. dir. pubb.*, 2019, 4, pp. 1149-1188.

STRADELLA E., *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, in *Medialaws*, 2019, 1, pp. 73-92.

TERRACCIANO G., *L'applicazione in campo giuridico delle reti neurali artificiali. Il programma "GiuriNet"*, in *TAR*, 1998, pp. 497-509.

TRESCA M., *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in *Medialaws*, 2018, 3, pp. 240-252.

USAI A., *Le elaborazioni possibili delle informazioni. I limiti alle decisioni amministrative automatiche*, in G. DUNI (a cura di), *Dall'informatica amministrativa alla teleamministrazione*, Ist. Poligrafico dello Stato, Roma, 1992, p. 55 ss.

USAI A., *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in *Dir. inf.*, 1993, p. 163 ss.

ZAFFARONI E., *L'informatizzazione della pubblica amministrazione,* in *Foro amm.*, 1996, 7/8, pp. 2516-2555.

ZENO-ZENCOVICH V., *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2018, 2, pp. 32-38.

V.

IL DOCUMENTO INFORMATICO E IL PROTOCOLLO INFORMATICO

Stefano D'Ancona

1. Cenni in merito alle nozioni di *fatto*, *atto* e *documento* e al requisito della forma scritta dell'atto e della sua sottoscrizione

Prima di affrontare la specifica tematica del documento informatico, va osservato come, in termini generali, il documento costituisca il prodotto essenziale dell'organizzazione amministrativa. Ogni Pubblica Amministrazione produce quotidianamente un'ingente quantità di documenti.

La nozione di *documento* non va confusa con quella di *atto* o *fatto*. Il documento è la *res*, la cosa, l'entità capace di rappresentare in maniera duratura un fatto o un atto attraverso la percezione di segni o di suoni o di immagini incorporati in essa (A. MASUCCI, 2004). In un certo senso, dunque, il *documento* è la

"veste" formale dell'atto e, in alcuni casi, soprattutto nel settore del diritto civile, assume rilevanza rispetto al tema della validità dell'atto stesso, ove la mancanza di forma è sanzionata, ad esempio, con la nullità.

La stretta connessione tra *documento* ed *atto* non sussiste tra *documento* e *fatto*, considerato che da un *fatto* derivano conseguenze giuridiche a prescindere da elementi formali (si pensi alle conseguenze che derivano *ex* art. 2043 c.c. da un fatto illecito).

Fornite le coordinate del tema, va evidenziato come sia nelle pronunce giurisprudenziali che in dottrina le nozioni di *atto amministrativo* e *documento* siano spesso utilizzate in maniera intercambiabile. Dunque, è necessario prestare particolare attenzione a cosa ci si riferisca effettivamente di volta in volta.

Nel diritto amministrativo, contrariamente rispetto al diritto civile, non esistono norme generali di riferimento rispetto alla necessità che l'atto sia supportato da un documento ai fini della sua validità. Appare dunque necessario soffermarsi sull'analisi dei diversi punti di vista dottrinari in argomento.

Si osserva comunemente che, tranne in casi specifici previsti dalla legge, non esiste un obbligo generale a che gli atti amministrativi siano contenuti in documenti e, dunque, siano rappresentati in maniera scritta. E ciò poiché non va confusa la nozione di *atto* o *provvedimento* amministrativo con quella di *documento* amministrativo (M.S. GIANNINI, 1959), cioè il supporto che contiene l'atto stesso, posto che l'uno non implica la necessità dell'incorporazione nell'altro.

Tuttavia, più di recente alcuni studiosi hanno ipotizzato l'esistenza di un principio di necessaria documentazione di ogni operazione svolta o decisione adottata, a meno che non vi ostino particolari motivi i quali inducano a preferire l'oralità (G. OROFINO, 2008). Questa tesi è stata avallata da alcune pronunce del giudice amministrativo, ove si è evidenziato che alcuni atti possano avere forma orale, quando la legge o altra fonte lo stabilisca (es. ordini di polizia, atto di convocazione previsto dallo Statuto o Regolamento, ecc. Si rinvia a T.A.R. Puglia, Bari, sez. I, 20 maggio 2004, n. 2227, conforme Cons. Stato, sez. V, 22 settembre 1999 n. 1136. Più recentemente T.A.R. Puglia, Bari sez. IV, 2 marzo 2017, n. 1124, che ricollega la necessità di forma scritta alla natura discrezionale dell'atto).

Parallelamente alla necessità della forma scritta dell'atto, e dunque alla sua incorporazione in un documento, altre pronunce riscontrano la necessità anche di un altro elemento da incorporare al documento: la sottoscrizione. Alla mancanza totale della sottoscrizione è stata ricollegata una causa di invalidità dell'atto, considerato che la funzione della sottoscrizione è quella fondamentale di individuare con certezza l'Autorità emanante (sul punto T.A.R. Sicilia, Catania, sez. II, 12 novembre 2019 n. 2713). Aderendo a questa impostazione

in dottrina, la mancanza della sottoscrizione del documento è stata ritenuta ipotesi di nullità ai sensi dell'art. 21-*septies* Legge n. 241/1990: si tratterebbe della carenza di un elemento essenziale dell'atto. Il presupposto di tale tesi è che l'art. 21-*septies* Lege n. 241/1990 rinvierebbe implicitamente al combinato disposto degli artt. 1325 n. 4 e 1350 c.c. relativi alla nullità di alcuni tipi di contratto, per mancanza di forma scritta (sul tema V. CERULLI IRELLI, 2006).

Con riferimento alla mancanza della sottoscrizione nel documento, tuttavia, la Corte Costituzionale pare avere superato le interpretazioni eccessivamente rigoriste. È stato infatti affermato dal Giudice delle Leggi che l'autografia della sottoscrizione è elemento essenziale degli atti amministrativi esclusivamente nei casi in cui esista una espressa previsione legislativa in tal senso, «essendo di regola sufficiente l'individuabilità certa dell'Autorità emanante, in base ai dati del documento» (Corte cost., ordinanza 21 aprile 2000, n. 117).

La giurisprudenza amministrativa ha seguito tale impostazione sottolineando come l'autografia della sottoscrizione non possa costituire requisito di validità giuridica dell'atto amministrativo, allorquando dal complesso dei documenti che lo accompagnano emergono altri elementi che permettono di individuare la provenienza da parte dell'ufficio preposto (Cons. Stato, sez. IV, 11 maggio 2007, n. 2325; sez. IV 5 ottobre 2010, n. 7309; sez. VI, 7 giugno 2011, n. 3414; sez. VI, 10 dicembre 2010, n. 8702; sez. VI, 5 dicembre 2010, n. 7309; sez. VI, 18 settembre 2009, n. 5622; sez. VI, 18 dicembre 2007, n. 6517).

È stato notato a questo proposito che, dal punto di vista normativo, questo principio di de-formalizzazione era già stato inaugurato proprio in quelle norme che, come vedremo nel prosieguo, rappresentano il primo *step* per il passaggio dell'Amministrazione dal documento analogico a quello informatico. Si tratta, in particolare, dell'art. 6-*quater* del D.L. 12 gennaio 1991, n. 6, convertito, con modificazioni, in Legge 15 marzo 1991, n. 80 (con riguardo agli atti degli Enti locali), e dell'art. 3 del D.Lgs. 12 febbraio 1993, n. 39 (con riguardo agli atti di qualsiasi Pubblica Amministrazione).

Queste disposizioni sono state interpretate nel senso che «l'autografia della sottoscrizione non è configurabile come requisito di esistenza o di validità degli atti amministrativi quando, … secondo le suindicate norme, nel caso di emanazione di atti amministrativi attraverso sistemi informatici e telematici, la firma autografa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile» (T.A.R. Piemonte, Torino, sez. I, 3 maggio 2010, n. 2290).

2. Le norme italiane ed europee degli anni '90 in tema di informatizzazione della Pubblica Amministrazione

2.1. La nozione di documento informatico e di firma digitale nella previgente disciplina

Per comprendere come, in questi ultimi anni, il processo di dematerializzazione – cioè la trasformazione dei documenti dal supporto cartaceo a quello informatico immateriale – sia divenuto importante, occorre svolgere un breve *excursus* delle fasi che lo hanno preceduto.

Risalgono agli anni '70 le prime disposizioni finalizzate a consentire alle pubbliche amministrazioni la produzione di documenti amministrativi mediante l'uso di macchine, c.d. provvedimenti automatizzati. Dopo una prima fase, quella della meccanizzazione a mezzo schede e nastri perforati, si avviò una seconda lunga fase, con la diffusione degli elaborati elettronici (M.G. LOSANO, 1969; v. anche G. DUNI, 2007). Fin dai primi anni di quest'ultima si utilizzò il termine *informatica* che deriva dalla combinazione delle espressioni informazione ed automatica (M.G. LOSANO, 1969, v. anche V. FROSINI, 1992).

L'informatizzazione tuttavia non consentiva di trasformare le attività cartacee in attività informatiche, poiché mancavano le norme di copertura per attribuire a queste ultime un pieno valore giuridico e una sicura attribuibilità di essa all'autore (G. DUNI, 2007). E non vi sarebbe stata la dematerializzazione fintanto che non si fossero approvate delle tecniche che assicurassero l'attribuibilità del documento informatico, e quindi dell'atto, al suo autore.

Proprio, per questo, è solamente con l'introduzione delle tecniche elettroniche di sottoscrizione che si avvia la fase della c.d. *telamministrazione* (G. DUNI, 2007). Ci si riferisce, in particolare, a quel metodo più evoluto che permette di sottoscrivere, ossia firmare e crittografare, i documenti informatici. A questo proposito, la scoperta della firma digitale, sviluppata con una tecnologia attribuibile ai matematici statunitensi Rivest, Shamir e Adleman (di qui l'acronimo RSA) fu estremamente importante.

In Italia il dibattito giuridico, a seguito della scoperta, si animò per merito di quella autorevole dottrina che, in un risalente scritto, fece riferimento alla possibilità di firmare elettronicamente i documenti (ci si riferisce a G. Duni, 1978). All'epoca il mondo del diritto ignorava l'istituto della firma mediante l'utilizzo delle tecnologie. In questo senso, l'intuizione di Duni fu di estremo rilievo.

Negli anni '90 il legislatore italiano comprese la necessità, per i documenti amministrativi, di rifarsi a supporti del tutto diversi rispetto a quello cartaceo. Già nella legge generale sul procedimento (Legge 7 agosto 1990, n. 241), dun-

que, si iniziò a prevedere, in maniera esplicita, che nell'ambito della definizione di "documento" rientrassero anche la «rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti» (art. 22 Legge n. 241/1990). Ed è proprio il documento in forma elettronica che rappresenta il passaggio chiave ponendo «una contrapposizione netta tra l'amministrazione attuale nella quale predomina la documentazione cartacea, ed un nuovo modo di amministrare la cosa pubblica che si basa sulla sostituzione della burocrazia cartacea con quella in forma elettronica» (G. DUNI, 2008).

Successivamente, nella legge delega per la razionalizzazione e la revisione delle discipline in materia di sanità, di pubblico impiego, di previdenza e di finanza territoriale (Legge 23 ottobre 1992, n. 421), il legislatore pose le basi per un cambiamento organizzativo. Al comma 1, lett. mm) dell'art. 2 della Legge n. 421/1992 si prevedeva infatti che il Governo adottasse decreti volti «al completamento del processo di informatizzazione delle amministrazioni pubbliche e alla più razionale utilizzazione dei sistemi informativi automatizzati». Ciò, evidentemente, non imponeva il riconoscimento del documento informatico.

In particolare, tra i decreti attuativi della Legge n. 421/1992 fu adottato il D.Lgs. 12 febbraio 1993, n. 39 recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche. Il Governo, in tale provvedimento legislativo, prescrisse che gli atti amministrativi fossero predisposti da tutte le pubbliche amministrazioni «tramite i sistemi informativi automatizzati» (art. 3, comma 1, D.Lgs. n. 39/1993).

Per la validità degli atti emessi fu tuttavia prevista l'apposizione della firma autografa, e che la stessa fosse «sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile» (art. 3, comma 2, D.Lgs. n. 39/1993). L'oggetto della disposizione è il c.d. atto ad elaborazione elettronica, atto che, predisposto dal *computer*, viene stampato e firmato (G. DUNI, 2007). La firma oggetto dell'art. 3, comma 2, D.Lgs. n. 39/1993, non è dunque la firma elettronica, bensì la sottoscrizione autografa del documento analogico prodotto attraverso l'automazione. Si tratta di un atto, evidentemente, assai differente dal documento informatico e che potrebbe essere al più inteso come suo antenato.

È con la c.d. legge Bassanini, ossia Legge 15 marzo 1997, n. 59, che si assiste ad un vero e proprio cambio di passo. In particolare, in quella legge si stabiliva che gli atti, dati e documenti «formati dalla pubblica amministrazione» e dai privati «con strumenti informatici o telematici», nonché la loro archiviazione e trasmissione con strumenti informatici fossero «validi e rilevanti a tutti gli effetti di legge» (art. 15, comma 2, Legge n. 59/1997).

Il comma 2 dell'art. 15 rinviava tuttavia ad un emanando regolamento «i criteri e le modalità di applicazione» al fine di garantire l'applicazione della disposizione (Regolamento che poi, come si vedrà a breve, sarà adottato lo stesso anno).

Si può ritenere che il legislatore abbia dunque mancato l'occasione per definire egli stesso le regole adeguate per garantire l'equiparazione del documento formato con strumenti informatici o telematici a quello su supporto cartaceo.

In attuazione della legge Bassanini (Legge n. 59/1997), il Governo approvò il D.P.R. 10 novembre 1997, n. 513 recante «Regolamento relativo ai criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici».

Nel Regolamento viene finalmente definito il documento informatico quale «rappresentazione» informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lett. a), D.P.R. n. 513/1997).

Deve considerarsi che la dottrina si interroga sulla materialità o immaterialità del supporto informatico e, dunque, del documento informatico. Un illustre studioso, favorevole alla tesi dell'immaterialità, ha sostenuto che il passaggio al documento informatico avrebbe rivoluzionato lo stesso concetto di documento che, per lungo tempo, è stato sviluppato in un mondo che non conosceva la virtualità e presupponeva l'incorporamento nel supporto dei segni rappresentativi del documento (A. MASUCCI, 2004).

A tale impostazione si oppone un altro orientamento secondo il quale il documento informatico sarebbe stato da considerarsi come una *res* modificata attraverso uno strumento informativo, in modo tale da tramandare memoria di uno o più fatti: ne conseguiva, secondo questa impostazione, che il documento informatico non fosse una rappresentazione, ma un'entità informatica che conservava una rappresentazione (C. DI BENEDETTO, S. BELLANO, 2002).

Il riferimento al concetto di «rappresentazione», contenuto nell'art. 1, lett. a), D.P.R. n. 513/1997, sembra tuttavia rafforzare la tesi dell'immaterialità proprio, rispecchiando il passaggio dal documento cartaceo al documento informatico, privo di qualunque supporto e dunque riconducibile alla mera rappresentazione anche "virtuale" (A. MASUCCI, 2004).

All'art. 3 il Regolamento prevedeva che, con D.P.C.M., sarebbero state fissate le regole tecniche per «la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale» dei documenti informatici e all'art. 10 si richiamava l'utilizzo della firma digitale ai fini della validità ed efficacia del documento informatico.

La solidità giuridica del documento informatico veniva attribuita dall'art. 5 del Regolamento ove si prevedeva che il documento informatico, sottoscritto con firma digitale, avesse la medesima efficacia di scrittura privata ai sensi

dell'art. 2702 del codice civile (comma 1) e che il documento informatico, munito dei requisiti previsti dal Regolamento stesso, avesse l'efficacia probatoria prevista dall'art. 2712 del codice civile e soddisfacesse l'obbligo previsto dagli artt. 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

Dunque, si tratta di una disposizione di estremo rilievo in quanto, introducendo l'elemento della firma digitale, parifica il documento informatico al documento cartaceo sottoscritto con firma autografa.

La firma digitale è definita all'art. 1, lett. b) del Regolamento. Essa consiste in una procedura informatica e diventa, come è evidente, l'elemento di novità su cui ruota la stessa nozione di documento informatico, conferendogli validità ed efficacia in termini probatori. Mentre nel documento cartaceo la firma è incorporata nello stesso supporto del testo, nel caso del documento informatico il nesso tra testo e firma è «indipendente» dal supporto ed è del tutto «interno» al contenuto del documento (A. MASUCCI, 2004).

In ogni caso, la funzione della sottoscrizione è la medesima sia nel documento cartaceo che informatico. Da una parte una funzione indicativa, cioè di individuare l'autore del documento; e dall'altra una funzione dichiarativa ossia idonea all'assunzione di paternità del documento da parte di chi sottoscrive (A. MASUCCI, 2004).

2.2. Il documento informatico e le firme elettroniche: cenno alla normativa europea e nazionale in materia di firme e superamento del sistema di unicità della firma digitale

Un breve cenno va compiuto con riferimento al rapporto tra normativa italiana, in cui è evidente il ruolo di supremazia della firma digitale, e la normativa europea.

Successivamente al Regolamento esaminato nel paragrafo che precede (D.P.R. n. 513/1997), a livello europeo fu adottata la Direttiva 1999/93/CE sulle firme elettroniche. La normativa europea scaturisce dall'esigenza di assicurare sicurezza ai rapporti giuridici con riferimento al commercio elettronico e promuovere i servizi della c.d. società dell'informazione.

È importante evidenziare che, differentemente rispetto a quanto era stato previsto dalle norme interne italiane, il legislatore comunitario di allora scelse di prevedere diversi modelli di firma elettronica, non delineando, peraltro, la *species* della firma digitale che rimase prerogativa nazionale. Il legislatore sovranazionale codificò, rispetto ad ogni tipologia di firma, i livelli minimi di garanzia.

La Direttiva 1999/93/CE sembrò sconvolgere il mondo scientifico italiano (G. DUNI, 2006), in quanto, come già esposto, il D.P.R. del 1997 aveva sposato in pieno il sistema della firma digitale. È condivisibile che, in effetti, la direttiva innovò il sistema inaugurando l'idea di un sistema misto, plurale e ispirato alla neutralità tecnologica (G. DUNI, 2006).

Con il successivo D.P.R. 28 dicembre 2000 recante «Disposizioni regolamentari in materia di documentazione amministrativa», che abrogava il D.P.R. n. 513/1997 riproponendo tuttavia molte delle disposizioni in esso contenute, il conflitto tra ordinamento europeo e italiano in materia di firme non fu risolto.

Il nuovo corpo normativo confermò infatti la scelta di privilegio per la firma digitale, nonostante le prescrizioni contenute nella direttiva che, come visto, teorizzavano il principio di neutralità tecnologica e dunque la possibilità di utilizzo di più tipologie di firme elettroniche. Solamente nel 2002, con il D.Lgs. 23 gennaio 2002, n. 10 il legislatore "regolarizzò" il sistema nazionale rinviando ad un emanando Regolamento (art. 13 D.Lgs. n. 10/2002).

In sede di attuazione, col D.P.R. 7 aprile 2003, n. 137, il legislatore governativo ha ripreso sostanzialmente le norme contenute nella Direttiva 13 dicembre 1999, n. 93. Alla firma digitale, si affiancavano dunque la firma elettronica (indicata comunemente come firma semplice), la firma elettronica avanzata e la firma elettronica qualificata (dell'art. 1 del D.P.R.). In seguito, il sistema di firme si è evoluto con l'approvazione in ambito europeo del Regolamento 2014/910/UE in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (c.d. eIDAS), che ha abrogato la Direttiva 1999/93/CE ed è stato recepito in Italia nell'ambito delle norme del Codice dell'Amministrazione digitale, di cui si tratterà approfonditamente nel paragrafo che segue.

3. L'attuale disciplina del documento informatico nella normativa italiana ed europea

3.1. Le nozioni di documento elettronico, documento informatico e documento analogico

Con la Legge 29 luglio 2003, n. 229 il Parlamento delegava il Governo ad adottare norme di riassetto in materia di società dell'informazione. In attuazione dell'art. 10 della Legge, veniva adottato il D.Lgs. 7 marzo 2005, n. 82 ossia il Codice dell'Amministrazione Digitale (CAD).

Le norme del CAD, per quello che interessa in questa sede, si pongono innanzitutto come il superamento delle disposizioni che erano state adottate in

prima attuazione della direttiva in materia di firme elettroniche e su cui ci si è soffermati. Nel CAD sono contenute inoltre le norme essenziali in tema di validità ed efficacia probatoria del documento informatico, anche in rapporto ai diversi sistemi di firma.

Il Codice fornisce la definizione di «documento informatico».

Secondo la formulazione originaria dell'art. 1 del CAD il documento informatico era «la rappresentazione informatica di atti fatti o dati giuridicamente rilevanti» (art. 1, lett. p), CAD). Tale disposizione nel tempo ha subito qualche modifica per cui, secondo la versione attuale, il documento informatico è un "documento elettronico" che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Con il D.Lgs. 30 dicembre 2010, n. 235 il legislatore ha introdotto anche la nozione di documento analogico che è «la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti» (art. 1, lett. p-*bis*), CAD, introdotto dall'art. 1, comma 1, lett. d), D.Lgs. 30 dicembre 2010, n. 235).

A ciò si aggiunga che, il rinvio all'art. 3 del Regolamento eIDAS (Regolamento UE n. 910/2014), contenuto nell'art. 1, comma 1-*bis*, del CAD, introduce nella definizione di documento informatico anche ciò che il legislatore europeo ha inteso con tale dizione: e cioè «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva» (art. 3, n. 35, Reg. eIDAS).

Le norme aiutano a comprendere che la distinzione tra documento informatico e documento analogico è fondata su un elemento di forma, ossia meramente esteriore. Un'autorevole dottrina ha parlato dunque di «atto amministrativo in forma elettronica» per indicare il provvedimento non su carta ma su supporto (G. DUNI, 1978). In questo caso, secondo alcuni, l'atto è definito impropriamente atto "informatico", ed è più corretto rifarsi alla nozione di documento informatico (D. MARONGIU, 2005).

Le norme contenute al Capo II Sezione del CAD, che si tratteranno in specifico nel paragrafo successivo, prevedono i requisiti di validità ed efficacia del documento informatico.

3.2. La firma dei documenti informatici ed il requisito della forma scritta

Le disposizioni del Codice dell'Amministrazione Digitale hanno subito nel corso del tempo diverse modifiche.

Nella parte relativa al documento informatico il CAD è stato integrato e modificato, tra le altre norme, dal D.Lgs. 4 aprile 2006, n. 159, dal D.Lgs. 30

dicembre 2010, n. 235 nonché, in ultimo dal D.Lgs. 26 agosto 2016, n. 179 che attua l'art. 1 della Legge 7 agosto 2015, n. 124 (c.d. legge Madia). Successivamente, sul già complesso reticolo di disposizioni, è intervenuto il legislatore con il D.Lgs. 13 dicembre 2017, n. 217.

Per comprendere quanto sia stata complicata l'evoluzione, basti ricordare i passaggi che hanno portato ad una diversa distribuzione della disciplina relativa al documento informatico, all'interno di differenti disposizioni del CAD.

Il comma 1 dell'art. 20, poi abrogato dal D.Lgs. n. 179/2016, prevedeva che il documento informatico da chiunque formato, nonché la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'art. 71, fossero «validi e rilevanti agli effetti di legge, ai sensi del Codice» (art. 20, comma 1, CAD, prima del D.Lgs. 179/2016). I contenuti della norma, con l'entrata in vigore dell'art. 17 del D.Lgs. n. 179/2016, sono poi andati a confluire nel dettato dell'art. 21, comma 1, CAD, rubricato «Documento informatico sottoscritto con firma elettronica» ove si era previsto che il documento informatico cui è apposta la firma elettronica «soddisfa il requisito della forma scritta» (art. 21, comma 1, prima parte CAD). Con l'art. 21 D.Lgs. 13 dicembre 2017, n. 217 anche questo assetto è stato modificato e le norme contenute nei primi commi dell'art. 21 del CAD, sono andate tutte a confluire nei commi 1-*bis* e seguenti dell'art. 20 dello stesso Codice.

A seguito di questa evoluzione, l'art. 20, comma 1-*bis*, CAD nel testo attualmente in vigore disciplina la validità ed efficacia probatoria dei documenti informatici. Secondo la norma, «il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile [relativo alla scrittura privata con firma autografa, n.d.a.] quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID [Agenzia per l'Italia Digitale, n.d.a.] ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore».

Orbene, secondo l'art. 2702 c.c., la scrittura privata fa piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente riconosciuta. Se la scrittura viene disconosciuta, ai sensi dell'art. 214 c.p.c., da chi l'ha sottoscritta, il terzo che voglia avvalersene «deve chiederne la *verificazione*, proponendo i mezzi di prova che ritiene utili e producendo o indicando le scritture che possono servire da comparazione» (art. 216 c.p.c.).

In relazione al documento informatico l'onere probatorio riferito alla sottoscrizione si inverte, tanto che, secondo un'autorevole dottrina, il rinvio del CAD all'art. 2702 c.c. poteva essere evitato, dal momento che la previsione di cui all'art. 21, comma 1-*ter*, dispone quasi il contrario (G. DUNI, 2008). L'art. 20, comma 1-*ter*, CAD dispone infatti che «l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria». In pratica, vi è un principio di presunzione di firma poiché in tal caso colui al quale appartiene il dispositivo di firma al fine di ottenere il disconoscimento deve provare che altri ha utilizzato la propria firma digitale contro la sua volontà: altrimenti non è possibile il disconoscimento.

Esiste anche nel caso della firma digitale l'istituto della verificazione, e, tuttavia, si distacca in maniera netta da quello previsto all'art. 216 c.p.c. con riferimento alla firma autografa. Nella scrittura informatica, la verificazione consta nella mera procedura di validazione informatica della firma. La peculiare differenza è che detta validazione informatica non consente di accertare chi abbia effettivamente utilizzato il sistema di firma per sottoscrivere il documento. Sicché può accadere che non vi sia coincidenza tra la persona fisica che ha apposto la firma e la persona fisica titolare di detta firma.

Una parte della dottrina evidenzia perciò come l'utilizzo di un dispositivo per apporre la firma elettronica avanzata, qualificata o digitale renda impossibile distinguere la volontà del suo titolare (C.M. BIANCA, 2002, G. FINOCCHIARO, 2000). Se è vero che la firma sarebbe riconducibile al titolare mediante il dispositivo e un certificato di firma, ciò non può escludere che tale dispositivo di firma possa essere stato utilizzato da un terzo. Nella migliore delle ipotesi, il dispositivo di firma potrebbe essere stato affidato al terzo volontariamente, mentre nella peggiore delle ipotesi potrebbe essere andato perduto o essere stato sottratto. Sulla base di tali riflessioni la firma digitale apposta da parte di un soggetto diverso dal titolare della firma non sarebbe da considerarsi una falsificazione in senso proprio. Secondo tale orientamento si tratterebbe piuttosto di un abuso del dispositivo di firma.

Anche per ridurre tali rischi, l'art. 32 CAD dispone tuttavia che il titolare è «tenuto ad assicurare la custodia» e ad «utilizzare personalmente il dispositivo di firma». Inoltre il terzo entrato in possesso del dispositivo di firma, per poter effettivamente sottoscrivere digitalmente un documento con una firma altrui, dovrebbe essere in possesso anche delle relative chiavi di accesso (PIN o altro codice segreto).

Altra parte della dottrina (F. FERRARI, 2007, F. ROTA, 2012, C. SANDEI, 2008) spinge al superamento dei tradizionali meccanismi di disconoscimento riconducibili alla firma autografa. In concreto, si sostiene l'impossibilità di

applicare la normativa relativa al disconoscimento ed alla verificazione della firma autografa. Sarebbe perciò necessario un meccanismo di verificazione che esca dagli schemi tipici della scrittura privata con firma autografa e che sia «*sui generis*, più agevole e maggiormente adeguata alla realtà tecnica dei documenti firmati digitalmente» (C. SANDEI, 2008).

Infine, una più recente tesi propone un'interessante terza via volta al superamento delle prime due. Secondo tale orientamento sarebbe sempre possibile risalire, per mezzo di presunzioni (art. 2727 c.c.), dalla segnatura digitale della scrittura informatica al suo autore (G. BUONOMO, A. MERONE, 2013). Tale corrente dottrinale parte dal presupposto che il fine della verificazione di una firma autografa, piuttosto che della firma elettronica avanzata, qualificata o digitale consiste primariamente nell'accertamento dell'effettiva provenienza di quest'ultimo attraverso elementi che la provino e che integrino la presunzione di cui all'art. 20, comma 1-*ter*, CAD. Questa parte della dottrina afferma che la prova della provenienza della scrittura informatica dovrebbe essere sostanzialmente ripartita tra colui che ha prodotto la scrittura privata e il presunto titolare. La prova che dovrebbe presentare il primo è piuttosto agevole in quanto consta nell'attestato del certificatore legato al documento in oggetto e la certificazione che la chiave privata appartiene al titolare della firma. Invece, il titolare della firma dovrebbe provare di non aver materialmente utilizzato il dispositivo di firma, con i mezzi probatori che di volta in volta appaiano all'uopo consoni, come ad esempio la denuncia di smarrimento o furto del dispositivo di firma antecedente alla sottoscrizione, corredata dalla revoca del certificato. A tal proposito la dottrina sottolinea peraltro che anche nel caso in cui non fosse stata sporta denuncia sarebbe possibile dimostrare il non utilizzo del dispositivo di firma da parte del titolare sulla base di ulteriori elementi. Ad esempio, potrebbe farsi ricorso a quei dati che i fornitori dei servizi di firma registrano al momento della sottoscrizione. Nella fattispecie l'ora, la data e il luogo nel quale è stata apposta la firma potrebbero essere utilizzati come prova per dimostrare che non possa essere stato il titolare del dispositivo di firma a sottoscrivere (digitalmente) un documento in quanto in quella data ora era in un luogo diverso da quello in cui risulti essere stata apposta la firma. Ne consegue che la procedura di verificazione potrebbe in tal caso essere svolta da un esperto informatico onde individuare dettagli tecnici atti a constatare che il dispositivo di firma non possa essere stato utilizzato dal titolare dello stesso.

Nel caso di sottoscrizione diversa da quella elettronica qualificata o digitale, lo stesso comma 1-*bis* dell'art. 20 CAD prevede invece che l'idoneità del documento informativo a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle carat-

teristiche di sicurezza, integrità e immodificabilità. Dunque, il legislatore affida al giudice il potere di ponderare, a seconda delle circostanze del caso concreto, l'affidabilità del documento informatico, in base alle caratteristiche tecniche.

La norma è stata criticata da una parte della dottrina, rilevando che si tratti di un potere di valutazione eccessivamente discrezionale (A. MASUCCI, 2004). Sul punto, pare tuttavia potersi osservare che, trattandosi di una valutazione tecnica, il giudice la potrà esperire in giudizio utilizzando un consulente nominato d'ufficio.

Al comma 3, l'art. 20 CAD rimanda comunque all'AgID il compito di definire, con proprie Linee Guida e secondo l'art. 71 CAD, regole tecniche per la formazione, trasmissione, conservazione, duplicazione riproduzione, validazione temporale dei documenti informativi nonché in materia di generazione di firme. A tali linee guida viene affidata anche la determinazione delle regole tecniche, organizzative e gestionali per garantire l'integrità, la disponibilità e la riservatezza dei dati personali, attinenti ai documenti informatici detenuti dall'Amministrazione.

L'art. 21 CAD definisce ulteriormente la disciplina in materia di documenti informatici. In particolare, con riferimento ai contratti solenni, cioè quelli per cui il legislatore del codice civile ha previsto l'obbligo di stipulazione in forma scritta (art. 1350 c.c.), il CAD stabilisce che il documento informatico deve essere sottoscritto con firma elettronica qualificata o digitale a pena di nullità (art. 21, comma 2-*bis*, CAD). È fatto salvo il caso di sottoscrizione autenticata di cui all'art. 25 CAD.

Si tratta, dunque, di una regola che specifica in termini restrittivi le prescrizioni contenute all'art. 20 CAD che lasciano la facoltà di sottoscrivere con diverse tipologie di firme elettroniche.

Solamente con riferimento ai contratti indicati al n. 13 dell'art. 1350 c.c. il CAD è più permissivo, prevedendo che essi siano validi se sottoscritti con firma elettronica avanzata, qualificata o digitale ovvero siano formati con le ulteriori modalità previste dall'art. 20, comma 1-*bis*, primo periodo (art. 21, comma 2-*bis*, CAD).

Infine, sono fatte salve le regole riferite agli atti pubblici (D.Lgs. 2 luglio 2010, n. 110), e dunque ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Anche i testimoni firmano con la stessa modalità, in presenza del pubblico ufficiale, oppure con firma autografa acquisita digitalmente e allegata agli atti (art. 21, comma 2-*ter*, CAD).

A chiusura della rassegna relativa alle norme in materia di documento informatico e firma vanno svolte alcune considerazioni.

È stato osservato come, nel disegno normativo del CAD riferito al documento informatico, la firma elettronica semplice sia dotata di «una sorta di forma scritta "minore"» (G. ARCELLA, S. CHIBBARO, M.C. CIGNARELLA, M. MANENTE, 2016), rendendo nulli i contratti informatici così sottoscritti. La notazione trova in effetti riscontro nella giurisprudenza: si è affermato ad esempio, in materia di appalti pubblici, che la mancata apposizione sul documento informatico costituente l'offerta economica della firma digitale, bensì della sola marcatura temporale, consente di attribuire certezza legale solo quanto a data e ora della relativa formazione, ma non anche a proposito della relativa provenienza ed integrità. Esclusivamente la firma digitale è idonea al diverso ed ulteriore scopo di «rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico» (T.A.R. Lazio, Roma, sez. III, 2 luglio 2019, n. 8605). E così, è stato affermato che il contratto di avvalimento, la cui forma scritta è richiesta a pena di nullità, può essere prodotto in forma di scrittura privata o attraverso l'uso del documento informatico e, a seconda dei casi, della relativa firma elettronica avanzata, qualificata o digitale *ex* art. 21, comma 2 e 2-*bis*, D.Lgs. 7 marzo 2005, n. 82 (Cons. giust. amm. Reg. Sicilia, sez. giurisd., 19 febbraio 2016, n. 52).

3.3. Dematerializzazione dei documenti analogici e copie digitali

Nelle norme successive (artt. 22 ss.) il CAD detta le regole di "ingaggio" con riferimento ai documenti informatici contenenti copie di atti pubblici o atti privati di documenti analogici. Le norme assumono rilievo in quanto codificano le regole per garantire l'attendibilità di ogni processo di dematerializzare di documenti analogici già esistenti. In secondo luogo, esse mirano a garantire l'immutabilità del documento informatico originato dal processo di dematerializzazione in forma elettronica.

Con riferimento al primo aspetto, il CAD all'art. 22 prevede che i documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere (compresi atti e documenti amministrativi) formati in origine su supporto analogico, spediti o rilasciati da depositari pubblici autorizzati o da pubblici ufficiali, hanno piena efficacia ai sensi degli artt. 2714 e 2715 c.c., se sono formati secondo le disposizioni di cui all'art. 20, comma 1-*bis*, CAD di cui si è già detto.

Si rammenta che, secondo l'art. 2714 c.c. le copie di atti pubblici spedite nelle forme prescritte da depositari pubblici autorizzati fanno fede come l'originale. La stessa fede fanno le copie di copie di atti pubblici originali, spedite da depositari pubblici di esse, a ciò autorizzati. L'art. 2715 c.c. dispone

invece che le copie delle scritture private depositate presso pubblici uffici e spedite da pubblici depositari autorizzati hanno la stessa efficacia della scrittura originale da cui sono estratte.

Secondo l'art. 22 comma 2 CAD le copie per immagine su supporto informatico hanno la stessa efficacia probatoria degli originali analogici se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'art. 71 del CAD stesso.

L'art. 22 del D.Lgs. n. 217/2017 ha introdotto nel CAD un'ulteriore previsione secondo cui la copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informativo abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo (comma 1-*bis* art. 22 CAD). Inoltre, le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale è attestata da un notaio o da altro pubblico ufficiale secondo le Linee Guida (comma 3, art. 22).

In conclusione, le copie informatiche formate secondo le predette disposizioni sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge. Ciò significa che l'Amministrazione gradualmente potrà eliminare gli originali analogici procedendo, secondo le disposizioni sopra rassegnate, alla produzione dei duplicati informatici.

In alcuni casi eccezionali individuati con D.P.C.M., tuttavia, permane l'obbligo di conservazione del documento analogico, per «esigenze di natura pubblicistica» (art. 22, comma 5), oppure, in caso di conservazione sostitutiva, la loro conformità all'originale analogico deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico (art. 22, comma 5, ultima parte).

Agli artt. 23 e 23-*bis* del CAD, il legislatore prescrive le regole inerenti alle copie analogiche di documenti informatici e le copie informatiche di documenti informatici. Le copie su supporto analogico hanno la stessa efficacia probatoria dell'originale informatico se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato (art. 23, comma 1, CAD). Le copie su supporto analogico hanno la stessa efficacia probatoria dell'originale informatico se la loro conformità non è espressamente disconosciuta (art. 23, comma 2, CAD). Resta comunque fermo l'obbligo di conservare l'originale informatico (art. 23, comma 2, secondo periodo CAD), diversamente da quanto disposto dall'art. 22 per i documenti originali analogici.

L'art. 20 del D.Lgs. n. 179/2016 e l'art. 23 D.Lgs. n. 217/2017 hanno introdotto una nuova norma che permette di sostituire l'attestazione del pubblico ufficiale di cui al comma 1 dell'art. 23 CAD. Infatti, il legislatore, ha previsto che sulle copie analogiche di documenti informatici possa essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le Linee Guida, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza tra esso e la copia analogica. I soggetti che procedono all'apposizione del contrassegno rendono disponibili gratuitamente sul proprio sito internet idonee soluzioni per la verifica del contrassegno stesso. Si tratta dunque di una prassi alternativa che garantisce la conformità della copia analogica all'originale informatico e comunque obbliga l'Amministrazione a predisporre un sistema di controllo per il cittadino.

L'art. 23-*ter* CAD rubricato «documenti amministrativi informatici» e introdotto nel CAD a seguito dell'entrata in vigore del D.Lgs. 30 dicembre 2010, n. 235, ha previsto una norma di principio. Secondo la disposizione gli atti formati dalle pubbliche amministrazioni nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare su diversi o identici tipi di supporto, duplicazioni e copie per gli usi di legge (art. 23-*ter*, comma 1, CAD).

Sia il comma 2 che 3 dell'art. 23-*ter* del CAD ribadiscono quanto già previsto nelle norme precedenti a garanzia del processo di dematerializzazione del patrimonio documentale analogico. Secondo la disposizione la copia su supporto informatico di documenti formati dalla Pubblica Amministrazione in origine su supporto analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto (art. 23-*ter*, comma 1-*bis*, CAD). Il comma 3 dell'art. 23-*ter* CAD rinvia all'importanza dell'attestazione di conformità del funzionario a ciò delegato dalle regole organizzative dell'Amministrazione di appartenenza (invece che genericamente pubblico ufficiale).

Il Ministero dei beni e delle attività culturali e del turismo assume competenza in ordine alla definizione delle Linee guida in materia di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni (art. 23-*ter*, comma 4, CAD).

3.4. Le regole tecniche per la formazione del documento informatico e i formati del documento informatico

Con il D.Lgs. 30 dicembre 2010, n. 235, il legislatore delegato modifica il CAD in maniera consistente e fornisce una spinta decisa verso l'attuazione

delle norme codicistiche in materia di documentazione amministrativa.

In particolare, all'art. 57, comma 6, del citato decreto si prevede che le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche, salvo quanto già disposto in materia di firma digitale, siano adottate entro dodici mesi dall'entrata in vigore del decreto stesso.

Seppure con un certo ritardo, dunque, con il D.P.C.M. 13 novembre 2014, in attuazione degli artt. 20, 22, 23-*bis*, 23-*ter*, 40, 41 e 71 del CAD, la Presidenza del Consiglio dei Ministri ha adottato le regole tecniche in materia di formazione trasmissione, copia, duplicazione riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione. Tali norme, insieme al D.P.C.M. 3 dicembre 2013 (regole tecniche per il protocollo informatico) di cui si tratterà oltre, definiscono le regole di riferimento ai fini di una corretta dematerializzazione dei documenti e dei procedimenti.

In concreto, le disposizioni tecniche impattano in modo significativo sulle pubbliche amministrazioni che hanno l'esigenza di riorganizzarsi nella prospettiva di una piena digitalizzazione documentale e di un'acquisita centralità delle procedure di corretta conservazione (E. CARLONI, 2015).

Secondo la normativa tecnica, il «documento informatico» è formato: a) mediante la redazione tramite l'utilizzo di appositi *software* (ad es. un elaboratore di testo); b) acquisizione di un documento informatico per via telematica o su un supporto informatico, acquisizione della copia per immagine su supporto informatico di documento analogico (ad esempio mediante scannerizzazione); c) registrazione informatica delle informazioni risultanti da processi informatici; d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi di dati (art. 3 D.P.C.M.).

Il documento informatico assume dunque diverse forme, dalla più tradizionale ad altre, come quelle di cui alla lett. c) e d). Tanto che, parte della dottrina, ha osservato che con il D.P.C.M. nel momento in cui si prospetta il trionfo del documento informatico, se ne segna anche la crisi (E. CARLONI, 2015). Il documento acquista, in sostanza, una dimensione dinamica abbandonando la rassicurante impostazione statica, propria della tradizione cartacea: sono da considerarsi documenti informatici anche i flussi informativi giuridicamente rilevanti, dei quali va in ogni caso, però, garantita l'immodificabilità (E. CARLONI, 2015).

Il documento informatico assume la caratteristica di immodificabilità se il formato e il contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Nel caso di cui al punto a) le caratteristiche di immodificabilità e integrità sono determinate da una o più delle seguenti operazioni: I) la sottoscrizione

con firma digitale; II) l'apposizione di una validazione temporale; III) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa; IV) la memorizzazione su sistemi di gestione documentale (Protocollo); V) il versamento ad un sistema di conservazione.

Nel caso di documento informatico formato ai sensi della lett. b), le caratteristiche di immodificabilità e integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione di documenti che garantisca l'inalterabilità dei documenti. La stessa cosa con riferimento alle modalità di cui alle lett. c) e d).

Al documento informatico immodificabile vengono associati i metadati che sono stati generati durante la sua formazione. I c.d. metadati sono informazioni relative al documento che ne descrivono determinate caratteristiche come l'identificativo, il riferimento temporale, l'oggetto, il soggetto che ha formato il documento o l'eventuale destinatario.

L'evidenza informativa corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 2 del D.P.C.M., in modo da assicurare: «indipendenza dalle piattaforme tecnologiche, interoperabilità tra i sistemi informativi e la durata nel tempo dei dati in termini di accesso e di leggibilità» (comma 8, art. 3, D.P.C.M.).

Per formato si intende «la convenzione usata per interpretare, leggere e modificare il file» (punto 2 dell'Allegato n. 2 al D.P.C.M.).

Si tratta dunque di un concetto non tanto giuridico quanto tecnologico, che tuttavia garantisce le finalità che persegue il CAD con riferimento ai contenuti dei file e cioè ai dati.

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (ad es. testo, immagini, filmati) e di disporre di funzionalità più specializzate per renderne più facile la creazione, la modifica e la manipolazione. Questo fenomeno ha portato all'aumento del numero di formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano. Ad esempio un formato di file particolarmente diffuso per i documenti di testo è il *Portable Document Format* (PDF) che consente di mantenere inalterati contenuti e layout indipendentemente dalla piattaforma utilizzata per la visualizzazione del file. Al par. 5 il D.P.C.M. prevede diversi formati, a seconda della tipologia di testo.

I formati vanno scelti – e preferiti – in base ad alcune caratteristiche che possano garantire maggiormente i principi dell'interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali. Inoltre i formati vanno scelti dall'Amministrazione in base ad alcuni principi di notevole rilievo e dunque devono possedere alcune caratte-

ristiche: i) apertura; ii) sicurezza; iii) portabilità; iv) funzionalità; v) supporto allo sviluppo; vi) diffusione.

Analizzando con ordine questi caratteri essenziali, con riferimento al primo, un formato si definisce "aperto" quando è conforme a specifiche pubbliche cioè disponibili (rese disponibili dal produttore) a chiunque abbia interesse ad utilizzare quel formato. Sul concetto di formato e dato aperto si tornerà più ampiamente nel capitolo sesto (G. CARULLO), al quale si rinvia.

Le norme fanno poi riferimento alla c.d. «neutralità» rispetto alle piattaforme e dunque alla possibilità di utilizzare il dato con diverse tipologie di software senza alcuna restrizione che possa creare una "discriminazione" tecnologica. La disponibilità delle specifiche tecniche del formato rende possibile la decodificazione dei documenti rappresentati in quel formato, anche in assenza di prodotti che effettuino tale operazione automaticamente.

Per formato "sicuro", invece, ci si riferisce al grado di immodificabilità del file e alla capacità di essere immune dall'inserimento di un codice maligno. Riguardo alla portabilità ci si riferisce poi alla facilità con cui i formati possono essere usati su piattaforme diverse, sia dal punto di vista *hardware* che *software*, inteso come sistema operativo.

Per "funzionalità" si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento.

Il supporto allo sviluppo, infine, si riferisce alle risorse necessarie alla manutenzione e sviluppo del formato, mentre la diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti.

I formati indicati dal legislatore per la conservazione dei documenti informatici sono aggiornati periodicamente.

4. Principi in materia di gestione e conservazione dei documenti informatici

Come attentamente rilevato da un'autorevole dottrina, il pieno riconoscimento giuridico del documento informatico «sarebbe stato poca cosa, se non fosse stato accompagnato da misure infrastrutturali capaci di far circolare in rete i documenti stessi» (A. MASUCCI, 2011).

E dunque la comunicazione elettronica di documenti rappresenta una nuova forma di conoscenza e richiede una determinata infrastruttura tecnica che ne permette la realizzazione. Questo è stato possibile grazie alla telematica. Il ricorso alla tecnologia telematica nella realtà amministrativa ha rappresentato una rivoluzione nella rivoluzione (A. MASUCCI, 2011).

La telematica permette di mettere in rete i diversi organismi, i soggetti pubblici e privati, ma anche i documenti e i dati che essi stessi producono, anche in relazione ai diversi procedimenti. Sotto questo aspetto la rete (M. EIFERT, 2006) diventa l'elemento centrale che permette l'esistenza di "questioni dinamiche" per cui è stato necessario delineare una disciplina giuridica.

Attraverso la rete gli organismi pubblici possono comunicare tra loro e, a loro volta, i cittadini possono comunicare con gli organismi pubblici. È per questo che sia la connessione che gli strumenti quali la posta elettronica certificata possono essere considerati componenti essenziali di un nuovo diritto di cittadinanza digitale.

Come si vedrà nel prosieguo, una delle norme più importanti a questo proposito, che hanno imposto alle amministrazioni di convertire i processi (e i procedimenti), è l'art. 1 della Legge n. 124/2015 che ha codificato il principio del *digital first*, ossia innanzitutto digitale.

Con il superamento del vincolo costituito dai supporti fisici, i bits contenuti nei documenti informatici – e con essi le informazioni – possono essere scambiabili ad una velocità infinitamente più rapida e ciò indubbiamente favorisce l'attuazione dei principi di economicità ed efficienza dell'azione amministrativa.

Ciò dà vita alla realizzazione di un'amministrazione completamente diversa, poiché dotata di altri mezzi, un'amministrazione elettronica (M. EIFERT, 2006 cfr. A. MASUCCI, 2019).

Ma, in disparte queste considerazioni di carattere generale, occorre sintetizzare i principi che devono regolare la gestione e la tenuta dei documenti informatici relativi agli atti e provvedimenti amministrativi.

In via preliminare, si evidenzia che, all'art. 34 CAD, il legislatore ha previsto che, ai fini della sottoscrizione, ove prevista, di documenti informatici «di rilevanza esterna» (e dunque, sicuramente provvedimenti amministrativi) le pubbliche amministrazioni: a) possano svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tal fine l'obbligo di qualificarsi ai sensi dell'art. 29 (recante «Qualificazione dei fornitori di servizi», tra cui, naturalmente, quello di fornitura della firma digitale); b) possono rivolgersi a Soggetti privati che prestano servizi di firma digitale o di altra firma elettronica qualificata, secondo la vigente normativa in materia di contratti pubblici (ossia mediante l'avvio di procedure di gara con cui si scelga l'operatore più adatto).

Una volta che i documenti risultano sottoscritti, interviene la fase di gestione e conservazione degli stessi a carico di ogni pubblica amministrazione.

L'art. 44, comma 1, CAD, rubricato «requisiti per la gestione e conservazione dei documenti informatici», dispone che «il sistema di gestione informa-

tica dei documenti delle pubbliche amministrazioni, di cui all'articolo 52 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è organizzato e gestito, anche in modo da assicurare l'indicizzazione e la ricerca dei documenti e fascicoli informatici attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida» dettate da AgID.

Gli altri requisiti si possono individuare nel corpo del CAD, come ad esempio il principio di certezza dell'identificazione del soggetto che ha formato il documento informatico nell'art. 20, comma 1-*bis*. È evidente che anche il protocollo, da sempre strumento essenziale della gestione, deve garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita.

Al comma 1-*ter*, l'art. 44, CAD invece stabilisce che, in tutti i casi in cui la legge prescrive obblighi di conservazione, anche a carico di soggetti privati, il sistema di conservazione assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida (art. 44 comma 1-*ter* CAD, come mod. dal D.L. n. 76/2020 conv. Legge n. 120/2020).

Infine, il legislatore stabilisce i principi organizzativi della gestione documentale digitalizzata. Il CAD prevede in particolare la distinzione tra responsabile del sistema di gestione e del sistema di conservazione e l'obbligo che queste due figure si coordinino (art. 44, comma 1-*bis*, CAD).

Il responsabile della conservazione opera d'intesa con altre figure (responsabile del trattamento dei dati personali, responsabile della sicurezza, e responsabile dei sistemi informativi) ed è scelto all'interno della struttura organizzativa dell'amministrazione. In alternativa, come accennato, il servizio di conservazione dei documenti informatici può essere affidato ad un soggetto terzo, pubblico o privato, che possa garantire quanto previsto dal comma 3 dello stesso art. 44 (art. 44, comma 1-*quater*, CAD) e che possieda i requisiti di qualità, sicurezza e organizzazione individuati, nel rispetto della disciplina europea, delle Linee Guida di cui all'art. 71 CAD, nonché di un Regolamento adottato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione (art. 34, comma 1-*bis*, CAD come modificato dal D.L. n. 76/2020 conv. Legge n. 120/2020).

Nei paragrafi successivi verranno dunque trattate le modalità di gestione del documento informatico – protocollo e fascicolo – nonché la conservazione.

4.1. La trasmissione dei documenti informatici: flussi in entrata e in uscita. La posta elettronica certificata

La trasmissione dei documenti segna il passaggio dalle questioni statiche, attinenti alla (corretta) formazione del documento informatico rappresentativo di atti, a quelle dinamiche.

La trasmissione consiste nel "passaggio" da un mittente ad un destinatario di determinati documenti o di dati attraverso l'uso della telematica. La trasmissione dei documenti informatici, in quest'ottica, si delinea, più propriamente, come un "flusso" di dati in entrata o in uscita.

La tematica della trasmissione attiene a due profili. Il primo relativo ai soggetti dell'operazione, e cioè mittente e destinatario; e l'altro che riguarda l'oggetto della trasmissione telematica.

Con riferimento al primo aspetto va osservato che il CAD si occupa sia della trasmissione tra Pubbliche Amministrazioni che tra Pubblica Amministrazione e cittadino. All'art. 47 rubricato «trasmissione dei documenti tra le pubbliche amministrazioni», il CAD prevede due modalità di trasmissione dei documenti tra le pubbliche amministrazioni: l'utilizzo della posta elettronica e la cooperazione applicativa.

Tali modalità per l'invio di un documento informatico sono valide ai fini del procedimento «una volta che ne sia verificata la provenienza» (art. 47, comma 1, CAD).

Perciò, per la verifica della provenienza, valgono le comunicazioni: I) sottoscritte con firma digitale o altra qualificata, II) dotate di segnatura di protocollo di cui all'art. 55 D.P.R. n. 445/2000 (*infra*); III) trasmesse attraverso sistemi di posta elettronica certificata; IV) per cui sia comunque possibile accertarne la provenienza in coerenza con la normativa vigente e le Linee Guida adottate da AgID. Da segnalare che tale disposizione esclude in ogni caso la possibilità di utilizzare il telefax.

Con riferimento alle comunicazioni tra Pubbliche Amministrazioni e cittadini (flussi in entrata), vale quanto previsto dall'art. 45 CAD. La disposizione prevede che i documenti trasmessi da "chiunque" ad una Pubblica Amministrazione con qualsiasi mezzo telematico o informatico, «idoneo ad accertarne la provenienza», soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale. Anche in questo caso è esclusa la possibilità di servirsi del telefax.

Similmente, dunque, rispetto alle comunicazioni tra Pubbliche Amministrazioni, nelle comunicazioni tra soggetti pubblici e privati è richiesta la certezza della provenienza e dunque un mezzo di trasmissione certificato (PEC) o

il contrassegno del documento informatico con strumenti di garanzia (firma digitale del privato cittadino).

Sulle modalità di comunicazione di atti, provvedimenti, comunicazioni da parte delle Pubbliche amministrazioni ai cittadini (flussi in uscita), oltre a quanto si esporrà con riferimento all'utilizzo del domicilio digitale (si rinvia al capitolo VII, S. D'ANCONA e P. PROVENZANO), occorre soffermarsi su alcune disposizioni recenti.

In particolare, nel contesto della legge finanziaria per l'anno 2020, il legislatore ha stabilito, a fini di contenimento della spesa pubblica, che, per la notificazione con valore legale di atti, provvedimenti, avvisi e comunicazioni della Pubblica Amministrazione, la Presidenza del Consiglio dei ministri, tramite società pubblica, sviluppa una piattaforma digitale per le notifiche (art. 1, comma 402, Legge 27 dicembre 2019, n. 160).

Le modalità di funzionamento della predetta piattaforma sono state di recente definite dal DL-semplificazioni n. 76/2020, convertito, con modificazioni, dalla Legge 11 settembre 2020, n. 120.

In particolare, l'art. 26, comma 3 del D.L., ha stabilito che il gestore della piattaforma assicura l'autenticità, l'integrità, l'immodificabilità, la leggibilità e la reperibilità dei documenti informatici resi disponibili dalle amministrazioni e, a sua volta, li rende disponibili ai destinatari, ai quali assicura l'accesso alla piattaforma, personalmente o a mezzo delegati, per il reperimento, la consultazione e l'acquisizione dei documenti informatici oggetto di notificazione. In questo nuovo contesto, ciascuna amministrazione individua le modalità per garantire l'attestazione di conformità agli originali analogici delle copie informatiche degli atti, provvedimenti, avvisi o comunicazioni.

A conclusione del presente paragrafo, ci si potrebbe domandare se *internet* risulti, allo stato, l'unico strumento utilizzabile ai fini della trasmissione dei documenti tra cittadino e Pubblica Amministrazione.

In dottrina, in passato, è stato posto in rilievo come la comunicazione da parte del privato all'amministrazione non debba essere necessariamente eseguita mediante tale canale. Si è in particolare osservato che le più moderne legislazioni tendono a superare una visione strettamente "internetcentrica" delle relazioni a distanza fra Pubblica Amministrazione e privato, prevedendo una pluralità di modalità di accesso a distanza alle attività in rete delle pubbliche amministrazioni (A. MASUCCI, 2011).

Tuttavia, ad avviso di chi scrive, la "multicanalità" pare oggi un tema superato. Infatti, la disposizione contenuta nell'art. 45 CAD, come visto, prevede che i documenti siano «trasmessi da chiunque ad una pubblica amministrazione» con «qualsiasi mezzo telematico o informatico» idoneo ad accertarne la fonte di provenienza. Anche se, per vero, la locuzione «qualsiasi» sembra aver perso un rilie-

vo concreto dal momento che, già con l'entrata in vigore del D.Lgs. n. 235/2010, il legislatore ha espunto dalla previsione la possibilità di utilizzare il fax nella trasmissione rendendo di fatto *internet* il mezzo prioritario di comunicazione.

4.2. Il Protocollo informatico e la gestione dei documenti informatici

Al capo III del CAD, il legislatore tratta della gestione e conservazione dei documenti informatici. L'art. 40, comma 1, prevede che le pubbliche amministrazioni formano «gli originali» dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al codice e le Linee guida adottate da AgID.

L'art. 27, comma 1, lett. a), D.Lgs. n. 235/2010 ha in effetti soppresso la locuzione, contenuta nella versione originaria dell'art. 40 CAD, secondo cui le Amministrazioni dovessero procedere alla formazione del documento in originale secondo quanto previsto solamente nei limiti delle «risorse tecnologiche» a disposizione.

Questa linea di tendenza è stata d'altra parte confermata dalla legislazione più recente anche con riferimento ai procedimenti amministrativi, ove all'art. 1, Legge n. 124/2015 (c.d. Legge Madia), il legislatore ha delegato il Governo ad emanare decreti volti a ridefinire e semplificare i procedimenti amministrativi nell'ottica della piena realizzazione del principio «innanzitutto digitale» (*digital first*).

L'art. 40-*bis* CAD disciplina uno degli istituti principali connessi alla gestione dei documenti informatici: il protocollo informatico.

La norma, rimandando all'art. 53 D.P.R. n. 445/2000 per la definizione del concetto della protocollazione (cioè dell'operazione che sta a monte del protocollo), disciplina i documenti che devono essere oggetto di protocollazione. Secondo l'art. 40-*bis* CAD formano «comunque» oggetto di registrazione di protocollo ai sensi dell'art. 53 del D.P.R. n. 445/2000: a) le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica certificata usate da altre Pubbliche amministrazioni (non si richiama espressamente il concetto di PEC ma lo si deduce dal richiamo agli artt. 6 *ter*, comma 1, 47, commi 1 e 3 del CAD stesso); b) le istanze e le dichiarazioni inviate ai sensi dell'art. 65 dai privati (ad esempio per un esposto, o per l'avvio di un procedimento, o una qualsiasi istanza).

Il riferimento alle norme richiamate nello stesso articolo, in particolare gli artt. 6-*ter*, 47 e 65, induce a restringere il campo delle comunicazioni oggetto di protocollazione a quei documenti informatici di cui sia verificata e garantita la provenienza. Ciò perché in queste due norme è imposto l'utilizzo dei mezzi

di sottoscrizione dei documenti informatici che rendono certo e univoco il soggetto che le invia. Ed in particolare ai documenti dell'Amministrazione di «rilevanza esterna» per i quali deve sicuramente essere verificata e garantita la provenienza mediante i sistemi di firma debole o forte (cfr. art. 34 CAD), nonché le istanze o dichiarazioni del privato aventi rilevanza procedimentale (si interpreta così il richiamo all'art. 65 CAD, ma si ritiene possano essere compresi anche gli scritti difensivi di cui all'art. 10, Legge n. 241/1990 o altri scritti a rilevanza infra-procedimentale, come nel contesto della procedura di cui all'art. 10-*bis*, Legge n. 241/1990).

Non sono protocollati i documenti informatici aventi mera rilevanza interna: d'altra parte, con l'abrogazione del comma 2 dell'art. 34 CAD, sembra che il CAD le abbia ritenute "fuori regime".

Occorre a questo punto chiarire cosa si intenda con protocollo informatico. Come intuibile dalla formulazione della norma, il CAD si rifà ad una nozione già ricostruita nel contesto del D.P.R. n. 445/2000 recante «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa». E, in effetti, è quest'ultimo il testo normativo che, per primo, ha disciplinato in maniera evoluta le nozioni in materia di gestione documentale e di protocollo.

Andando dunque a esaminare il Capo IV del D.P.R. n. 445/2000 (artt. 50-70), rubricato «Sistema di gestione informatica dei documenti», si ritrovano le norme utili a integrare le disposizioni del CAD.

A livello organizzativo ciascuna amministrazione deve individuare gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per «grandi aree organizzative omogenee», assicurando uniformi criteri di classificazione e archiviazione (art. 50, comma 4, D.P.R. n. 445/2000). Ciò comporta che, per ogni area organizzativa omogenea, le Amministrazioni dovranno istituire un Ufficio protocollo (con relativa PEC dalla quale inviare le comunicazioni o alla quale farle pervenire). Tale obbligo viene ribadito, come si dirà a breve, nel D.P.C.M. 3 dicembre 2013 che ha attuato in termini tecnici, l'art. 40-*bis* del CAD relativa al protocollo.

In secondo luogo, è il caso di rilevare che l'art. 53 D.P.R. n. 445/2000 non definisce il protocollo, ma l'operazione ad esso connessa, e cioè la «registrazione di protocollo». Ed infatti, secondo la disposizione, per ogni documento ricevuto o spedito le pubbliche amministrazioni effettuano la memorizzazione di informazioni non modificabili. In particolare, ci si riferisce al «numero di protocollo» del documento «generato automaticamente dal sistema e registrato» (il "numero di protocollo" è progressivo e costituito da almeno sette cifre numeriche, ai sensi dell'art. 57 D.P.R. n. 445/2000), alla data di registrazione di protocollo «assegnata automaticamente dal sistema», al mittente, all'oggetto

del documento, alla data e protocollo del documento ricevuto, ecc. (Art. 53, comma 1, D.P.R. n. 445/2000).

Il «sistema di gestione informatica dei documenti» deve garantire la sicurezza e l'integrità del sistema stesso, nonché la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita. Si può affermare che si tratta di un sistema che regola i «flussi documentali» più che i documenti, presi singolarmente in considerazione.

Il sistema inoltre, deve fornire informazioni sul «collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali» (art. 52 D.P.R. n. 445/2000).

Da questa disposizione si comprende che, nella progettazione informatica del protocollo, deve tenersi conto dell'esigenza giuridica di collegare gli atti e i documenti che confluiscono in uno stesso procedimento ai sensi della Legge n. 241/1990.

A questo proposito va sottolineato che nel contesto di un procedimento la protocollazione dovrà permettere l'utilizzo di uno stesso codice che permetta, ad esempio, di identificare e collegare l'istanza che ha avviato il procedimento ad un eventuale parere rilasciato nel contesto dello stesso procedimento, fino al provvedimento che lo ha concluso.

Il sistema deve inoltre consentire il reperimento delle informazioni riguardanti i documenti registrati, nonché la sicurezza e cioè l'accesso alle informazioni da parte dei soggetti interessati nel rispetto della riservatezza (art. 52 D.P.R. n. 445/2000).

Il sistema produce il c.d. "registro giornaliero di protocollo" (art. 53, comma 2, D.P.R. n. 445/2000). Il registro giornaliero è, in un certo senso, la memoria sintetica del protocollo (si tratta di un foglio), giacché è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo di uno stesso giorno.

La protocollazione informatica garantisce dunque in maniera maggiore certezza e sicurezza documentale rispetto al protocollo cartaceo. Si consideri infatti che l'assegnazione delle informazioni nelle operazioni di protocollazione (*in primis* l'assegnazione della data, del mittente e del numero progressivo di protocollo) «è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti da parte dell'operatore» (art. 53, comma 3, D.P.R. n. 445/2000). Ciò rileva se si pensa alle prassi che spesso caratterizzavano la tenuta del protocollo cartaceo, alle quali era connessa un'incertezza del dato rappresentativo (soprattutto la data) riferito ai documenti protocollati.

La seconda operazione descritta dal legislatore del 2000, dopo quella riferita alla registrazione di protocollo, è la «segnatura di protocollo». All'art. 55 D.P.R. n. 445/2000 si prevede che la segnatura, diversamente dalla registra-

zione di protocollo che consta nella produzione di un documento autonomo, ossia il registro giornaliero, è un'operazione che si esegue sul documento stesso (in entrata o in uscita). È, infatti, «l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso» (art. 55, comma 1, D.P.R. n. 445/2000).

Ovviamente la segnatura prevede l'apposizione del numero di protocollo che, come detto, è generato automaticamente al momento dell'uscita o dell'entrata del documento. Dunque, vi è una «contemporaneità» tra protocollazione del documento e segnatura di protocollo sul documento stesso (art. 55, comma 2, D.P.R. n. 445/2000). Sul documento è segnata anche la data del protocollo, l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'art. 50, comma 4, D.P.R. n. 445/2000.

Con il D.P.C.M. 3 dicembre 2013 si è provveduto ad attuare le disposizioni di cui agli artt. 40-*bis*, 41, 47, 57-*bis* e 71 CAD prevedendo regole tecniche per il protocollo informatico. Le operazioni, in esse previste, ai fini della protocollazione sono in sintesi:

a) registrazione: ossia l'assegnazione al documento di un'identificazione univoca al momento dell'immissione nel sistema di gestione documentale. La registrazione è obbligatoria per i documenti richiamati all'art. 40-*bis* CAD (*supra*);

b) segnatura di protocollo: ossia l'apposizione o associazione all'originale del documento in forma permanente non modificabile delle informazioni riguardanti il documento;

c) classificazione: ossia l'organizzazione in modo sistematico dei documenti in categorie strutturate logicamente rappresentate in un piano;

d) fascicolazione: inserimento del documento informatico considerato in una apposita struttura aggregativa, cioè il fascicolo elettronico di cui si tratterà nel paragrafo che segue.

A livello organizzativo il D.P.C.M. conferma che le pubbliche amministrazioni debbano individuare le aree organizzative omogenee e i relativi uffici di riferimento ai sensi dell'art. 50 D.P.R. n. 445/2000 per le operazioni di protocollazione. Per ogni area organizzativa deve essere istituita una casella di PEC direttamente associata al Registro di protocollo (indirizzo pubblicizzato sul sito istituzionale dell'Ente e riportato nel Manuale di gestione e nell'indice delle pubbliche amministrazioni oltre che nel sito istituzionale, cfr. art. 18, comma 3, D.P.C.M.).

È obbligatoria, per ciascuna delle aree organizzative omogenee, la nomina del responsabile della gestione documentale, ed, eventualmente, quando ri-

corrono più aree omogenee, la nomina del coordinatore della gestione documentale (art. 3 D.P.C.M.).

Le norme sulla gestione e conservazione documentale si ispirano al principio di regolazione del procedimento informatico. In questo senso, esistono figure di riferimento che sono: 1) il responsabile del protocollo, 2) il responsabile della gestione documentale, 3) il responsabile dell'archivio, 4) il responsabile della conservazione. I predetti soggetti possono coesistere nella stessa persona che è responsabile della redazione del manuale di gestione.

Secondo il D.P.C.M. ogni Pubblica Amministrazione è obbligata a redigere un manuale di gestione coerentemente con le dimensioni della propria struttura organizzativa. Nel manuale di gestione sono contenute le istruzioni per il corretto funzionamento del servizio di gestione e conservazione dei documenti e per la tenuta del protocollo informatico, dei flussi documentali e degli archivi (art. 5 D.P.C.M.). In pratica, il manuale di gestione non è nient'altro che lo strumento che descrive il sistema di gestione informativa dei documenti. Diversamente il manuale di conservazione illustra l'organizzazione e le infrastrutture per la conservazione dei documenti.

Il sistema di protocollo informatico deve assicurare, secondo le norme tecniche, l'univoca identificazione ed autenticazione degli utenti, la protezione delle informazioni relative a ciascun utente nei confronti degli altri, la garanzia di accesso alle risorse esclusivamente agli utenti abilitati, la registrazione delle attività rilevanti (art. 7 D.P.C.M.). Tutto ciò è garantito dalla qualificazione e dalla tracciabilità degli accessi che presidia il sistema di gestione.

Il registro giornaliero di protocollo, di cui si è detto, deve essere trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendo l'immodificabilità del contenuto (art. 7, comma 5, D.P.C.M.).

Il sistema di protocollo rispetta le regole dell'allegato B del Codice in materia di protezione dei dati personali del quale si tratterà in breve nella parte dedicata ai dati. All'art. 18 il D.P.C.M. stabilisce le modalità di registrazione dei documenti informatici: ad ogni messaggio ricevuto o spedito da una area organizzativa omogenea corrisponde un'unica operazione di registrazione di protocollo, secondo quanto previsto dall'art. 53 D.P.R. n. 445/2000. Alla registrazione vengono associate le ricevute generate dal sistema di protocollo informativo e, nel caso di registrazione di messaggi di posta elettronica certificata spediti, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione. L'eventuale indicazione dell'ufficio utente, ovvero del soggetto destinatario del documento, va riportata nella segnatura di protocollo secondo le modalità di cui agli artt. 20 e 21 del D.P.C.M. stesso (art. 18 D.P.C.M.).

È lasciata libertà organizzativa alle diverse amministrazioni pubbliche sulle modalità di inoltro ed assegnazione dei documenti al singolo ufficio utente che tuttavia devono essere descritte nel manuale di gestione.

4.3. Il fascicolo informatico

Seguendo un ordine logico – ma anche la prospettazione che ci propone il CAD – dopo le operazioni riferite alla protocollazione del documento informatico, viene l'analisi della "fascicolazione". Anche questa operazione rientra, naturalmente, nell'ambito del Capo II sulla gestione del documento e prelude alla conservazione del documento informatico.

Nel procedimento tradizionale l'esigenza per la Pubblica Amministrazione procedente e per le altre interessate, oltre che per i privati, di poter conoscere agevolmente i documenti e gli atti riguardanti il procedimento ha suggerito di tenerli insieme fisicamente dentro una "camicia" (A. MASUCCI, 2011).

Il CAD stabilisce che la Pubblica Amministrazione titolare del procedimento raccoglie in un «fascicolo informatico» gli atti, i documenti e i dati del procedimento medesimo da chiunque formati (art. 41, comma 2, CAD). All'atto della comunicazione dell'avvio del procedimento l'Amministrazione comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'art. 10 Legge n. 241/1990 (deposito memorie e documenti).

Tenendo conto della progressione evidenziata dal legislatore anche nel D.P.C.M. richiamato nel paragrafo precedente, la fascicolazione è dunque l'operazione finale e consiste nell'inserimento del documento informativo in una apposita struttura aggregativa. Si tratta di un insieme virtuale organizzato secondo una struttura logica: non è dunque necessario che la memorizzazione dei documenti riferiti al medesimo fascicolo avvenga sul medesimo supporto informatico per garantire il collegamento funzionale, ma solo che questi documenti siano "conservati" in base ad un'organizzazione logica che li conduca ad un unico insieme (A. MASUCCI, 2011).

Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento e dagli interessati attraverso i servizi di cui all'art. 40 *ter* e all'art. 64 *bis* del CAD stesso.

La prima disposizione prevede la prossima istituzione di un sistema che permetta di individuare documenti contenuti nel protocollo o nei fascicoli, nonché che ne consenta l'accesso *on-line* ai soggetti che ne abbiano diritto ai sensi della disciplina vigente. L'art. 64 *bis* CAD, che già si è analizzato, prevede invece la realizzazione di un punto unico di accesso telematico per il citta-

dino ai servizi forniti dalla Pubblica Amministrazione. Questa modalità di gestione fornisce la possibilità per il cittadino di verificare e conoscere, in maniera immediata, lo stato di avanzamento dei procedimenti per cui è interessato, i documenti depositati dalle Amministrazioni coinvolte e gli atti eventualmente emessi.

Tali facoltà possono considerarsi come una declinazione più specifica del più ampio diritto del cittadino all'uso delle tecnologie di cui all'art. 3, comma 1, CAD. La norma infatti prevede che chiunque abbia il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti previsti dal Codice, nei rapporti con le Amministrazioni, anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo (v. capitolo III, D.-U. GALETTA).

Il fascicolo elettronico consente inoltre anche alle altre amministrazioni coinvolte in un procedimento – amministrazioni diverse da quella procedente – di compiere in maniera diretta e simultanea le attività di propria competenza (si pensi a procedimenti in cui intervengono più amministrazioni rilasciando propri pareri, nulla osta, ecc.). Ciò consente una maggiore efficienza con riferimento ai tempi di conclusione del procedimento e di scambio informativo tra pubbliche amministrazioni (F. COSTANTINO, 2015). Ma anche per l'Amministrazione procedente la possibilità di utilizzare la telematica consente di accedere a basi di dati detenute da altre amministrazioni e di alimentare il fascicolo elettronico con i dati ivi contenuti ritenuti utili (G. CARULLO, 2016).

Bibliografia

ARCELLA G., CHIBBARO S., CIGNARELLA M.C., MANENTE M., *Le modifiche al Codice dell'Amministrazione Digitale*, pubblicazione del Consiglio Nazionale del Notariato, in http://www.dirittoegiustizia.it/allegati/PP_OSS_FirmaElettronicaCad_s.pdf, 2016.

BIANCA C.M., *La firma elettronica, si apre un nuovo capitolo*, in *Studium juris*, 2002, p. 1431 ss.

BUONOMO G., MERONE A., *La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio*, 2013, in https://www.judicium.it/wp-content/uploads/saggi/457/Buonomo,%20Merone.pdf.

CARLONI E., *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in *Giorn. dir. amm.*, 2015, 2, p. 148 ss.

CARULLO G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, Torino, 2017.

CARULLO G., *Big Data e Pubblica Amministrazione nell'era delle banche dati interconnesse, in Concorrenza e mercato,* 2016, p. 181 ss.

COSTANTINO F., (Voce) *Open Government*, in *Digesto discipline Pubblicistiche,* Torino, Utet, aggiornamento 2015.

CERULLI IRELLI V., *Lineamenti di diritto amministrativo*, Giappichelli, Torino, 2006.
DI BENEDETTO G., BELLANO S., *I linguaggi del processo*, Giuffrè, Milano, 2002.
DUNI G., (Voce) *L'amministrazione digitale*, in *Annali I*, *Enc. dir.*, Giuffrè, Milano, 2008.
DUNI G., (Voce) *Teleamministrazione*, in *Enc. giur.*, Roma, 2007.
DUNI G., *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunti per una teoria dell'atto amministrativo emanato nella forma elettronica*, in *Riv. Amm.*, 1978.
EIFERT M., *Electronic Government*, Nomos, Baden Baden, 2006.
FERRARI F., *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. dir. proc. civ.*, 2007, p. 415 ss.
FINOCCHIARO G., *La firma digitale (artt. 2699-2720). Supplemento d.P.R. 10 novembre 1997, n. 513*, in F. GALGANO (a cura di) *Commentario del codice civile Scialoja-Branca*, Zanichelli e Roma Società Editrice del Foro Italiano, Bologna, 2000, p. 30 ss.
FROSINI V., (Voce) *Telematica e informatica giuridica*, in *Enc. dir.,* Giuffrè, Milano, 1992.
GIANNINI M.S., *Atto amministrativo*, in *Enc. dir.*, vol. III, Giuffrè, Milano, 1959.
LOSANO M.G., *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Einaudi, Torino, 1969.
LOSANO M.G., *L'informatica giuridica in Italia*, in *Il Ponte*, XXV, 1969, p. 600 ss.
LOSANO M.G., *Gli studi di Giuscibernetica*, in R. TREVES (a cura di), *Nuovi sviluppi della sociologia del diritto* (1966-1967), Edizioni di Comunità, Milano, 1968, p. 307 ss.
MARONGIU D., *L'attività amministrativa automatizzata*, Maggioli, Rimini, 2005.
MASUCCI A., *Il documento informatico*, in *Riv. dir. civ.*, 2004, 5, p. 10749 ss.
MASUCCI A., *Digitalizzazione dell'amministrazione e servizi pubblici on line*, in *Diritto Pubblico*, 2019, 1, p. 117 ss.
MASUCCI A., *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Giappichelli, Torino, 2011.
OROFINO G., *Forme elettroniche e procedimenti amministrativi*, Cacucci, Bari, 2008.
ROTA F., *Il documento informatico*, in M. TARUFFO (a cura di), *La prova nel processo civile*, in *Trattato di diritto civile e commerciale* diretto da A. CICU-F. MESSINEO-L. MENGONI, Giuffrè, Milano, 2012, p. 723 ss.
SANDEI C., *Valore formale e probatorio del documento informatico alla luce del D.lgs. 4 aprile 2006, n. 159*, in *Nuove leggi civ. comm*., 2008, p. 15 ss.

VI.

DATI, BANCHE DATI, *BLOCKCHAIN* E INTEROPERABILITÀ DEI SISTEMI INFORMATICI NEL SETTORE PUBBLICO

Gherardo Carullo

1. I dati quali nuovi strumenti dell'amministrazione digitale

L'art. 50 del Codice dell'Amministrazione Digitale (CAD) dispone che «i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati».

Tra gli strumenti propri dell'amministrazione digitale possiamo perciò ricomprendere i dati memorizzati su supporto digitale, quale naturale evoluzione che va ad affiancarsi e gradualmente sostituirsi al supporto cartaceo (G.

DUNI, 2008). Mentre gli archivi tradizionali, sino a pochi decenni fa, costituivano pressoché l'unica modalità di conservazione delle informazioni in mano pubblica, gli strumenti offerti dalle tecnologie dell'informazione e della comunicazione permettono l'introduzione, anche nella sfera pubblica, di nuove logiche e meccanismi per la gestione, il mantenimento e lo sfruttamento dei dati delle amministrazioni (F. BENVENUTI, 1992).

Nel trattare di tale fenomeno si deve peraltro prendere atto della vastità delle informazioni che vengono in gioco. In proposito l'ottavo considerando della Direttiva 2019/1024/UE relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, riconosce che «il settore pubblico degli Stati membri raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni in molti settori di attività, per esempio informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione».

Rispetto al contesto cartaceo, l'innovazione digitale muta il rapporto tra l'amministrazione e tali masse di informazioni di cui sono detentrici. I dati assumono una rinnovata dimensione – digitale – dalla quale discendono importanti conseguenze la cui rilevanza può essere apprezzata in rapporto a tutta l'attività amministrativa (G. CARULLO, 2016). Indipendentemente dal settore analizzato, infatti, il rinnovato contesto tecnologico fa sì che la gestione delle informazioni da parte dell'amministrazione digitale avvenga attraverso modalità del tutto nuove rispetto al contesto cartaceo. Per apprezzare l'ampiezza di tale fenomeno, si può avviare il discorso partendo dal concetto stesso di dato, e le sue diverse categorie.

2. Definizione di dato e sue categorie

2.1. La nozione di dato, in senso tecnico, in contrapposizione alla nozione di informazione, intesa quale elemento conoscitivo

Per comprendere per quale motivo la conservazione in forma digitale dei dati rappresenti un elemento di forte innovazione per le pubbliche amministrazioni, occorre tenere presente la distinzione tra il concetto di *dato* e quello di *informazione* tipica del linguaggio tecnico-informatico.

Secondo il vocabolario dell'*International Organization for Standardization* (ISO) relativo alle tecnologie dell'informazione, il termine *data* può essere definito quale rappresentazione reinterpretabile di informazioni in modo formalizzato, idoneo alla loro comunicazione, interpretazione od elaborazione. Possiamo perciò affermare che il concetto di dato è distinto da quello di informa-

zione, essendo quest'ultima il frutto della reinterpretazione di ciò che è rappresentato dal dato. In altri termini, i dati diventeranno informazioni o conoscenza solo quando sono interpretati da esseri umani o, in alcuni casi, da sistemi di intelligenza artificiale.

Tale distinzione assume un particolare rilievo in quanto occorre considerare che i dati sono anzitutto dei beni immateriali che devono essere immagazzinati, elaborati ed interpretati affinché questi possano esprimere un qualche valore conoscitivo. Perché l'amministrazione possa sfruttare il proprio patrimonio informativo conservato digitalmente deve in altre parole essere in grado, anzitutto, di gestire ed utilizzare efficacemente i dati di cui è in possesso.

Sulla base della nozione tecnica di dato si può poi anche distinguere quest'ultimo dal concetto di *documento*. I documenti elettronici sono anch'essi beni immateriali nei quali sono rappresentate una o più informazioni, che anche in questo caso possono esser estratte solo attraverso l'opera interpretativa di un essere umano, o, talora, di un sistema di intelligenza artificiale. In proposito l'art. 23-*ter* del CAD parifica dati e documenti informatici, qualificando entrambi quali fonti di «informazione primaria ed originale».

Occorre peraltro considerare che i documenti elettronici sono a loro volta memorizzati ed elaborati quali sequenze di bit, ossia quali serie di dati. Sicché si può ritenere che anche un documento elettronico sia qualificabile, sotto un profilo tecnico, come un dato (*recte*, un insieme di dati).

In ultima analisi, dunque, quando parliamo di dati delle pubbliche amministrazioni ci riferiamo ad un elemento digitale, e quindi immateriale, che permette la memorizzazione e lo scambio di informazioni di qualsiasi tipo. Dette informazioni possono riferirsi al semplice nominativo di un soggetto, così come, a seconda dei casi, a più complesse fattispecie.

2.2. Categorie di informazioni rilevanti nel settore pubblico

Data la varia natura e le diverse tipologie di informazioni di cui le pubbliche amministrazioni possono venire in possesso (J.B. AUBY, 2018), al fine di operarne una classificazione si possono richiamare le categorie identificate dal *Libro Verde sull'informazione del settore pubblico nella società dell'informazione* (Libro Verde sull'informazione, COM(1998) 585).

Il Libro Verde sull'informazione introduce anzitutto la distinzione tra «informazioni amministrative» ed «informazioni non amministrative». La prima categoria «si riferisce alle funzioni governative e dell'amministrazione stessa; la seconda, all'informazione sul mondo esterno, raccolta nell'esecuzione di un pubblico mandato». Rientrano in tali nozioni, ad esempio, gli albi, elenchi,

pubblici registri ed ogni altra raccolta di dati concernenti stati, qualità personali e fatti. Queste categorie presuppongono un collegamento con un potere pubblico in quanto, per quanto riguarda le informazioni amministrative, si tratta di informazioni senza le quali l'amministrazione non potrebbe operare, mentre quelle non amministrative presuppongono in ogni caso che le stesse siano state acquisite in esecuzione di un pubblico mandato.

In secondo luogo, il Libro Verde sull'informazione distingue tra «informazioni che sono fondamentali per il funzionamento della democrazia (come leggi, cause in tribunale, informazioni parlamentari)» e altre informazioni «prive di un carattere così fondamentale». Questa distinzione è utile per sottolineare l'importanza che determinati dati hanno non solo per l'amministrazione che ne è depositaria, ma anche per il pubblico. Il che, dunque, può avere una precisa valenza in relazione alla disciplina della trasparenza in quanto può connotare certi dati di una particolare rilevanza esterna.

Che le informazioni delle pubbliche amministrazioni possano essere di grande interesse per i privati è del resto espressamente confermato dallo stesso Libro Verde sull'informazione che, secondo altra prospettiva, distingue le informazioni detenute dalle pubbliche amministrazioni proprio in base a quelle che «interessano il grande pubblico (come le informazioni parlamentari)» e quelle che, viceversa, riguardano «un gruppo ristretto con un interesse diretto». Il che, dunque, in tema di trasparenza può trovare corrispondenza in relazione ai diversi strumenti di ostensione delle informazioni, attraverso l'istituto dell'accesso civico (D.Lgs. n. 33/2013), ovvero l'accesso procedimentale (Legge n. 241/1990) (v. capitolo VIII, S. ROSSA).

Proprio in ragione dell'interesse che il grande pubblico, o gruppi ristretti di persone, possono nutrire in relazione a determinate informazioni, il Libro Verde sull'informazione distingue in ultimo le informazioni in base al loro «(potenziale) valore economico», preoccupandosi di precisare che tanto le informazioni amministrative, quanto quelle non amministrative, «possono avere un valore di mercato considerevole». Anche questa distinzione è particolarmente importante in quanto mette in luce l'importanza che i dati delle pubbliche amministrazioni possono avere per gli operatori economici e, quindi, per lo sviluppo di nuovi servizi innovativi basati su di essi.

Oltre alle categorie di informazioni elencate dal Libro verde, nella legislazione europea e nazionale troviamo molte altre definizioni settoriali di dati. Tra queste meritano una menzione particolare quelle di dati personali e di *open data*.

2.3. I dati personali

La categoria dei dati personali è stata in ultimo individuata e definita dalla normativa europea al fine di delimitare l'ambito di applicazione oggettivo del Regolamento del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. Regolamento Generale sulla Protezione dei Dati, anche noto secondo l'acronimo inglese GDPR) (v. capitolo II, F. ROSSI DAL POZZO).

Ai sensi dell'art. 4, comma 1, n. 1, del GDPR, per dati personali si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")». Lo stesso comma aggiunge che «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

Anzitutto si deve rilevare che vengono contemplati solo i dati relativi alle persone fisiche. Se ne deve quindi dedurre che i dati delle persone giuridiche non sono tutelati dal GDPR. Quanto invece ai dati delle persone fisiche collegati a persone giuridiche, la Corte di giustizia ha più volte chiarito da ultimo nella sentenza del 9 marzo 2017 nella causa C-398/15 che per garantire la certezza del diritto nelle relazioni tra le società ed i terzi all'interno del mercato comune è indispensabile che chiunque intenda intrattenere rapporti d'affari con società aventi la propria sede in altri Stati membri possa conoscere agevolmente i dati costituitivi essenziali delle società commerciali e i dati essenziali relativi ai poteri dei loro rappresentanti. Il che dunque impone un bilanciamento tra il diritto alla protezione dei dati personali e la necessità che i nominativi di tali persone fisiche siano resi pubblici nei registri delle imprese degli Stati membri.

Quanto alle tipologie di dati che possono considerarsi idonei a rendere una persona fisica identificabile, si deve anzitutto prendere atto che l'elencazione fornita dal citato art. 4 non ha carattere tassativo. Il legislatore europeo ha infatti espressamente utilizzato la preposizione «come» nel fornire la citata elencazione, con ciò quindi indicando che anche ulteriori categorie di dati possono essere considerati personali. Deve perciò essere l'interprete a verificare, di volta in volta, rispetto a tutte le circostanze del caso concreto, se determinati dati siano o meno in grado di indentificare una persona fisica e, quindi, siano qualificabili come dati personali.

Tale operazione interpretativa volta a verificare se un dato debba essere considerato come personale ai sensi del GDPR deve peraltro tenere conto dal

fatto che la capacità di un dato di rendere identificabile una persona fisica va valutata in relazione a tutte le informazioni disponibili. Ciò significa che anche laddove un dato, in sé considerato, non sia idoneo a identificare una persona fisica, se questo, combinandolo con altri, può conseguire tale risultato, deve essere considerato, insieme a tutti gli altri, come un dato personale. In proposito, il considerando 30 del Regolamento afferma che gli «identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza […] possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

Alla luce di quanto precede, ci si potrebbe quindi chiedere se un indirizzo IP ossia una stringa numerica od alfanumerica che identifica i punti di origine e di destinazione delle informazioni su internet possa essere considerato come un'informazione atta ad identificare una persona fisica. La risposta ad un tale interrogativo dipenderà necessariamente dal contesto in cui viene generato e raccolto tale indirizzo IP, e dalla capacità di tale dato, eventualmente unitamente ad altri, di identificare una persona fisica. Laddove in ipotesi un utente navighi in Internet tramite una rete pubblica, quale il WI-FI dell'università, è ragionevole escludere che il solo indirizzo IP consenta di identificare in modo univoco la persona fisica, essendo tale dato riferibile ad ogni utente collegato da tale WI-FI. Viceversa, ove a tale indirizzo IP venga associato un codice identificativo unico, atto ad individuare il singolo utente, eventualmente collegando lo stesso ad account registrati su uno o più servizi, quali social network o motori di ricerca, allora si dovrà concludere che l'indirizzo IP sia un dato personale.

2.4. *Open data* (dati di tipo aperto), dati pubblici e *big data*

Tra le diverse categorie con cui vengono descritte le caratteristiche dei dati, quella di *open data* è particolarmente importante in quanto descrive un modo di essere dei dati che ne rende particolarmente agevole la fruizione (J. GURIN, 2014). Ai sensi dell'art. 1, comma 1, lett. l-*ter*), CAD, i «dati di tipo aperto» sono quelli resi fruibili di norma gratuitamente, a favore di chiunque, anche a fini commerciali, attraverso gli strumenti offerti dalle tecnologie dell'informazione e della comunicazione (Ict), in formati aperti e suscettibili di essere elaborati anche senza l'intervento umano.

Tra le varie declinazioni di tale nozione (B. PONTI, 2008), la definizione

accolta dal nostro legislatore mira a garantire la massima accessibilità dei dati qualificati come «aperti». Vengono rimosse sia le barriere legali, tramite l'adozione di licenze che ne permettono il riuso senza limiti di sorta, sia tecniche, con la distribuzione degli stessi tramite canali digitali (es. internet) e, soprattutto, in formati caratterizzati da una predeterminata e conoscibile struttura atta a garantire che gli stessi siano «leggibili meccanicamente».

Tale nozione è stata da ultimo disciplinata dall'art. 2, comma 1, lett. 13) della citata Direttiva 2019/1024/UE, che ha riproposto in modo invariato la definizione già dettata dalla previgente Direttiva 2003/98/CE, a sua volta recepita nel nostro ordinamento dall'art. 1, lett. c-*bis*), del D.Lgs. n. 36/2016. Ai sensi di tali norme, è un «formato leggibile meccanicamente» quello «strutturato in modo tale da consentire alle applicazioni software di individuare, riconoscere ed estrarre facilmente dati specifici, comprese dichiarazioni individuali di fatto e la loro struttura interna».

Questa caratteristica dei dati è di particolare importanza in quanto, in mancanza della stessa – laddove quindi i dati non siano distribuiti in formati leggibili meccanicamente – ne sarebbe assai meno agevole, se non impossibile, la fruizione.

In proposito è bene sgombrare il campo da un possibile equivoco circa la relazione tra la nozione di *open data* e quella di *big data*. Secondo quanto spiegato dall'AgID nel Piano triennale per l'informatica nella Pubblica Amministrazione 2017-2019, quest'ultima espressione identifica, riassuntivamente, «un insieme di dati da memorizzare e/o elaborare di dimensioni così grandi, e/o con una varietà di formati così elevata, e/o con una velocità di crescita così alta da richiedere l'uso di software non convenzionali […] per estrapolare, gestire e processare informazioni entro un tempo ragionevole».

I *big data* sono perciò masse enormi di dati che, di norma, sono fruibili attraverso tecniche e *software* specializzati, in grado di estrarre il valore conoscitivo che la massa di dati, nel suo complesso è in grado di esprimere. Si parla in proposito anche di *data lake* (lago di dati), proprio per rappresentare la vastità dei dati che caratterizza la nozione di *big data*, nonché la difficoltà di estrarre un qualche valore informativo da tale "lago" senza strumenti specifici. Si può raffigurare tale ultimo concetto con una metafora. Se si provasse a pescare in un lago a mani nude, semplicemente raccogliendo l'acqua e lasciandola fluire di nuovo nel lago, sarebbe praticamente impossibile pescare anche solo un pesce. Per poter ottenere un qualche risultato sarebbe necessario uno strumento apposito, come ad esempio una rete. Gettandola sapientemente nel lago, si potrebbe auspicabilmente pescare qualcosa. Lo stesso avviene in relazione ai *data lake*. Interrogando manualmente il database contenente la massa di dati, ed analizzando quindi i risultati uno ad uno, difficilmente si potrebbe estrapo-

lare una qualche informazione utile diversa da quella espressa dal singolo dato. Viceversa, con uno strumento specializzato, si potrebbe mettere in luce non solo il valore informativo del singolo dato, ma anche le relazioni di questo rispetto agli altri. Ad esempio, in un database universitario, si potrebbe analizzare la percentuale degli studenti fuori corso, ed in ipotesi studiare come tale dato si rapporti ad altri onde verificare quali correlazioni vi siano tra questo e determinate ulteriori variabili (v. capitolo IV, R. CAVALLO PERIN e I. ALBERTI).

Sulla base di tale ultima definizione, si può perciò rilevare che quello di *open data* e quello di *big data* sono concetti tra loro distinti ed autonomi. Ben si potrà avere un set di dati aperti che non sia qualificabile come *big data*, così come si potranno avere set di *big data* che non costituiscono dati aperti, e viceversa. D'altro canto, la quantità di dati processati nel settore pubblico è tale da qualificare buona parte dei set di dati in possesso delle amministrazioni quali *big data*. Il che permette di comprendere – e condividere – la scelta del legislatore di prevedere che i dati di tipo aperto siano resi disponibili in formati leggibili meccanicamente. I dati ottenuti dai database pubblici possono infatti in tal modo essere analizzati attraverso procedure automatizzabili, rendendone così più agevole la fruizione.

Venendo alla concreta individuazione di quali dati siano oggi qualificati come *open data*, l'art. 52, comma 2, CAD dispone che «i dati e i documenti che le amministrazioni titolari pubblicano […] si intendono rilasciati come dati di tipo aperto». Di norma, dunque, i dati delle pubbliche amministrazioni oggetto di pubblicazione sono qualificati come *open data*, salvo diversa ed espressa norma che disponga in senso contrario.

Si tratta di previsione dotata di una certa rilevanza in quanto l'ambito dei dati soggetti a pubblicazione è stato progressivamente esteso. Oltre alle specifiche norme di settore – che per ragioni di spazio non è possibile in questa sede analizzare (E. CARLONI, 2014) –, si può richiamare in via generale quanto prescritto dal D.Lgs. n. 33/2013 che, a seguito delle modifiche di cui al D.Lgs. 25 maggio 2016, n. 97, ha introdotto una nozione particolarmente ampia di trasparenza (D.-U. GALETTA, 2016).

Viene in proposito in rilievo l'art. 9-*bis* D.Lgs. n. 33/2013 che tratta precisamente della «pubblicazione delle banche dati» ai sensi del quale le pubbliche amministrazioni sono tenute alla pubblicazione dei dati contenuti nei database di cui siano titolari tra quelli elencati dall'Allegato B del decreto stesso. Tutti questi dati, dunque, sono certamente qualificabili come pubblici (A. SCOGNAMIGLIO, 2005).

Quanto ai restanti dati, viene invece in rilievo l'art. 5, comma 2, D.Lgs. n. 33/2013, nell'ampia portata risultante dalle ultime modifiche, che ha sancito il diritto di chiunque di «di accedere ai dati e ai documenti detenuti dalle pub-

bliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione». Quanto al regime applicabile ai suddetti dati, l'art. 7 del D.Lgs. n. 33/2013 conferma quanto previsto in via generale dal citato art. 52, comma 2, CAD, sancendo che «i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, resi disponibili anche a seguito dell'accesso civico di cui all'articolo 5 […] sono pubblicati in formato di tipo aperto ai sensi dell'articolo 68 [CAD, oggi art. 1, c. 1, lett. l-ter), CAD, n.d.a.]». Sul punto anche la giurisprudenza ha avuto modo di confermare che i documenti soggetti all'accesso civico sono «dati pubblici» (Cons. Stato, Sez. VI, 24 febbraio 2014, n. 865).

Ne consegue che – salvo non sia previsto diversamente – può ritenersi che, di regola, tutti i dati e i documenti detenuti dalle pubbliche amministrazioni possano essere considerati come dati «di tipo aperto».

3. Gli strumenti per la conservazione digitale dei dati

3.1. Nozioni essenziali sul concetto di banca dati

Come si è già accennato, con il passaggio dal cartaceo al digitale stiamo assistendo ad una profonda rimodulazione delle modalità di gestione dei dati in mano pubblica. Già da qualche tempo le informazioni vengono conservate in archivi digitali che permettono – a vario modo e secondo diverse logiche – la catalogazione, la strutturazione e l'indicizzazione dei dati ivi contenuti (F. CARDARELLI, 2002).

Come si è accennato, tale circostanza, tra i numerosi effetti che comporta, ha l'importante conseguenza di conferire una nuova dimensione ai dati, ove considerati nel loro complesso unitario. Da cataloghi mantenuti staticamente su supporti cartacei, le informazioni in mano pubblica, organizzate e strutturate con gli strumenti offerti dalle tecnologie dell'informazione e della comunicazione, hanno assunto nel loro complesso la rinnovata veste dinamica di banche dati digitali (o database).

Per comprendere il significato di tale termine, sotto un profilo giuridico una definizione di database la possiamo trovare nell'art. 1, comma 2, della Direttiva 96/9/CE sulla tutela giuridica delle banca dati, recepito dal nostro legislatore all'art. 1, comma 1, n. 9, della Legge 22 aprile 1941, n. 633 (c.d. legge sul diritto d'autore). Ai sensi di tale normativa per «banca di dati» «si intende una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo». Si noti che la norma citata prevede espressamente che le

raccolte in questione possono essere «accessibili grazie a mezzi elettronici o in altro modo», sicché si possono anche avere banche dati memorizzate su supporti analogici. In questa sede, in ogni caso, ci occupiamo esclusivamente dei profili relativi a quelle digitali.

Come già fatto in relazione alla nozione di dato, anche in questo caso possiamo altresì richiamare quanto previsto dal vocabolario ISO/IEC 2382:2015 dell'*International Organization for Standardization* (ISO), secondo cui una banca dati è una raccolta di dati organizzata secondo una struttura concettuale che ne descrive le caratteristiche e le relazioni tra loro, supportando una o più aree di applicazione.

Tali definizioni ci forniscono alcuni utili riferimenti in merito agli elementi che compongono le banche dati: non viene menzionato né il supporto sul quale le stesse sono conservate (*hardware*), né alcun programma informatico necessario al loro funzionamento (*software*). Gli unici elementi che vengono in rilievo sono i record di dati contenuti nella banca dati, la struttura secondo cui gli stessi sono memorizzati, le loro caratteristiche e le relazioni tra i vari record. Si tratta, quindi, di elementi aventi una propria dimensione (virtuale), del tutto autonoma rispetto all'infrastruttura fisica (*hardware*) ed informatica (*software*) necessaria al loro funzionamento.

Conferma tale circostanza anche il ventitreesimo considerando della citata Direttiva 96/9/CE, ai sensi del quale «il termine "banca di dati" non deve applicarsi ai programmi per elaboratore utilizzati per la costituzione o per il funzionamento di una banca di dati». Ciò in quanto la banca dati può esistere ed avere una propria consistenza (digitale) indipendentemente dai programmi informatici necessari per accedere ai contenuti della stessa. E ciò anche perché per una medesima banca dati vi possono essere molteplici programmi informatici atti a consentire la fruizione dei contenuti, sicché l'autonomia tra i due concetti comporta (anche) la possibilità di selezionare il software più appropriato in base alle esigenze del caso.

Altra importante caratteristica delle banche dati è che le stesse, in quanto risorse digitali, possono essere replicate un numero indeterminato di volte, su un qualsiasi sistema in grado di ospitarle, senza che ciò comprometta l'integrità della fonte da cui gli stessi vengono estratti. Il che è particolarmente rilevante in quanto comporta per l'amministrazione la possibilità di dare accesso ai propri dati consentendone l'estrazione dai propri database.

L'aspetto infrastrutturale, ossia l'*hardware* sul quale la banca dati viene ospitata rappresenta in ogni caso un aspetto fondamentale da considerare. Giova dunque analizzare due opposti modelli di conservazione dei dati, quelli centralizzati e quelli decentralizzati, per comprenderne caratteristiche e funzionalità essenziali.

3.2. I *data center* quali strumenti di conservazione centralizzata dei dati

I dati, per essere conservati in forma digitale, devono essere memorizzati su supporti materiali, quali ad esempio un computer. Tanto è maggiore il numero dei dati da memorizzare, tanto più aumenta la complessità dell'infrastruttura necessaria per la conservazione degli stessi. Per masse di dati quali quelle possedute dalle pubbliche amministrazioni è solitamente necessario predisporre strutture *ad hoc* deputate alla memorizzazione dei dati. Si tratta dei c.d. *data center*, anche comunemente noti come *cloud*, ossia strutture ove, anche in ambito privato, è oggi comune conservare i propri dati. L'uso del termine *cloud* (nuvola) non deve tuttavia trarre in inganno: queste strutture sono solitamente ben radicate nel territorio, all'interno di edifici realizzati o comunque attrezzati in vista dell'ottimizzazione dei sistemi e sono di norma ben protette, sia da minacce informatiche che da pericoli del mondo materiale, quali ad esempio calamità naturali. Nulla dunque di più lontano dall'idea che il termine nuvola trasmette: tant'è che queste strutture sono spesso addirittura sotterranee.

Tali *data center* hanno la funzione di accentrare in un unico luogo la conservazione dei dati. Tale accentramento non esclude tuttavia la possibilità di effettuare copie di sicurezza (c.d. *back-up*). Al contrario, è buona prassi prevedere la duplicazione dei dati in più *data center* per far fronte ad eventi disastrosi che possano rendere indisponibile il sito principale cui è affidata la gestione ordinaria del servizio.

Onde consentire la continuità del servizio e delle attività amministrative, è perciò di regola prevista l'implementazione di misure tecniche e organizzative atte a garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. Al centro di elaborazione dati primario sono a tal fine affiancati uno o più centri di elaborazione dati secondari in funzione di *disaster recovery*. Si deve tuttavia sottolineare che in questo modello di gestione dei dati di tipo centralizzato, pur anche ove esistano più centri secondari, la fonte dei dati deve essere identificata in un unico *data center*, mentre gli altri – in condizioni normali di servizio – hanno la sola funzione di replicarne passivamente le informazioni. In altri termini, anche ove esistano più copie della stessa banca dati, in vista del loro utilizzo il contenuto di tutte queste deve necessariamente essere riconducibile ad un'unica versione, sicché le diverse repliche devono essere considerate un *unicum* nell'ottica dell'amministrazione che se ne deve avvalere.

La conservazione in detti *data center* postula, rispetto agli archivi tradizionali, opportunità del tutto inedite, derivanti dalle diverse caratteristiche proprie dello strumento digitale. Tra queste va menzionata la possibilità di delocalizzare l'infrastruttura di memorizzazione dei dati. L'archivio cartaceo, per

ragioni di accessibilità e praticità, è per lo più opportuno che sia territorialmente prossimo al punto di utilizzo, ma ciò non vale per le banche dati digitali. La prossimità o la distanza del luogo di memorizzazione fisica di un dato digitale è generalmente indifferente, ove il sistema (informatico) di accesso allo stesso permetta la fruizione di contenuti remoti. Ne deriva che per le amministrazioni ciò comporta il notevole vantaggio di poter delocalizzare i propri archivi in aree relativamente remote del territorio, con i conseguenti risparmi che ciò può garantire, mantenendo al contempo gli uffici e le strutture nei centri più prossimi alla realtà amministrata.

3.3. La tecnologia *blockchain* quale strumento di decentralizzazione

Nel trattare delle modalità di gestione e conservazione dei dati merita una menzione la *blockchain*, una tecnologia a registro distribuito (o *Distributed Ledger Technologies*, DLT) che ha di recente acquistato una certa visibilità per le radicali innovazioni che questa introduce. In particolare, rispetto ai sistemi di tipo centralizzato descritti nel paragrafo precedente, la *blockchain* consente di implementare sistemi informatici decentralizzati che innovano profondamente le logiche di funzionamento dei sistemi di conservazione e gestione dei dati.

L'art. 8-*ter* del D.L. n. 135/2018 ha fornito una definizione delle «tecnologie basate su registri distribuiti», ai sensi della quale si considerano tali «le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».

Tra le caratteristiche di maggior rilievo nella nozione accolta dal nostro legislatore possiamo rilevare anzitutto la fondamentale componente del registro distribuito. Con il termine *registro* in questo caso intendiamo nella sostanza un database nel quale può essere registrata una qualsiasi informazione, al pari delle banche dati di cui si è detto *supra*. La sostanziale differenza con le suddette banche dati risiede nella totale sovversione del carattere centralizzato delle stesse.

La natura distribuita del database delle DLT comporta che lo stesso è condiviso su una rete informatica in modo che lo stesso sia replicato su tutti i dispositivi (c.d. nodi) di coloro che partecipino alla condivisione dei dati. La notevole differenza rispetto ai sistemi centralizzati è che in questo caso il sistema

è decentralizzato in quanto ogni nodo su cui è conservato il database è depositario, alla pari degli altri, del registro distribuito. Non esistono nodi passivi o secondari. Ciò ha il doppio vantaggio di consentire una perfetta trasparenza dei contenuti del registro, e di evitare che lo stesso possa essere compromesso da un singolo punto di errore.

La partecipazione alla rete può essere pubblica o privata. Nelle reti pubbliche chiunque può replicare sul proprio dispositivo il registro distribuito e può in tal modo divenire un nodo della rete. In quelle private hanno invece accesso solo i soggetti a ciò abilitati. Vi sono poi registri distribuiti c.d. *permissioned*, e registri c.d. *permissionless*. I primi sono basati su un sistema di autenticazione per cui non tutti gli utenti hanno i medesimi poteri sui dati conservati nel registro distribuito, i secondi sono invece privi di una qualsiasi misura di autenticazione, per cui chiunque può compiere operazioni sui dati conservati nel registro.

Il carattere distribuito del registro su cui si basano le tecnologie *blockchain* è alla base dell'esigenza di gestire «la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati» «su basi crittografiche», ossia sulla base di complessi algoritmi matematici volti a validare i contenuti e le operazioni effettuate sulle DLT.

Sul punto va anzitutto chiarito il concetto di catena di blocchi. A differenza dei database tradizionali, quelli in esame registrano i dati da memorizzare unitamente ad una serie di ulteriori metadati – che nel loro complesso costituiscono un c.d. blocco – grazie ai quali ogni nuova operazione è concatenata crittograficamente alle precedenti, così che sia possibile verificare ogni modifica registrata sul database. Attraverso complessi algoritmi matematici tale concatenazione permette di garantire nel tempo che le informazioni contenute in ciascun blocco non possano essere alterate. In tal modo, anche se il database è distribuito su un numero elevatissimo di nodi, si può sempre verificare che ciascuna copia del registro sia integra e che quindi tutte le informazioni distribuite su tutti i nodi siano univoche e concordanti tra loro. Meccanismi di consenso distribuito sono di norma del pari implementati anche per l'aggiunta di nuovi blocchi, attraverso modelli matematici particolarmente complessi in grado di convalidare le informazioni da inserire con gli altri partecipanti alla rete su cui è distribuita la *blockchain*.

Tale caratteristica delle DLT consente di garantire l'integrità ed il funzionamento del sistema senza un'autorità centrale. I modelli matematici che gestiscono la rete garantiscono essi stessi il corretto funzionamento del sistema. Tale capacità di autoregolazione ha consentito alla *blockchain* di assumere una certa diffusione nel settore delle monete virtuali, a partire dalla nascita del Bitcoin. Come ha rilevato la Corte di giustizia nella sentenza del 22 ottobre

2015 nella causa C-264/14, *Hedqvist*, tale moneta virtuale, essendo basata sulla *blockchain*, «non ha un unico emittente ma viene creata direttamente in una rete tramite uno speciale algoritmo» (par. 11).

Il citato art. 8-*ter* ha disciplinato anche un nuovo istituto denominato «smart contract», sul che si rinvia al relativo capitolo in questo manuale (v. capitolo X, B. CAPPIELLO e G. CARULLO).

Quanto agli effetti giuridici che le DLT possono produrre nel nostro ordinamento, l'art. 8-*ter* prevede che la registrazione di un dato su di una DLT conforme a determinati standard possa produrre gli effetti giuridici della validazione temporale elettronica. Si tratta dunque di effetti per il momento limitati rispetto alle potenzialità di tali tecnologie, che cionondimeno ci permettono di prospettare una certa utilità delle DLT anche nel settore pubblico.

In primo luogo, le DLT potrebbero avere una certa utilità nei procedimenti complessi, ossia ove più amministrazioni debbano interagire per l'esercizio di un determinato potere pubblico, specie nei casi in cui ciò avvenga a livello sovrastatale, ad esempio nelle fattispecie di coamministrazione europea. In questi casi lo scambio delle informazioni tra le amministrazioni potrebbe avvenire grazie a *blockchain* private sulle quali ciascun ente abbia facoltà di registrare i dati di propria competenza, nonché accedere a quelli registrati dagli altri che siano funzionali allo svolgimento dei propri compiti. Il vantaggio rispetto ad un sistema centralizzato sarebbe dato in questo caso dalla parificazione di tutti i nodi, ossia di tutte le amministrazioni coinvolte, rimuovendo quindi la necessità di prevedere un punto centrale di raccolta a livello sovranazionale.

Si può inoltre prospettare che le DLT possano consentire una maggiore trasparenza nella condivisione con i privati dei dati delle pubbliche amministrazioni. Ciò potrebbe avvenire grazie ad una distribuzione dei dati orizzontale attraverso *blockchain* – pubbliche o private a seconda della natura dei dati o documenti da condividere – *permissioned* nelle quali l'autorità pubblica mantenga il controllo sull'aggiornamento dei dati, consentendo al contempo ai privati di avere accesso agli stessi in modo immediato e diretto. In questo caso il vantaggio rispetto ai sistemi centralizzati potrebbe essere rappresentato dal fatto che un sistema basato su DLT permetterebbe ai cittadini di essere essi stessi co-depositari delle informazioni di loro interesse, potendovi così accedere direttamente senza l'intermediazione di servizi volti a consentire l'accesso ai dati. Un utilizzo di tal tipo è stato ad esempio prospettato nella relazione illustrativa del D.L. n. 76/2020, convertito con la Legge 11 settembre 2020, n. 120, ove, in relazione alla «Piattaforma per la notificazione digitale degli atti della pubblica amministrazione» di cui all'art. 26, si è ipotizzato che l'autenticità, l'integrità, l'immodificabilità e la leggibilità dei documenti informatici re-

si disponibili tramite la piattaforma sia garantita «eventualmente anche mediante l'utilizzo di tecnologie basate su registri distribuiti (blockchain)».

Infine, sul filo dell'ultimo caso, si può anche prospettare la possibilità che i privati partecipino alla co-creazione del database distribuito, immettendo loro stessi determinati dati. Ciò potrebbe essere di una qualche utilità ogniqualvolta l'amministrazione abbia necessità di acquisire dati dai privati. Il che potrebbe avvenire tramite *blockchain* pubbliche o private, garantendo adeguati livelli di autenticazione e validazione delle informazioni inserite rispetto alle diverse fattispecie considerate. Ciò, rispetto ai sistemi centralizzati, potrebbe consentire alle amministrazioni di acquisire le informazioni di cui necessitino con le garanzie di immodificabilità che il sistema di blocchi delle DLT garantisce, consentendo una perfetta e completa tracciabilità di tutte le operazioni svolte sul registro distribuito.

4. I dati nel procedimento amministrativo: verso un'istruttoria interconnessa e più informata

La capacità delle amministrazioni di gestire le informazioni con strumenti tecnologici può andare a vantaggio dell'azione amministrativa, dei cittadini e delle imprese. L'art. 12 CAD ha in proposito da tempo qualificato «le tecnologie dell'informazione e della comunicazione» quali strumenti «per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione». La norma promuove la condivisibile idea per cui attraverso l'aggiornamento in chiave digitale degli strumenti in possesso degli uffici pubblici sia possibile conseguire un più rapido ed efficiente trattamento delle informazioni necessarie nelle diverse fasi procedimentali.

Il progressivo ricorso agli strumenti offerti dalle tecnologie dell'informazione e della comunicazione per la raccolta, la conservazione e la fruizione delle informazioni di cui l'amministrazione necessiti per lo svolgimento dei propri compiti determina in tal senso un cambiamento radicale nelle modalità di svolgimento dell'istruttoria procedimentale. Grazie alla digitalizzazione del patrimonio informativo pubblico, le amministrazioni possono estrarre dai propri database le informazioni di cui abbiano bisogno per deliberare.

Prima dell'avvento delle tecnologie dell'informazione e della comunicazione, lo strumento di conservazione dei dati delle pubbliche amministrazioni era il supporto cartaceo o, comunque, analogico. Tra le molteplici differenze che caratterizzano il supporto cartaceo rispetto a quello digitale si può annoverare la staticità del primo. I limiti intrinseci ai metodi di archiviazione cartacea – quali la localizzazione dei supporti, i tempi di ricerca e di estrazione, nonché

le modalità di trasferimento dei dati da un luogo ad un altro – hanno fatto sì che, sino all'avvento delle più recenti tecnologie, non fosse possibile effettuare rapide operazioni su larga scala di ricerca, modifica, elaborazione, incrocio o scambio dei dati.

Da un contesto in cui le informazioni venivano conservate su supporti cartacei, a loro volta custoditi in archivi fisici, con il passaggio al digitale, e quindi la conservazione dei dati in database digitali, diventa possibile svolgere complesse attività di analisi prima materialmente impossibili. Il sesto considerando del GDPR conferma in proposito che «la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività». Oltre a consentire la rapida estrazione di un singolo dato, le nuove tecnologie consentono altresì di combinare, incrociare, comparare ed utilizzare i dati secondo modalità del tutto inedite rispetto a quanto consentiva il supporto cartaceo.

Da informazioni statiche in possesso degli uffici pubblici da valutare nell'ambito di un determinato procedimento, nel momento in cui i dati sono inseriti e strutturati all'interno di un database digitale questi divengono vere e proprie risorse funzionali allo svolgimento di molteplici attività. Si può perciò contrapporre alla precedente staticità dei documenti che caratterizzava, e caratterizza, la gestione cartacea, la natura dinamica delle operazioni da svolgere sui dati conservati digitalmente.

Tale dinamicità discende dalla possibilità di produrre un preciso *set* di dati in grado di esprimere un valore conoscitivo od informativo ulteriore rispetto a quello espresso dai singoli dati in sé considerati, variabile e adattabile in base alle esigenze istruttorie di volta in volta da assolvere. In proposito è eloquente quanto affermato dalla Cassazione in relazione alla disciplina sulla tutela dei dati personali. È stato più volte ribadito dalla Corte come «colui che compia operazioni di trattamento di tali informazioni, accostamento, comparazione, esame, analisi, congiunzione, rapporto, incrocio, ecc., possa ricavare ulteriori informazioni che si rivelino, perciò stesso, un "valore aggiunto informativo", un *quid pluris* non ricavabile dalle singole unità isolatamente considerate» (*ex multis* sez. I, 25 giugno 2004, n. 11864; sez. I, 17 luglio 2015, n. 15096).

Nel contesto del procedimento amministrativo ciò si traduce nella possibilità per il funzionario che conduce l'istruttoria di accedere ad uno o più database ed estrarre ogni volta una serie di dati diversa, secondo criteri da esso stesso definiti in rapporto alle esigenze del caso concreto, onde acquisire una o più informazioni risultanti dall'aggregazione di più dati. In concreto possiamo trovare un esempio di tale *modus agendi* nella circolare n. 16/E del 28 aprile 2016, nella quale l'Agenzia delle Entrate ha reso noto che, nell'ambito delle misure volte alla prevenzione ed al contrasto dell'evasione fiscale, avrebbe av-

viato procedimenti di verifica nei confronti dei «soggetti passivi IVA che presentano anomalie derivanti dall'incrocio dei dati dichiarati nel 2013 e quelli acquisiti dall'Agenzia delle entrate ai sensi dell'articolo 21 del decreto legge 31 maggio 2010, n. 78 e successive modificazioni (c.d. spesometro)» (v. capitolo IV, R. CAVALLO PERIN e I. ALBERTI).

Si realizza in tal modo il passaggio da un'istruttoria per fatti e documenti, ad una incentrata sui dati e sulle informazioni da questi ricavabili (G. CARULLO, 2017). Il *dato* diviene il mezzo attraverso il quale l'amministrazione acquisisce le *informazioni* necessarie per l'espletamento delle proprie funzioni, così che lo stesso assurge a componente fondamentale dell'azione amministrativa, quale strumento di conoscenza e interpretazione della realtà. Il che significa che il patrimonio di dati delle pubbliche amministrazioni può essere considerato come un'immensa miniera informativa dalla quale i soggetti pubblici possono attingere quanto necessitano per avere una corretta rappresentazione della realtà amministrata.

4.1. Lo scambio di informazioni tra amministrazioni

Affinché la suesposta interconnessione del patrimonio di dati pubblico possa realizzarsi, e quindi sia effettivamente possibile fruire appieno del potenziale informativo da questo ricavabile, è essenziale che i sistemi informatici delle pubbliche amministrazioni siano tra loro interoperabili. Sul punto si può richiamare quanto sottolineato dalla Commissione europea nella Comunicazione del 26 settembre 2003, (COM(2003) 567), secondo cui l'interoperabilità dei sistemi informatici è il «mezzo grazie al quale ottenere un intercollegamento tra sistemi, informazioni e metodi di lavoro: all'interno di una stessa amministrazione o tra amministrazioni diverse; a livello nazionale o in tutta Europa, oppure con le imprese» (p. 21). In altri termini, grazie all'interoperabilità è possibile scambiare dati in modo automatizzato tra un sistema informatico ed un altro.

Per le amministrazioni ciò significa che l'interoperabilità è funzionale alla realizzazione di sistemi in grado di consentire un agevole e rapido scambio di informazioni sia nell'ambito dei rapporti interni ad una medesima organizzazione (rapporti interorganici), sia in relazione a quelli tra più enti (rapporti intersoggettivi), nonché nelle comunicazioni con i privati (A. MASUCCI, 2003). È infatti opportuno che i sistemi di cui si dotino le amministrazioni siano realizzati in modo tale da consentire sia che diversi uffici possano scambiarsi dati, sia che ciò sia possibile in rapporto a tutte le altre amministrazioni e soggetti privati che siano coinvolti in un dato procedimento.

L'interoperabilità assume dunque rilevanza sia nei rapporti interorganici, sia in quelli intersoggettivi. Un ufficio, ovvero un ente, grazie a sistemi informatici interoperabili può avere accesso alle informazioni detenute da un altro ufficio, ovvero da un'altra amministrazione, senza la necessità – quantomeno tecnica – di alcuna interazione tra i funzionari. Al richiedente può bastare accedere, attraverso il proprio sistema informatico, ai dati di cui necessiti, e così automaticamente recuperare le informazioni richieste dal sistema messo a disposizione dall'altro ufficio.

Sotto altro profilo, la capacità di interconnessione dei database informatici permette anche di realizzare nuove forme di accesso dei singoli (privati e imprese) ai dati detenuti dalle pubbliche amministrazioni. L'alta probabilità che tale informatizzazione porti ad una sempre più penetrante ed estesa interconnessione dei sistemi in dotazione alle amministrazioni pubbliche è del resto ben rappresentata dalle parole della Commissione europea. Con la recente Comunicazione in materia di mercato interno digitale, si è auspicato che si possa presto realizzare una «società elettronica inclusiva», nella quale «i cittadini e le imprese abbiano le competenze necessarie e possano usufruire di servizi elettronici interconnessi e plurilingue che spazino dalla pubblica amministrazione alla giustizia, dalla sanità all'energia e ai trasporti» (p. 4.3).

Sempre in ambito europeo, anche il legislatore sembrerebbe aver recepito con favore i suggerimenti di quella dottrina che ha auspicato, tra gli altri, l'introduzione nel procedimento amministrativo europeo di sistemi di automazione e digitalizzazione delle interazioni tra pubbliche amministrazioni. Si è infatti evidenziato in dottrina che «le informazioni che raccolgono, aggregano e distribuiscono a vari attori a livello UE e a livello degli Stati membri spesso costituiscono un fattore centrale nell'attività decisionale» e che, per tale ragione, «sono necessari approcci creativi per l'uso dei sistemi informatici nelle attività provvedimentali, in quelle di regolamentazione e nei contratti» (P. CRAIG *et al.*, 2016, p. 20).

A livello nazionale la rilevanza dell'interoperabilità è ben testimoniata dall'attenzione che il legislatore da tempo vi presta. Già l'art. 1, comma 3, lett. a), del D.Lgs. n. 39/1993 prevedeva che «lo sviluppo dei sistemi informativi automatizzati […] risponde ai […] criteri [di] integrazione ed interconnessione dei sistemi medesimi». I successivi interventi legislativi hanno progressivamente intensificato gli sforzi verso l'interoperabilità dei sistemi.

Più di recente il legislatore italiano ha definito le modalità di interconnessione tra i sistemi informatici delle pubbliche amministrazioni all'art. 73, comma 1, del CAD, attraverso il c.d. «sistema pubblico di connettività e cooperazione (SPC)», ossia un «insieme di infrastrutture tecnologiche e di regole tecniche che assicura l'interoperabilità tra i sistemi informativi delle pubbliche

amministrazioni, permette il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e tra queste e i sistemi dell'Unione europea ed è aperto all'adesione da parte dei gestori di servizi pubblici e dei soggetti privati». Quella della interconnessione e dello scambio dei dati non è, peraltro, una logica nuova nell'ambito del Codice, basti pensare che, prima della citata ultima novella, l'art. 58, comma 2, già prevedeva che «le pubbliche amministrazioni comunicano tra loro attraverso la messa a disposizione a titolo gratuito degli accessi alle proprie basi di dati alle altre amministrazioni mediante la cooperazione applicativa di cui all'articolo 72, comma 1, lettera e)».

Ancor più recentemente, l'art. 50-*ter*, introdotto dall'art. 34 del D.L. n. 76/2020 (D.L. 16 luglio 2020, n. 76, Misure urgenti per la semplificazione e l'innovazione digitale, convertito con la Legge 11 settembre 2020, n. 120), è intervenuto in relazione alla c.d. Piattaforma Digitale Nazionale Dati (PDND). Questa «è costituita da un'infrastruttura tecnologica che rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici» ed è «finalizzata a favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto, per finalità istituzionali, [da detti soggetti], nonché la condivisione dei dati tra i soggetti che hanno diritto ad accedervi ai fini della semplificazione degli adempimenti amministrativi dei cittadini e delle imprese».

Dunque, la prospettata evoluzione in senso tecnologico ed interconnesso degli strumenti in dotazione alle amministrazioni non è meramente teorica, ma trova già riscontro pratico in molteplici fattispecie. Tale circostanza può così determinare una ridefinizione delle modalità di interazione dei procedimenti. Da una prospettiva atomistica in cui ogni amministrazione è detentrice delle informazioni funzionali all'esercizio delle proprie competenze, si può passare ad una dimensione fortemente collaborativa in cui i dati complessivamente acquisiti nella sfera pubblica sono posti al servizio delle amministrazioni nel loro complesso – nei limiti necessari allo svolgimento della funzione –, grazie all'interconnessione delle banche dati.

Perché ciò possa efficacemente avvenire, tuttavia, è necessario che i sistemi delle varie amministrazioni siano interoperabili. Per il che occorre passare a parlare più nello specifico di tale concetto.

4.2. La nozione di interoperabilità dei sistemi informatici

Come si è evidenziato, il concetto di interoperabilità è molto importante affinché le pubbliche amministrazioni possano interagire tra loro in un contesto

digitalizzato. Questa nozione, di natura tecnica e che descrive un modo di essere dei sistemi informatici, è in particolare essenziale al fine di garantire che i vari sistemi si possano interfacciare tra loro, nell'ambito di reti interconnesse. Laddove si parla di reti interconnesse, si indica un sistema (informatico) nell'ambito del quale due o più unità funzionali (ad esempio, due *personal computer*) sono in grado di comunicare e quindi scambiare tra loro informazioni in modo automatizzato, consentendo così l'accesso a dati conservati su un sistema diverso da quello richiedente le informazioni stesse.

Quanto alla nozione di interoperabilità, si può richiamare la Comunicazione sulla strategia per il mercato unico digitale in Europa (COM(2015) 192) della Commissione europea ove viene chiarito che «nell'economia digitale l'"interoperabilità" significa garanzia di comunicazione effettiva tra componenti digitali quali dispositivi, reti o archivi di dati» (p. 4.2).

Partendo da tale assunto, in dottrina si è sottolineata la distinzione, introdotta dalla stessa Commissione, tra le varie prospettive sotto le quali si può parlare di interoperabilità: tecnica, semantica ed organizzativa. Secondo tale tripartizione, l'interoperabilità tecnica si occupa delle modalità di interconnessione dei sistemi informatici, e quindi della definizione delle interfacce, dei formati dei dati e dei protocolli; l'interoperabilità semantica si occupa di garantire che il significato delle informazioni scambiate sia comprensibile da qualsiasi applicazione interconnessa; infine, quella organizzativa ha per oggetto l'attività di modellazione dei processi, allineando le architetture di informazione con gli obiettivi organizzativi ed aiutando l'integrazione dei processi produttivi (H. KUBICEK, R. CIMANDER e H.J. SCHOLL, 2011).

In termini tecnici, queste interconnessioni tra i sistemi informatici sono anche state descritte come *network* virtuali, vale a dire come reti che non si basano su connessioni fisiche, ma su legami invisibili tra i loro nodi. Tali collegamenti, costituenti siffatta rete virtuale, sono poi talvolta raffigurati anche quali lingue in quanto rappresentano i modi in cui i diversi sistemi "si parlano" – ossia, comunicano tra loro – e, quindi, i mezzi attraverso i quali le informazioni vengono scambiate.

Volendo ulteriormente specificare tale preliminare definizione, ci si scontra tuttavia con la molteplicità di situazioni in cui tale concetto può venire in gioco. Si è infatti detto che il significato da attribuire al termine interoperabilità può variare sensibilmente in base al contesto nel quale lo stesso viene utilizzato. Tra le accezioni del termine suscettibili di avere una più ampia portata possiamo ricordare quella secondo la quale l'interoperabilità è la capacità di due sistemi di interagire utilizzando il medesimo protocollo di comunicazione, ovvero quella per cui l'interoperabilità è la capacità di apparecchi di diversi produttori (o diversi sistemi) di comunicare tra loro su di un'infrastruttura

comune (lo stesso sistema), o su di un diverso sistema, in *roaming*, ovvero ancora può essere intesa quale capacità di due o più sistemi o componenti di scambiare dati e utilizzare informazioni.

Possiamo dunque affermare che, per ritenere due sistemi tra loro interoperabili, deve essere possibile uno scambio effettivo ed automatizzato di dati o di informazioni. Tale è, del resto, la prospettiva che risulta aver da ultimo adottato anche il nostro legislatore il quale, nel riformare il CAD, è intervenuto nel 2016 proprio sulla nozione di interoperabilità, definendola all'art. 1, comma 1, lett. dd) quale «caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi». La novella ha così superato le definizioni di «interoperabilità di base» e di «interoperabilità evoluta», precedentemente contenute nell'oggi abrogato art. 72. Tali nozioni facevano riferimento, anziché ad un modo di essere dei sistemi informatici, ai servizi realizzati sulla base di tale «caratteristica» per realizzare in concreto l'interoperabilità, presupponendo perciò implicitamente la definizione oggi esplicitata dalla citata norma.

L'attuale nozione fornita dal CAD pone invece l'accento sull'abilità di due sistemi informatici di scambiarsi dati in modo automatizzato, ossia senza il necessario intervento umano. A tal fine, viene sottolineato che le interfacce di un sistema interoperabile devono essere «pubbliche e aperte».

Non viene tuttavia chiarito dalla norma cosa si intenda con tali due aggettivi in tale contesto. In mancanza di una definizione specifica, possiamo evincerne il significato ricavandolo per analogia da altre disposizioni relative a sistemi informatici che presuppongono tali caratteristiche, fornendone al contempo una definizione. Quanto al carattere pubblico delle interfacce, si può fare riferimento alla definizione di «dato pubblico» fornita dall'art. 2, comma 1, D.Lgs. n. 36/2006 ai sensi del quale è tale «il dato conoscibile da chiunque». In base a tale disposizione si può perciò ritenere che le interfacce siano qualificabili come «pubbliche» laddove siano «conoscibili da chiunque». Il che appare coerente con quanto si è esposto poc'anzi in merito alla necessità di conoscere le interfacce per poter realizzare sistemi tra loro interoperabili. Quanto al carattere «aperto», può essere utile la definizione di cui si è già detto nel capitolo precedente di «dati di tipo aperto» di cui all'art. 1, comma 1, lett. l-*bis*), CAD. Applicando per analogia i tre requisiti che connotano tale figura, in questo caso, le interfacce, per essere aperte, devono rispondere a tre requisiti: essere sottoposti a licenze senza restrizioni di utilizzo, essere facilmente accessibili online ed essere tendenzialmente gratuite, salvo circoscritte eccezioni.

Così intese, tali qualità delle interfacce sono particolarmente importanti in quanto lo sviluppo di un sistema informatico che si vuole rendere interopera-

bile con altri deve essere conforme ad un preciso schema di funzionamento, ossia a predeterminate interfacce. Solo in tal modo detto sistema informatico, una volta ultimato, può essere effettivamente in grado di comunicare automaticamente con altri dispositivi conformi alle medesime interfacce. Ne discende quindi che, ove le specifiche tecniche delle interfacce non siano conosciute, diventa estremamente difficile – se non impossibile – poter realizzare sistemi tra loro interoperabili. Sicché si può certamente condividere la scelta del legislatore di aver previsto che, per poter parlare di interoperabilità, siano necessarie interfacce «pubbliche e aperte».

4.3. Il problema dei costi di uscita (c.d. *lock-in*) nella selezione dei mezzi digitali

L'adozione di strumenti interoperabili è particolarmente importante anche in vista della riduzione dei possibili costi di uscita che determinate tecnologie impongono laddove si voglia passare ad altra soluzione.

Anzitutto va considerato che l'adozione di una determinata tecnologia esclude talvolta il ricorso ad altre, pur ove tecnicamente equipollenti, e può perciò vincolare in modo sostanziale le opzioni da adottare a valle. Ciò, ad esempio, può avvenire in quanto determinati applicativi possono essere eseguiti solo su determinati dispositivi *hardware*, ovvero solo a condizione che su un dato dispositivo siano preinstallati altri *software*.

Tale circostanza può avere ricadute particolarmente significative in quanto, una volta che sia stata selezionata ed implementata una data soluzione, ne possono derivare molteplici vincoli. Tra questi va in particolare ricordato il fenomeno di c.d. *lock-in*, anche definito quale «costo di uscita». Ai sensi dell'art. 1, comma 1, lett. l), della *Direttiva ministeriale del 19 dicembre 2003 in materia di sviluppo e utilizzazione dei programmi informatici da parte delle pubbliche amministrazioni* (nel proseguo, Direttiva), questo consiste nell'«insieme dei costi da sostenere per abbandonare una tecnologia o migrare verso una tecnologia o soluzione informatica differente», ivi inclusi «i costi di conversione dati, di aggiornamento dell'hardware, di realizzazione interfaccia e di formazione».

Nell'ambito del settore delle ICT, il *lock-in* dipende generalmente dall'uso di una «tecnologia proprietaria», ossia, ai sensi dell'art. 1, comma 1, lett. c) della Direttiva, di una «una tecnologia posseduta in esclusiva da un soggetto che in genere ne mantiene segreto il funzionamento» e che, pertanto, impedisce o comunque riduce la fungibilità dei sistemi basati su di essa. In particolare il fenomeno si può avere quando una determinata soluzione si basa su di un «formato proprietario» – ossia su di «un formato di dati utilizzato in esclusiva

da un soggetto che potrebbe modificarlo a proprio piacimento» (art. 1, comma 1, lett. d), Direttiva) – ovvero quando i processi produttivi impiegano «programmi di tipo proprietario» – ossia «applicazioni informatiche basate su tecnologia di tipo proprietario, cedute in uso dietro pagamento di una licenza, che garantisce solo la fornitura del codice eseguibile e non del codice sorgente» (art. 1, comma 1, lett. i), Direttiva) –.

In tutti questi casi, ossia ogniqualvolta le soluzioni ICT siano sotto il controllo esclusivo di un soggetto diverso dall'utilizzatore delle stesse, il fenomeno di *lock-in* vincola l'amministrazione all'uso di una determinata soluzione, pena la necessità di far fronte ad elevati costi di uscita per svincolarsi dalle tecnologie proprietarie adottate. Ciò si verifica in quanto può accadere che la commercializzazione di tali sistemi sia volta a rendere gli stessi infungibili, ossia non (facilmente) sostituibili con prodotti concorrenti.

Tra le varie tecniche che possono essere utilizzate per realizzare tale risultato, può essere utile menzionare il caso in cui i dati processati da un'applicazione siano memorizzati in formati proprietari che ne rendono il contenuto fruibile solo tramite uno specifico *software*. In tal caso, l'impiego di tale applicazione, e quindi del relativo formato di file, impone all'utente, alternativamente, di mantenere invariata la configurazione del sistema, ovvero se tecnicamente possibile di convertire tutti i file in altro formato, con i relativi costi.

Si consideri peraltro che tale valutazione è particolarmente delicata sia per le ricadute che può avere sull'amministrazione e sulla capacità di questa di agire efficacemente e nel rispetto dei princìpi di economicità ed efficienza, sia perché la stessa può avere ricadute anche sui privati. Ogniqualvolta le dotazioni informatiche dell'amministrazione abbiano rilevanza non solo interna, ma anche esterna, la selezione di un determinato strumento piuttosto che un altro può influire sulle modalità di interazione tra soggetti pubblici e tra questi ed i privati, e quindi – direttamente od indirettamente – anche sulle modalità di organizzazione ed azione di questi ultimi.

Anche per tale motivo si può perciò condividere la previsione di cui all'art. 68, comma 1, del CAD secondo cui la scelta dell'amministrazione deve essere effettuata nel rispetto, tra gli altri, del principio di «neutralità tecnologica», di modo da evitare soluzioni che possano obbligare i privati all'utilizzo di tecnologie potenzialmente comportanti, ad esempio, elevati costi di uscita. Anche in giurisprudenza si è del resto argomentato che il problema del *lock-in* impone alle amministrazioni una «valutazione comparativa tra le diverse soluzioni tecnologiche» che si basi «da un lato sulla rispondenza della soluzione scelta alle esigenze concrete dell'amministrazione e, dall'altro, sulla attenta valutazione dei costi di uscita dal sistema in uso» (T.A.R. Trentino Alto-Adige, Bolzano, sez. I, 25 maggio 2012, n.188).

4.4. II ruolo delle autorità pubbliche nella definizione degli standard tecnici

Ove più enti siano dotati di autonomia organizzativa in relazione ai sistemi informatici da adottare, l'eventuale mancanza di un coordinamento tra i diversi centri decisionali può determinare il rischio che vengano implementati molteplici sistemi informatici tra loro non interoperabili. Ciò può avvenire per varie ragioni, ad esempio in quanto, nonostante le interfacce dei programmi siano «pubbliche e aperte», gli stessi siano stati realizzati senza tener conto delle interfacce adottate dagli altri sistemi, così rendendo gli stessi non interoperabili.

In un ordinamento multilivello quale il nostro, caratterizzato da un marcato pluralismo istituzionale, e improntato alla tutela delle autonomie locali e regionali, e dove si inseriscono, anche a livello statale, molteplici soggetti dotati di forte autonomia ed indipendenza, la mancanza di azioni di armonizzazione nel processo di digitalizzazione delle amministrazioni può portare ad un contesto nel quale i sistemi adottati dai diversi enti non sono tra loro interoperabili.

Per ovviare a tale problema il legislatore ha adottato diverse strategie. In proposito viene anzitutto in rilievo l'art. 69 CAD ai sensi del quale le amministrazioni, ove possibile, dovrebbero rendere riutilizzabili, e quindi riutilizzare, i sistemi informatici, così che più enti, anche se tra loro autonomi, siano incentivati a dotarsi dei medesimi mezzi digitali. Il che, oltre a poter ridurre i costi facilitando economie di scala, può anche ridurre la frammentazione dei sistemi informatici.

Un altro strumento attraverso cui il legislatore ha inteso garantire l'interoperabilità dei sistemi delle pubbliche amministrazioni è stato attraverso il conferimento all'AgID, quale soggetto dotato di elevata competenza tecnica, del compito di individuare standard tecnici a cui i sistemi adottati dalle amministrazioni devono uniformarsi.

In ultimo è anche stato introdotto il c.d. Codice di condotta tecnologica di cui all'art. 13-*bis*, comma 2, CAD, inserito dall'art. 32 del D.L. n. 76/2020, convertito con la Legge 11 settembre 2020, n. 120. Detto «codice di condotta tecnologica disciplina le modalità di progettazione, sviluppo e implementazione dei progetti, sistemi e servizi digitali delle amministrazioni pubbliche, nel rispetto del principio di non discriminazione, dei diritti e delle libertà fondamentali delle persone e della disciplina in materia di perimetro nazionale di sicurezza cibernetica». Con l'introduzione del Codice, il legislatore ha dunque intesto fornire un documento in grado di guidare le amministrazioni nelle scelte tecnologiche, onde garantire una certa omogeneità delle soluzioni adottate nel settore pubblico.

Tra le diverse modalità attraverso cui è possibile garantire un certo livello

di interoperabilità, lo strumento più comune per la realizzazione di sistemi interoperabili è infatti stato, anche a livello europeo, la standardizzazione, ossia la definizione di specifiche tecniche aventi lo scopo di stabilire un design comune per un prodotto o un processo. Del resto, si è notato che le reti di computer tendono di norma verso standard *de facto*, e di solito si basano su pochi standard di comunicazione, sicché non stupisce che, per i sistemi informatici, l'interoperabilità sia solitamente conseguita attraverso tale metodo.

La conformazione allo standard comporta la necessità di adeguare il funzionamento di una o più parti di un sistema ad un dato modello – ad esempio un formato di file – di modo che qualsiasi altro software realizzato conformemente a tale standard sia parimenti in grado di interfacciarsi con tale modello. Senonché la definizione di standard non è priva di controindicazioni. Oltre alle ovvie difficoltà tecniche che possono venire in gioco, possono sorgere problemi anche a causa di una sovra-regolamentazione.

Per comprendere in cosa consista l'attività di regolazione volta alla definizione di standard informatici si può richiamare il parallelismo tra le reti informatiche ed i linguaggi umani. È pacifico che, nelle interazioni umane, una differenza linguistica può costituire un ostacolo allo scambio di informazioni. Di conseguenza, per stabilire una comunicazione tra due soggetti, è necessario definire un linguaggio comune che entrambe le parti possano comprendere.

Lo stesso vale per i sistemi informatici. Anche in relazione a questi, come si è detto, si parla espressamente di interoperabilità semantica quale elemento essenziale di qualsiasi ecosistema interoperabile. Affinché due sistemi possano interfacciarsi, occorre dunque individuare gli standard ed i protocolli da applicare alle comunicazioni tra loro, attraverso la definizione delle c.d. Specifiche Tecniche di Interoperabilità (STI). Tali regole hanno il compito di stabilire dei modelli di comunicazione da applicare ai sistemi da interconnettere. Le STI comprendono, ad esempio, la definizione del formato che devono assumere i dati da scambiare e, quindi, le modalità stesse con cui il trasferimento deve avvenire.

Il ricorso alla standardizzazione comporta naturalmente molteplici vantaggi, tra cui, oltre l'interoperabilità tra sistemi, anche la creazione di economie di scala, di effetti di rete necessari per lo sviluppo di nuove tecnologie e di piattaforme per la realizzazione di nuovi prodotti. Attraverso la definizione di standard, tuttavia, si determina anche un effetto normalizzante, in quanto tutti i sistemi coinvolti devono necessariamente uniformarsi agli standard stabiliti dalle suddette regole per poter interfacciarsi con gli altri sistemi.

È proprio tale necessità di cristallizzare in regole predefinite i modelli di funzionamento dei sistemi interconnessi che, tuttavia, può porre i più delicati problemi. Tra questi, *in primis*, vengono in rilievo quelli di obsolescenza ed

inefficienza del sistema stesso, considerato che l'innovazione tecnologica può procedere – e di fatto di sovente procede – a un ritmo più veloce di quello con il quale vengono adottate revisioni della relativa regolamentazione.

Non solo. Gli standard, una volta definiti, tendono a diffondersi indipendentemente dalla loro effettiva efficienza, in quanto la necessità di adeguarvisi per instaurare un regime di interoperabilità spinge gli operatori ad adottarli nonostante vi possano essere soluzioni migliori sul mercato. Il che, di conseguenza, può portare ad una indesiderata riduzione di efficienza dei sistemi interconnessi.

Strettamente connesso con tale problema è poi quello per cui un'eccessiva standardizzazione può anche portare ad un'indesiderata riduzione degli investimenti in ricerca ed innovazione. Si è infatti sostenuto che ove vi siano standard che tutti gli operatori del mercato sono tenuti a rispettare, si riduce, od elimina, l'utilità di ricercare nuove e più efficienti soluzioni considerato che queste, anche qualora fossero portate sul mercato, dovrebbero comunque cedere il passo alle STI, anche laddove queste ultime fossero, in ipotesi, meno efficienti.

Come conferma la previsione del CAD ai sensi della quale le interfacce dei sistemi interoperabili devono essere «pubbliche e aperte», un fattore particolarmente critico nella regolamentazione è la presenza di standard proprietari. L'eventuale difficoltà ad accedere alle specifiche tecniche può infatti limitare le opportunità di sviluppo di nuove soluzioni, riducendo quindi le opzioni a disposizione degli utenti, ed aumentando il rischio di *lock-in*. Il risultato, in altre parole, è che laddove le interfacce adottate da un'amministrazione non siano aperte e pubbliche, l'adozione a livello normativo di un dato standard può causare una indebita restrizione della concorrenza.

Non solo. Nella prospettiva di garantire la maggior circolazione possibile delle tecnologie, e favorire quindi una più ampia scelta ad amministrazioni e privati nella selezione delle soluzioni conformi ad un determinato standard, occorre anche tenere in debita considerazione l'effettiva diffusione e rilevanza di un dato standard, specie ove ne esitano molteplici tra loro fungibili. In tal caso appare preferibile ricorrere a quelli aventi maggiore diffusione e, possibilmente, rilievo internazionale. In tal modo le soluzioni indicate a livello regolatorio possono avere maggiori chance di attrarre fornitori stranieri, a tutto beneficio dell'offerta ai clienti finali, aumentando al contempo la visibilità delle iniziative adottate nel nostro ordinamento e, quindi, le possibilità che queste siano esportate altrove.

V'è poi da considerare che la creazione di nuovi livelli di interoperabilità rimane uno sforzo complesso e costoso; ciò in quanto, per definire delle STI è necessario predefinire esattamente tutte le interazioni che si vorranno permet-

tere tra due o più sistemi, identificando e strutturando di conseguenza i relativi dati che dovranno essere scambiati. La realizzazione di un sistema interoperabile comporta perciò, di norma, un grado di complessità assai maggiore rispetto alla creazione di un sistema isolato, che va naturalmente ad aumentare tanti più siano i sistemi che tra loro devono interagire e la quantità e la varietà delle informazioni da scambiare.

Proprio in ragione di tali criticità, si può condividere l'idea secondo cui l'interoperabilità dovrebbe essere vista non come fine a sé stessa, ma piuttosto quale mezzo strumentale al raggiungimento di un altro, e ben preciso, fine. Secondo tale prospettiva si dovrebbe dunque procedere alla definizione di STI solo qualora sia effettivamente necessario permettere a due sistemi di interfacciarsi, evitando viceversa di aggiungere complessità al sistema qualora ciò non sia richiesto dalle concrete esigenze cui dare risposta.

Non solo. A causa delle preoccupazioni che la standardizzazione e la creazione di sistemi interoperabili possono determinare, si può accogliere l'idea secondo cui sia preferibile tentare di conseguirne i relativi benefici avendo cura di ridurre al minimo le conseguenze negative che dalla stessa possano derivare. Senza comunque dimenticare che, come ha dimostrato l'esperienza relativa alle liberalizzazioni avvenute a partire dagli anni '90 in attuazione del diritto europeo, l'interoperabilità può portare numerosi vantaggi, sia in termini di prevenzione del *lock-in* dei consumatori, sia quale motore dell'innovazione. Si tratta, in altri termini, di trovare il giusto bilanciamento tra un sistema del tutto isolato, ed uno eccessivamente standardizzato.

4.5. I criteri per la valutazione comparativa delle soluzioni tecnologiche e relativi oneri per l'amministrazione

Considerati i numerosi profili critici che connotano la selezione degli strumenti informatici da parte delle pubbliche amministrazioni, il legislatore ha disciplinato questa delicata fase al fine di indirizzare le pubbliche amministrazioni verso soluzioni dotate di determinate caratteristiche tecniche ritenute maggiormente satisfattive delle esigenze del settore pubblico

L'attuale formulazione degli artt. 68 e seguenti del CAD indicano una serie di criteri e princìpi per lo sviluppo, l'acquisizione ed il riuso di sistemi informatici nelle pubbliche amministrazioni (V. FINOTTO e A. FORTE, 2004), come meglio specificati anche dalle «Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni» dell'AgID (Linee Guida).

In particolare, l'art. 68, comma 1, CAD prevede che «le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei

princìpi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico». La norma prosegue elencando tra quali «soluzioni disponibili sul mercato» le amministrazioni debbano condurre tale valutazione comparativa, secondo un ordine preferenziale decrescente: «software sviluppato per conto della pubblica amministrazione»; «riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione»; «software libero o a codice sorgente aperto»; «software fruibile in modalità cloud computing»; «software di tipo proprietario mediante ricorso a licenza d'uso»; «software combinazione delle precedenti soluzioni».

I criteri per la valutazione comparativa tra tali diverse opzioni sono dettati dal successivo comma 1-*bis*, in base al quale le pubbliche amministrazioni devono tenere in considerazione tre elementi chiave: il «costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto»; il «livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione»; nonché le «garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito».

A norma del comma 1-*ter*, detta valutazione comparativa tecnico-economica deve essere effettuata secondo le modalità ed i criteri definiti dall'AgID con le citate Linee Guida. Queste ultime indicano quale primo passaggio l'«individuazione delle esigenze», nel quale «la pubblica amministrazione definisce le esigenze (bisogni e vincoli) che condizionano le scelte per l'individuazione di una soluzione» (p. 2.4). La prima fase individuata all'uopo dall'AgID consiste nella «analisi del fabbisogno», nel quale devono essere svolte diverse attività, tra cui, in primis, lo «studio del contesto attraverso la descrizione delle caratteristiche dell'amministrazione: finalità, struttura ed organizzazione» e la «descrizione dei flussi operativi interessati dal software da acquisire, che la pubblica amministrazione mette in atto per dare seguito alle procedure amministrative» e quindi l'«identificazione degli "strumenti" (definizione degli obiettivi) necessari alla realizzazione dei processi operativi individuati».

Le Linee Guida mettono dunque in luce che sotto un profilo tecnico la selezione di una tecnologia informatica comporta una duplice valutazione vertente sia sulla soluzione in sé considerata, sia sul contesto dei processi produttivi nel quale la stessa dovrà essere implementata. Le competenze necessarie per l'esatta individuazione e risoluzione delle problematiche che vengono a tal fine in rilievo appaiono perciò caratterizzate da marcati tratti di interdisciplinarietà, tra cui si possono agevolmente ricomprendere le competenze elencate

dall'art. 13, comma 1-*bis*, del CAD in relazione alle politiche di «formazione informatica dei dipendenti pubblici», ossia «competenze tecnologiche, di informatica giuridica e manageriali».

Per quanto le Linee guida possono costituire un valido ausilio con numerose indicazioni in grado di guidare le operazioni delle amministrazioni in sede di valutazione delle tecnologie informatiche da acquisire, occorre rilevare che sono le stesse Linee Guida a sottolineare che il loro contenuto e la metodologia ivi descritta «sono da intendersi come ausilio a un percorso decisionale che rimane sotto la piena responsabilità delle amministrazioni, sia nel momento in cui condividano le soluzioni sia quando le adottino in riuso nel rispetto della normativa vigente, in particolare in materia di pubblica amministrazione digitale, contratti pubblici e protezione dei dati personali» (p. 1.1).

Le Linee Guida non sono dunque finalizzate a trasferire il momento di valutazione delle diverse opzioni dall'amministrazione all'AgID. Al contrario, resta in capo all'amministrazione l'onere di svolgere le summenzionate attività finalizzate all'individuazione ed all'acquisizione delle tecnologie informatiche necessarie per lo svolgimento delle proprie funzioni. Considerato tuttavia il carattere interdisciplinare delle competenze richieste per compiere tale valutazione, è facile immaginare che, specie nelle amministrazioni più piccole, possa risultare poco agevole individuare personale sufficientemente qualificato in grado di ingegnerizzare una complessa soluzione informatica.

Non solo. Il processo di digitalizzazione, in caso di errore, può comportare costi molto elevati laddove la soluzione implementata si dimostri fallimentare, o comunque impropria e richieda perciò ulteriori interventi di adeguamento o ridefinizione. L'individuazione e l'acquisizione delle tecnologie informatiche è perciò anche alquanto delicata. La scelta di una soluzione inadeguata – ad esempio perché inefficace sotto un profilo operativo, ovvero perché non conforme al contesto normativo regolante la fattispecie di utilizzo –, potrebbe determinare conseguenze particolarmente dannose, quali il blocco delle attività dell'amministrazione, come anche l'onere di dover implementare *ex novo* un diverso sistema informatico, con tutti i costi ed i rischi a ciò connessi.

Tale circostanza porta così alla luce un ulteriore elemento di complessità nelle operazioni di valutazione delle soluzioni tecnologiche. Il processo decisionale può risentire del timore in capo agli agenti di incorrere in responsabilità amministrativa. Sicché, coloro che siano chiamati a svolgere tale compito potrebbero essere indotti ad optare per la soluzione che li esponga a minori rischi – ad esempio selezionandone una di ampia diffusione, ancorché proprietaria – piuttosto che una che valorizzi effettivamente i criteri normativi e massimizzi le opportunità di sviluppo ed efficientamento per l'ente di riferimento.

Non va poi sottaciuto il fatto che nella valutazione delle diverse opzioni disponibili l'amministrazione sconta con ogni probabilità un marcato *deficit* informativo. Così come si è ampiamente dimostrato in relazione alle procedure ad evidenza pubblica, anche nella ricognizione delle tecnologie disponibili l'amministrazione è altamente probabile che sia soggetta ad una certa asimmetria informativa dovuta alla difficoltà sia di individuare tutte le tecnologie effettivamente esistenti, sia di raccogliere in modo esaustivo tutte le informazioni utili relative a ciascuna di esse.

In sintesi, la valutazione delle soluzioni informatiche da implementare può risultare non agevole per le amministrazioni per almeno tre ordini di ragioni. In primo luogo, la comparazione delle soluzioni da implementare postula il possesso di elevate competenze tecnologiche, di informatica giuridica e manageriali. In secondo luogo, i funzionari pubblici possono essere condizionati nelle scelte dal rischio percepito circa loro eventuali responsabilità. Infine, può risultare complesso ottenere un quadro informativo completo circa tutte le tecnologie disponibili.

Bibliografia

AUBY J.-B., *Données publiques*, in *AD*, 109-30, 2018.

BENVENUTI F., *Il nuovo cittadino*, in *Scritti giuridici*, vol. I, 2006, p. 869.

CARDARELLI F., *Le banche dati pubbliche: una definizione*, in *Il diritto dell'informazione e dell'informatica*, 2002, 2, p. 321.

CARLONI E., *L'amministrazione aperta. Regole strumenti limiti dell'open government*, Rimini, 2014.

CARULLO G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2017.

CARULLO G., *Big Data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Concorrenza e mercato*, vol. 23, 2016, pp. 181-204.

CRAIG P., CURTIN D., DELLA CANANEA G., HOFMANN H.C., MIR O., SCHNEIDER J.-P., WIERZBOWSKI M., J. ZILLER, *Libro I – Disposizioni generali*, in G. DELLA CANANEA, D.-U. GALETTA, H.C.H. HOFMANN, J.-P. ZILLER (a cura di), *Codice ReNEUAL del procedimento amministrativo dell'Unione Europea*, Napoli, 2016, p. 1.

DUNI G., *L'amministrazione digitale: il diritto amministrativo nella evoluzione telematica*, Milano, 2008.

FINOTTO V., FORTE A., *Riuso delle soluzioni e software open source nelle amministrazioni pubbliche*, in E. DI MARIA, S. MICELLI (a cura di), *Le frontiere dell'e-government: cittadinanza elettronica e riorganizzazione dei servizi in rete*, Milano, 2004, p. 149.

GALETTA D.-U., *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in Federalismi.it, 2016, 5, p. 1.

GURIN J., *Open Data Now*, New York, 2014.

KUBICEK H., CIMANDER R., SCHOLL H.J., *Organizational Interoperability in E-Government: Lessons from 77 European Good-Practice Cases*, Berlin, 2011, p. 23.

MASUCCI A., *Erogazione on line dei servizi pubblici e teleprocedure amministrative. Disciplina giuridica e riflessi sull'azione amministrativa*, in *Diritto pubblico*, 2003, p. 991.

PONTI B. (a cura di), *Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale*, 2008.

SCOGNAMIGLIO A., *Diritto di accesso e banche dati pubbliche*, in *Foro amministrativo c.d.s.*, 2005, 2, p. 492.

VII.

GLI STRUMENTI DELLA CARTA DELLA CITTADINANZA DIGITALE

Stefano D'Ancona e Paolo Provenzano[*]

SOMMARIO: 1. Il diritto alla connessione e l'effettività delle norme sulla cittadinanza digitale: considerazioni introduttive. – 2. Il diritto all'uso delle tecnologie e il diritto a servizi *on line* semplici e integrati. – 3. Diritto (obbligo) al domicilio digitale. – 4. L'identità digitale e la firma digitale (rinvio). – 5. Partecipazione democratica elettronica. – 6. Diritto di effettuare i pagamenti con modalità informatiche.

1. Il diritto alla connessione e l'effettività delle norme sulla cittadinanza digitale: considerazioni introduttive

Prima di analizzare gli istituti più importanti che vanno a confluire nella c.d. Carta della cittadinanza digitale è opportuno spendere, in via preliminare, qualche riflessione sul diritto alla connessione alla rete internet che costituisce immancabile supporto all'esercizio delle facoltà previste dalla Carta.

Vale anzitutto la pena di evidenziare come, nonostante la centralità del diritto di connessione, il CAD non contenga alcuna norma ad esso espressamente dedicata, ad eccezione del riferimento, certamente insufficiente, di cui all'art. 8 *bis* CAD (Connettività alla rete internet negli uffici e luoghi pubblici) di cui si dirà.

Una carenza che, senza dubbio, va ad incidere negativamente sulla stessa portata degli istituti di cittadinanza digitale, nonché, in generale, sul diritto all'uso delle nuove tecnologie da parte dei cittadini, ove gli stessi non abbiano la

[*] S. D'ANCONA ha provveduto alla stesura dei parr. 1, 2, 4 e 5. P. PROVENZANO ha provveduto alla stesura dei parr. 3 e 6.

disponibilità di mezzi per la connessione ad una rete internet (v. anche capitolo III, D.-U. GALETTA).

Come ebbe a notare un illustre giurista: «attraverso la considerazione dei diritti fondamentali … si giunge così al tema della cittadinanza digitale, per molti versi ancora nebuloso» (S. RODOTÀ, 2012, p. 384) Punto d'avvio della sua autorevole riflessione era proprio il diritto di accesso a Internet inteso «non solo come diritto a essere tecnicamente connessi alla rete, bensì come espressione di un diverso modo d'essere della persona nel mondo»: sicché, avvertiva l'A., appare insufficiente riferirsi al "servizio universale", «poiché si rischia di concentrarsi quasi esclusivamente sull'apparato tecnico da mettere a disposizione degli interessati» (S. RODOTÀ, 2012, p. 384). Il diritto di accesso ad Internet, infatti, si presenta ormai come sintesi tra una situazione strumentale e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete.

Mentre a livello internazionale vi si fa riferimento via via più sovente in documenti delle Nazioni Unite (cfr. T.E. FROSINI, 2019), a livello europeo il diritto di accesso ad Internet è sancito, seppure in via indiretta, dal Regolamento 2015/2120/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la Direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il Regolamento 2012/531/UE relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione. Il predetto Regolamento, all'art. 3, prevede infatti che gli utenti finali hanno il diritto di accedere a informazioni e contenuti e di diffonderli tramite il servizio di accesso a Internet.

Va tenuto conto che solamente in taluni Paesi è riconosciuto il diritto alla connessione in termini espliciti. In Finlandia, il decreto n. 732/2009 del Ministero dei Trasporti e delle Comunicazioni fa riferimento al livello minimo di accesso funzionale a internet come servizio universale. Nel luglio 2010 è entrata poi in vigore una legge che qualifica espressamente l'accesso a Internet come un diritto da garantire a tutti i cittadini del Paese. Analoga è l'impostazione del legislatore spagnolo, che con legge sull'economia sostenibile risalente al 2011, ha elevato l'accesso a internet al rango di servizio universale. In Francia, il *Conseil constitutionnel* ha affermato che la connessione a internet è stata riconosciuta come un diritto fondamentale del cittadino (décision n. 2009-580 DC del 10 giugno 2009). Infine, la Grecia ha modificato la propria Costituzione per introdurre l'art. 5-*bis*, il cui secondo comma stabilisce che «tutte le persone hanno il diritto di partecipare alla società dell'informazione, facilitandone l'accesso alle informazioni trasmesse elettronicamente, così come il diritto di produrre, scambiare e diffondere informazioni mediante mezzi elettronici costituisce un obbligo dello Stato, nel rispetto delle garanzie degli artt. 9 e 19 Cost.».

In Italia, il riferimento è agli artt. 17 e 18 Cost. che tuttavia non se ne occupano ovviamente in modo diretto (sul tema si rinvia al capitolo I, A. SIMONCINI). Qualche spiraglio è poi fornito solamente da alcune normative regionali. Ad esempio, la Legge Reg. Umbria 13 dicembre 2013, n. 31, che ha riconosciuto «il diritto di tutti i cittadini di accedere a internet quale fondamentale strumento di sviluppo umano e di crescita economica e sociale e promuove lo sviluppo delle infrastrutture di telecomunicazione al fine di assicurare la partecipazione attiva alla vita della comunità digitale» (art. 1, comma 1). In Emilia Romagna, la Legge Reg. del 24 maggio 2004, n. 11, definisce il proprio impegno nel garantire ai cittadini «un più facile e diffuso accesso alla conoscenza» (art. 1, comma 1, lett. a), promuovendo in particolare «l'accesso generalizzato dei cittadini all'utilizzo delle tecnologie, anche mediante l'organizzazione di corsi di formazione finalizzati a promuovere l'alfabetizzazione digitale» (art. 3, comma 2, lett. c). Infine, la Legge Reg. Piemonte 26 marzo 2009, n. 9, all'art. 1, «favorisce il pluralismo informatico, garantisce l'accesso e la libertà di scelta nella realizzazione di piattaforme informatiche e favorisce l'eliminazione di ogni barriera dovuta all'uso di standard non aperti».

Al di là di questo, a livello nazionale si segnala esclusivamente un documento della Camera dei Deputati, titolato «Dichiarazione dei diritti di Internet» ed approvato il 28 luglio 2015 dalla Commissione per i diritti e i doveri relativi ad Internet. All'art. 2 la dichiarazione prevede il diritto di accesso a Internet quale «diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale» (per una rassegna, G. FINOCCHIARO, 2016. V. anche al capitolo I, A. SIMONCINI).

Per concludere occorre osservare che, durante l'emergenza COVID-19, l'accesso ad internet ha indubbiamente rappresentato il principale – se non unico – strumento che ha permesso ai cittadini di fruire di servizi pubblici essenziali, quali ad esempio l'istruzione, sia di base che universitaria. Ma ha anche rappresentato un fondamentale elemento di integrazione tra diritti fondamentali garantiti dalla Carta costituzionale quale il diritto alla salute (art. 32) e il diritto al lavoro (art. 2 Cost.) (si consideri l'utilizzo delle formule organizzative flessibili di *smart working*).

È evidente tuttavia che, uscendo da una logica emergenziale, questa non potrà che essere la "strada" futura in grado di fare evolvere il sistema in maniera più coerente con i principi di uguaglianza e giustizia sociale. In questo senso, è da accogliere con favore la recente modifica, inserita all'art. 12, comma 3-*ter*, del CAD dal D.L. n. 76/2020 (D.L. 16 luglio 2020, n. 76 Misure urgenti per la semplificazione e l'innovazione digitale convertito, con modificazioni, dalla Legge 11 settembre 2020, n. 120).

Il legislatore, proprio nell'intento di diffondere buone prassi in tema di organizzazione lavorativa, ha previsto infatti che le pubbliche amministrazioni «al

fine di agevolare la diffusione del lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato acquistano beni e progettano e sviluppano i sistemi informativi e i servizi informatici con modalità idonee a consentire ai lavoratori di accedere da remoto ad applicativi, dati e informazioni necessari allo svolgimento della prestazione lavorativa».

Ogni evoluzione organizzativa dovrà avvenire nel rispetto della normativa lavoristica, « assicurando un adeguato livello di sicurezza informatica, in linea con le migliori pratiche e gli standard nazionali ed internazionali per la protezione delle proprie reti, nonché a condizione che sia data al lavoratore adeguata informazione sull'uso sicuro degli strumenti impiegati, con particolare riguardo a quelli erogati tramite fornitori di servizi in cloud, anche attraverso la diffusione di apposite linee guida, e disciplinando anche la tipologia di attività che possono essere svolte, previa informazione alle organizzazioni sindacali » (art. 12, comma 3-*ter,* cit.).

Un'altra questione, strettamente connessa, attiene all'effettività delle norme in materia di cittadinanza digitale.

Se da una parte è estremamente importante che le disposizioni del CAD abbiano dato riconoscimento agli istituti di cittadinanza digitale, il legislatore non ha previsto sanzioni a carico delle Pubbliche Amministrazioni inadempienti rispetto agli obblighi di riorganizzazione e modellazione di procedimenti amministrativi e dei servizi-on line secondo i nuovi strumenti messi a disposizione del cittadino-utente.

A questo proposito, il Consiglio di Stato, nel parere sulla bozza del testo del Codice, afferma che le norme contenute nel CAD non forniscono ai cittadini alcuno strumento di tutela amministrativa e giurisdizionale avverso l'inadempimento degli obblighi digitali da parte delle Amministrazioni (Parere Consiglio di Stato Adunanza 7 febbraio 2015 n. 11995/04, punto 7, in www.giustizia-amministrativa.it).

È dunque auspicabile che, ai fini di una maggiore effettività delle norme in questione, il legislatore prenda posizioni nette su questo aspetto.

Certo, l'analisi delle disposizioni in tema di cittadinanza digitale porta in evidenza l'emersione di nuove posizioni giuridiche soggettive prima sconosciute nell'ambito del rapporto tra cittadini e pubbliche amministrazioni.

2. Il diritto all'uso delle tecnologie e il diritto a servizi *on line* semplici e integrati

Il CAD prevede, all'art. 3, che chiunque ha il «diritto» di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice «nei

rapporti» con le pubbliche amministrazioni e i gestori di servizi pubblici (art. 3, comma 1, CAD). Ciò «anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo», fermi restando i diritti delle minoranze linguistiche riconosciute (art. 3, comma 1, cit.).

La norma è strettamente connessa con l'art. 7 CAD sui servizi *on-line* il quale prevede che chiunque ha diritto di «fruire dei servizi» erogati dai soggetti pubblici, in forma digitale e in modo integrato, «tramite gli strumenti telematici messi a disposizione dalle pubbliche amministrazioni, anche attraverso dispositivi mobili» (art. 7, comma 1, CAD). Tali disposizioni sono volte a rafforzare le previsioni già contenute nella Legge 9 gennaio 2004, n. 4 recante «Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici», ove all'art. 1, il legislatore aveva espressamente garantito il «diritto di accesso ai servizi informatici e telematici della pubblica amministrazione, nonché alle strutture ed ai servizi aperti o forniti al pubblico attraverso i nuovi sistemi e le tecnologie di informazione e comunicazione in rete e ai servizi di pubblica utilità da parte delle persone con disabilità, in ottemperanza al principio di uguaglianza ai sensi dell'articolo 3 della Costituzione» (art. 1, Legge n. 4/2004, modificato dal D.L. n. 76/2020, convertito con la Legge 11 settembre 2020, n. 120).

Tornando alle norme del CAD sopra richiamate, va evidenziato innanzitutto che si tratta di disposizioni generali dirette non solo ai cittadini ma, in virtù della locuzione «chiunque», a tutti i soggetti (siano essi persone giuridiche, siano essi persone fisiche) che hanno rapporti con le Amministrazioni pubbliche o gestori di servizi pubblici.

Dal punto di vista sostanziale, i disposti dei due articoli, per l'ampiezza di formulazione, rafforzano le norme specifiche contenute nella Sezione II del Capo I concernenti il domicilio digitale, i pagamenti con modalità informatiche e tecnologiche e l'identità digitale.

Mentre l'art. 3 CAD infatti va a "coprire" generalmente i "rapporti" tra cittadino e P.A., anche in ambito procedimentale, l'art. 7 CAD lascia spazio per immaginare servizi *on-line* di ogni genere, erogati da Pubbliche amministrazioni o gestori di servizi pubblici e a cui il cittadino avrebbe diritto di accedere da casa propria o da qualunque altro posto in cui vi sia la disponibilità di un accesso a *internet* (C. FLICK, V. AMBRIOLA, 2006). Allo stato, tuttavia, tale situazione è di difficile configurazione, considerato che, spesso, per accedere ai servizi, i cittadini sono costretti rivolgersi a "mediatori" specializzati che si rapportano con l'Amministrazione (si pensi alle ispezioni ipotecarie e visure catastali, attraverso avvocati e notai, al pagamento di imposte e tasse e ricorsi in materia tributaria, attraverso commercialisti e centri autorizzati di assistenza fiscale CAF e infine allo svolgimento di pratiche urbanistiche, attraverso architetti, geometri e agenzie).

La situazione potrà evolversi solamente allorché le Amministrazioni si assumeranno più responsabilità nel processo di digitalizzazione (in termini di informazione dettagliata verso il cittadino, ma anche di riorganizzazione per erogare i servizi nelle nuove forme) e i cittadini assumeranno la consapevolezza di dover acquisire le necessarie competenze digitali per fruire in maniera piena dei nuovi diritti e facoltà (C. FLICK, V. AMBRIOLA, 2006). Con riferimento a questo ultimo aspetto, peraltro, il CAD prevede l'obbligo dello Stato di favorire tra i cittadini la diffusione della cultura digitale e promuovere fenomeni di alfabetizzazione informatica (cfr. art. 8 CAD).

Nel quadro dei servizi on line, il CAD configura in capo alle Pubbliche Amministrazioni, un obbligo, seppure generale, di riorganizzazione e aggiornamento dei servizi resi (art. 7, comma 1, CAD).

Tale obbligo è parametrato sulla base di un'analisi di costi e benefici e secondo livelli di qualità individuati dall'Agenzia per l'Italia Digitale.

In caso di violazione, al comma 4 dell'art. 7 CAD, è prevista una forma blanda di tutela per i cittadini che possono agire mediante la *class action* contro le inefficienze dei servizi della P.A., secondo le disposizioni contenute nel D.Lgs. n. 198/2009, oppure rivolgersi al difensore civico digitale.

All'art. 3, come sopra accennato, il CAD estende l'utilizzo delle nuove tecnologie ai procedimenti amministrativi.

La norma, dunque, crea un collegamento con la Legge n. 241/1990.

Si rammenta come, proprio nel contesto di quest'ultima normativa generale, il legislatore avesse inserito nella Legge n. 241/1990, all'art. 3-*bis*, poco prima dell'emanazione del CAD, la disposizione secondo cui «per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati» (art. 3-*bis* Legge n. 241/1990 come integrato dall'art. 3 Legge 11 febbraio 2005, n. 15). Dunque, l'art. 3 CAD costituisce un completamento del percorso normativo già avviato nel contesto della legge generale sul procedimento.

Nonostante la tensione posta dal legislatore nella disposizione codicistica – che usa l'espressione «diritti» –, sembrerebbe che non si tratti di "diritti" in senso stretto, ma semplicemente di interessi strumentali rispetto a posizioni giuridiche qualificate (F. CARDARELLI, 2015).

Secondo altra tesi, l'art. 3 CAD costituirebbe addirittura una mera norma di principio che va a coniugare, rispetto all'amministrazione digitale, posizioni giuridiche soggettive comunque riconosciute dall'ordinamento attraverso la mediazione dell'art. 2 della Costituzione quale fattispecie aperta ai mutamenti della coscienza sociale, o quale principio generale del libero sviluppo della personalità (E. D'ORLANDO, 2011).

L'incertezza nell'inquadramento dal punto di vista sostanziale del diritto all'utilizzo delle nuove tecnologia incide anche sull'effettività della tutela giurisdizionale. L'art. 3, comma 3-*bis*, CAD prevede che essa sia in capo al giudice amministrativo e, tuttavia, la giurisprudenza parla espressamente di pretesa non azionabile.

Ha osservato, infatti, il Consiglio di Stato che «la situazione soggettiva tutelata non è un diritto soggettivo in senso proprio, poiché tale situazione non è tutelata nella sua pienezza allorché non vi siano le necessarie risorse» (ossia, le risorse per le Pubbliche Amministrazioni necessarie alla riorganizzazione in funzione dei diritto all'uso delle nuove tecnologie) (Consiglio di Stato parere Sez. consultiva atti normativi, parere 31/2006 con riferimento alla disposizione, poi abrogata nel 2010, sui limiti di applicabilità del principio a seconda delle risorse disponibili; cfr. parere Cons. Stato 7 febbraio 2005 n. 11995). Né, ovviamente, continuano i Giudici amministrativi, «sarebbe costituzionalmente consentito differenziare la situazione soggettiva in relazione alla diversa amministrazione (statale o meno) cui il cittadino o l'impresa chiede l'uso delle tecnologie» (Cons. Stato, *cit.*, in dottrina D. DE GRAZIA, 2011).

Proprio per questa carenza, in termini pratici, il giudice potrebbe soddisfare le pretese del cittadino solamente nel caso in cui, dal mancato rispetto dell'art. 3 CAD, derivi un pregiudizio risarcibile ai sensi dell'art. 2043 c.c. (F. CAMILLETTI, 2008).

Questa, del resto, è la posizione assunta dalla giurisprudenza nel caso in cui venga violata in generale una norma procedimentale strumentale all'esercizio di facoltà da parte del cittadino (Cons. Stato, sez. IV, 22 ottobre 2015, n. 4823).

Strettamente connesso all'art. 3 CAD è infine il successivo art. 8-*bis* del medesimo CAD.

Si tratta, come già accennato, della norma sulla connettività alla rete Internet negli uffici e luoghi pubblici. Essa si differenzia rispetto al generale diritto alla connessione cui si è fatto cenno nella premessa, poiché non ha ad oggetto quello che da alcuni è definito un servizio universale.

Analizzando la disposizione, in effetti, sembra che il legislatore abbia volontariamente limitato il diritto di connessione a luoghi ben definiti, circoscrivendolo, piuttosto che connotandolo, quale *pendant* di un più ampio diritto di cittadinanza digitale.

3. Diritto (obbligo) al domicilio digitale

Come chiarito dall'art. 1, lett. n-*ter*) del CAD, con la locuzione "domicilio digitale" s'intende «un'indirizzo elettronico eletto presso un servizio di posta

elettronica certificata o un servizio elettronico di recapito certificato qualificato (…) valido ai fini delle comunicazioni elettroniche aventi valore legale». Si tratta, in altri termini, di un indirizzo di posta elettronica che assume rilevanza ufficiale, posto che le comunicazioni ivi trasmesse si considerano, ad ogni effetto di legge, come inviate al loro destinatario e dallo stesso conosciute.

Ai sensi dell'art. 6 CAD, infatti, «le comunicazioni elettroniche trasmesse [ad un domicilio digitale] producono quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono [di regola] alla notificazione per mezzo della posta».

La disciplina del "domicilio digitale" è oggi fissata da sei diverse disposizioni del CAD. Essa, infatti, è contenuta, oltre che nel già citato art. 6, nei successivi articoli da 6-*bis* a 6-*quinques* e anche, e prima ancora, nell'art. 3-*bis*, che costituisce la norma principale in materia, della quale si passa a trattare.

Inserito nel *corpus* del Codice nel 2012, per opera del D.L. n. 179/2012, l'art. 3-*bis* ha nel corso degli anni subito cinque sostanziali riforme, che ne hanno, anzitutto, modificato la rubrica. Detta norma, infatti, originariamente titolata «Domicilio digitale del cittadino», è oggigiorno rubricata «Identità digitale e Domicilio digitale», dopo essere stata titolata, tra il 2016 e il 2018, e più precisamente tra il D.Lgs. n. 169/2016 e il D.Lgs. n. 217/2017, «Domicilio digitale delle persone fisiche».

Come si evince già dalle modifiche operate alla sua intestazione, la disciplina in parola ha visto nel corso degli anni estendere progressivamente il suo ambito di applicazione soggettivo.

Quella sul "domicilio digitale", infatti, non è più una disciplina rivolta ai soli "cittadini" o alle sole "persone fisiche", ma riguarda, almeno potenzialmente, "chiunque" e, dunque, tutte le persone fisiche e tutte le persone giuridiche (siano esse private, siano esse pubbliche).

Occorre tuttavia segnalare che il citato art. 3-*bis* opera una netta distinzione tra soggetti che sono *obbligati* a dotarsi di un "domicilio digitale" e soggetti che hanno, viceversa, almeno per il momento, la semplice *facoltà* di eleggerne uno.

Rientrano nella prima categoria, anzitutto, le Pubbliche amministrazioni, i gestori di servizi pubblici e le società a controllo pubblico. E ciò in virtù del rinvio all'art. 2, comma 2, CAD operato dal primo comma dell'articolo in questione.

L'obbligo di dotarsi di un "domicilio digitale" sussiste poi, come previsto sempre dal comma primo della norma in commento, anche in capo ai «professionisti tenuti all'iscrizione in albi ed elenchi» (si tratta degli avvocati, degli architetti, degli ingegneri, ecc.) e ai «soggetti tenuti all'iscrizione nel registro delle imprese».

Come osservato in dottrina, con riferimento a tali soggetti il legislatore (a torto o a ragione) ha operato una sorta di «presunzione di alfabetizzazione informatica» (E. CARLONI, 2011), da cui ha fatto scaturire l'obbligatorietà dell'elezione di un "domicilio digitale".

Come si è anticipato, l'art. 3-*bis* prevede poi che i soggetti diversi da quelli per cui sussiste l'obbligo di individuazione di un "domicilio digitale", abbiano comunque la *facoltà* di eleggerne uno e, dunque, di indicare l'indirizzo di posta elettronica a cui intendono ricevere (anzitutto dalla Pubblica Amministrazione) le comunicazioni ufficiali.

Una volta che tali ultimi soggetti abbiano esercitato detta facoltà, gli stessi sostanzialmente si "autovincolano" al rispetto delle medesime disposizioni applicabili a coloro che abbiano, invece, l'obbligo di elezione di un "domicilio digitale".

Tutti i soggetti dotati di un "domicilio digitale" sono, infatti «obblig(ati) [a] far(ne) un uso diligente e [a] comunicare ogni modifica o variazione del medesimo» (art. 3-*bis*, comma 1-*quater*, CAD). Modifiche e variazioni di cui si deve dare atto negli appositi elenchi cui fa riferimento l'art. 6 CAD.

In base a tale ultima previsione, infatti, tutti i "domicili digitali" (siano essi eletti obbligatoriamente o facoltativamente) devono essere riportati in appositi elenchi ufficiali. Si tratta di tre distinti elenchi menzionati dal comma 1-*ter* dell'art. 6 CAD e che vengono poi specificamente disciplinati dai successivi artt. 6-*bis*, 6-*ter* e 6-*quater* del medesimo CAD.

Il primo di detti elenchi (c.d. elenco INI-PEC, che sta per Indice Nazionale dei domicili digitali) è quello che contiene gli indirizzi di posta elettronica certificata (*id est* i "domicili digitali") delle imprese, ivi incluse le Società in mano pubblica, e dei professionisti. Detto elenco, come chiarito dall'art. 6-*bis* CAD, è istituito presso il Ministero per lo sviluppo economico, che lo predispone acquisendo, anzitutto, gli indirizzi pec indicati nel registro delle imprese e negli albi degli ordini e dei collegi professionali, nonché dagli elenchi o registri di professionisti detenuti dalle Pubbliche amministrazioni, come da ultimo previsto dal D.L. n. 76/2020, convertito con la Legge 11 settembre 2020, n. 120.

Il citato art. 6-*bis* chiarisce poi che «i domicili digitali inseriti in tale Indice costituiscono *mezzo esclusivo* di comunicazione e notifica con i soggetti [pubblici]», ribadendo, così, quanto già stabilito dal comma 1-*quater* dell'art. 6 CAD, a mente del quale le Pubbliche amministrazioni «notificano direttamente presso i domicili digitali [risultanti dagli elenchi in questione] i propri atti, compresi i verbali relativi alle sanzioni amministrative, gli atti impositivi di accertamento e di riscossione e le ingiunzioni [fiscali]», e quanto previsto (anche e prima ancora) dal comma 4 dell'art. 3-*bis* CAD, che, a sua volta, prevede che «a decorrere dal 1° gennaio 2013 (…) le amministrazioni pubbliche o esercen-

ti di pubblici servizi comunicano con il cittadino *esclusivamente* tramite il domicilio digitale dallo stesso dichiarato».

Gli indirizzi pec riportati in detto elenco acquisiscono, però, rilevanza – è bene chiarirlo – non soltanto nei rapporti tra amministrazione e privati. Essi, infatti, possono essere utilizzati anche nei rapporti interprivatistici, ad esempio per la notifica di una diffida.

Il secondo elenco cui fa riferimento il comma 1-*ter* dell'art. 6 CAD è quello che contiene i "domicili digitali" delle Pubbliche amministrazioni e dei gestori dei servizi pubblici. Si tratta del c.d. elenco IPA, nel quale, a mente dell'art. 6-*ter* CAD, «sono indicati i domicili digitali da utilizzare per la comunicazione e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati».

L'art. 6-*ter* prevede poi, da un lato, che la realizzazione e la gestione di detto elenco è demandata all'AgID e, dall'altro, che spetta a ciascuna amministrazione e a ciascun gestore di pubblico servizio il compito di aggiornare «gli indirizzi e i contenuti dell'Indice tempestivamente e comunque con cadenza semestrale». Detta medesima norma dispone poi che, in caso di mancata comunicazione, i soggetti responsabili sono passibili di responsabilità dirigenziale.

L'ultimo elenco richiamato dal più volte citato comma 1-*bis* dell'art. 6 è quello in cui vengono riportati i "domicili digitali" di tutti gli altri soggetti che, pur non essendovi obbligati, abbiano comunque facoltativamente deciso di eleggere un proprio "domicilio digitale".

Per differentiam, detto elenco, noto come elenco INAD, contiene dunque gli indirizzi pec «delle persone fisiche, dei professionisti e degli altri enti di diritto privato *non* tenuti all'iscrizione nell'indice di cui all'articolo 6-*bis*» (art. 6-*quater* CAD), che abbiano cionondimeno autonomamente deciso di eleggere "domicilio digitale", con tutte le conseguenze di cui si è detto in precedenza e tra queste – giova ribadirlo –, anche quella, per cui, una volta eletto, il domicilio facoltativo diventa lo strumento *esclusivo* di cui si avvalgono le amministrazioni pubbliche per inviare comunicazioni ai privati.

Anche tale elenco è tenuto dall'AgID, che sta all'uopo predisponendo delle apposite linee guida, in cui si disciplinano, anzitutto, le modalità di iscrizione in detto elenco. Iscrizione che, in base a quanto previsto dall'art. 3-*bis* CAD, come modificato dal D.L. n. 76/2020, è condizionata all'effettiva operatività del domicilio digitale. Il novellato comma 1-*bis* di detto articolo dispone, infatti, che «nel caso in cui il domicilio eletto risulti *non più attivo* si procede alla cancellazione d'ufficio [dello stesso] dall'indice di cui all'articolo 6-*quater*».

Ne deriva, dunque, che il soggetto che abbia *sua sponte* eletto un domicilio

digitale, pur non essendovi tenuto, può sempre tornare sui propri passi disattivando lo stesso, con conseguente automatica cancellazione del medesimo dall'Indice di cui si discorre.

Sempre con riferimento a tale elenco è, infine, previsto che verranno all'uopo predisposte delle linee guida volte a disciplinare le modalità di gestione e di aggiornamento dello stesso. E ciò anche «nei casi di decesso del titolare del domicilio digitale eletto o di impossibilità sopravvenuta di avvalersi del domicilio» (art. 3-*bis*, comma 1-*quater*, CAD).

Ciò detto, occorre sottolineare che, ai sensi dell'art. 6-*quinques* CAD, gli elenchi testé passati in rassegna devono poter essere accessibili da «chiunque senza necessità di autenticazione». Essi, dunque, devono poter essere consultati gratuitamente on-line. Il che porta inevitabilmente al rischio che i "domicili digitali", in quanto alla mercé di tutti, possano essere impropriamente utilizzati per l'invio di comunicazioni indesiderate.

Al fine di limitare tale rischio è stato opportunamente chiarito (e da ultimo ribadito dal più volte citato D.L. n. 76/2020) che l'invio, senza il previo consenso dei destinatari, di comunicazioni commerciali di carattere promozionale e di materiale pubblicitario ai "domicili digitali" porta all'irrogazione delle sanzioni di cui al D.Lgs. n. 70/2013, nonché a quelle previste dal Regolamento 2016/679/UE (c.d. GDPR).

Tornando agli elenchi di cui si è detto, è appena il caso di osservare che la loro stessa esistenza, com'è stato osservato in dottrina, «pales(a) un grave insuccesso del processo di riforma» e, più precisamente, la difficoltà operativa che si è riscontrata (e continua a riscontrarsi) nella creazione della Anagrafe nazionale della popolazione residente (ANPR) di cui all'art. 62 CAD (B. CAROTTI, 2018). Anagrafe che, negli intendimenti del legislatore, dovrebbe contenere, tra l'altro, anche tutti i "domicili digitali" delle persone fisiche.

Al di fuori di quanto sin qui detto, è necessario segnalare che è, sia pur in via a transitoria, prevista, sempre dal CAD, la possibilità di eleggere per determinati atti o affari un domicilio digitale speciale ai sensi dell'art. 47 del codice civile, cui devono, dunque, essere indirizzate tutte le comunicazioni relative a quel determinato atto o affare. E ciò vale sia per i soggetti che non abbiano alcun "domicilio digitale", sia per quelli che abbiano già un "domicilio digitale", ma che decidano di avvalersi per le questioni attinenti a quel determinato rapporto di un "domicilio digitale" diverso da quello a loro riconducibile in base agli elenchi di cui si è detto in precedenza (si pensi, ad esempio, all'impresa che nei rapporti con l'Agenzia dell'Entrate dedica di eleggere, come domicilio speciale, quello del proprio commercialista).

In tale evenienza, come espressamente previsto dal comma 4-*quater* del più volte citato art. 3-*bis* CAD, «colui che ha eletto [domicilio speciale] non può

opporre eccezioni relative alla forma e alla data di spedizione e del ricevimento delle comunicazioni o notificazioni ivi indirizzate».

Fin qui si è trattato della disciplina attualmente vigente come da ultimo integrata dal D.L. n. 76/2020. Si deve tuttavia segnalare che il comma 3-*bis* dell'art. 3-*bis* CAD, anch'esso in parte novellato dal c.d. DL-semplificazioni, contiene una norma di carattere programmatico, che prevede che in un prossimo futuro (incerto nel *quando* e diremmo anche nell'*an*) tutti i soggetti, e quindi anche quelli non tenuti ad avere un domicilio digitale e che non ne abbiano autonomamente individuato uno, potrebbero vedersi «reso disponibile un domicilio digitale».

Si prevede, infatti, che con Decreto del Presidente del Consiglio dei ministri o di un Ministro delegato per la semplificazione e la Pubblica Amministrazione verrà «stabilita la data a decorrere dalla quale le comunicazioni tra i soggetti [pubblici] e coloro che non hanno provveduto a eleggere un domicilio digitale (…) *avve(rranno) esclusivamente in forma elettronica*». L'idea dunque pare essere quella di estendere a chiunque la disciplina oggi prevista dall'art. 5-*bis* CAD nelle comunicazioni tra imprese e amministrazioni, che già oggi devono avvenire «esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione».

Si tratta, a parere di chi scrive, di un ambizioso obiettivo di cui ben si comprendono i vantaggi in termini di risparmio delle risorse e di efficienza dell'agire amministrativo, ma che non potrà certamente essere raggiunto prima dell'effettivo superamento del divario digitale (sia strutturale, sia culturale) presente nel nostro Paese e che è risultato ancor più evidente durante i mesi di *lockdown* collegati all'esplosione della pandemia da COVID-19. Diversamente, infatti, si correrebbe il rischio, come già evidenziato in altra occasione, di assistere a una sorta di «reviviscenza, ma in chiave 2.0, della distinzione tra "Paese legale" (chi ha accesso ad *internet* e, di conseguenza, al proprio "domicilio digitale") e "Paese reale" (tutti gli altri soggetti che, per un motivo o per un altro, hanno viceversa difficoltà ad accedere al *web*» (P. PROVENZANO, 2016).

4. L'identità digitale e la firma digitale (rinvio)

La stretta connessione della nozione di "identità digitale" a quella di "identità personale" impone una breve notazione in ordine a tale ultima espressione.

L'identità personale costituisce, secondo la dottrina, il contenuto di un "diritto personale" che consiste nel diritto di essere se stessi.

Il diritto all'identità personale, tuttavia, non è tanto l'immagine che il soggetto ha di sé (verità personale), quanto piuttosto l'immagine socialmente me-

diata del soggetto stesso (G. BAVETTA, 1970). Proprio per questa ragione, la tutela del diritto all'identità personale è inteso come il diritto a «non vedere travisata la propria personalità individuale» (A. DE CUPIS, 1961).

Secondo la giurisprudenza l'identità personale è, dunque, un bene — valore costituito dalla proiezione sociale della personalità dell'individuo, cui si collega un interesse del soggetto ad essere rappresentato con la sua vera identità (Cass., 7 febbraio 1996, n. 978, in *Foro it.*, 1996, I, 1253; cfr. anche Corte cost., 3 febbraio 1994, n. 13, in www.cortecostituzionale.it).

Al diritto all'identità personale, che è dunque espressione intima della persona, attengono due modalità di espressione nel mondo esterno.

La prima riferita alla corretta proiezione sociale del soggetto cui si è fatto cenno, la seconda riconducibile a dati oggettivi, cioè ai segni identificativi del soggetto oggettivamente rilevabili (es. dati anagrafici), che servono ad identificare il soggetto nei suoi rapporti con i poteri pubblici e a distinguerlo dagli altri consociati (G. FALCO, 1938).

Mentre nel primo caso l'interesse alla tutela dell'identità personale è soprattutto del soggetto cui è riferita l'identità, nel secondo caso l'interesse ad una corretta identificazione è non solo del soggetto cui è riferita l'identità ma anche degli altri consociati e delle Amministrazioni, per una problematica connessa alla sicurezza dei rapporti giuridici (G. FINOCCHIARO, 2010).

Secondo una più moderna accezione, oltre ai dati anagrafici, l'identità personale è rappresentata oggettivamente da altri dati sempre attinenti alla persona. Tale prospettazione trova conferma fin dalla prima versione del Codice in materia di protezione dei dati personale, all'art. 1 Legge n. 675/1996 (ora art. 2 D.Lgs. n. 196/2003): le predette norme tuttavia non forniscono definizioni specifiche di "identità personale" che trova dunque riscontro in quanto già esposto dalla dottrina e giurisprudenza (G. RESTA, 2007) (sulla nozione di dato personale v. capitolo II, ROSSI DAL POZZO e capitolo VI, G. CARULLO).

Passando all'esame della nozione di "identità digitale" può preliminarmente osservarsi che per diritto all'identità digitale si intende, in questa sede, qualcosa di diverso rispetto a ciò che si intende per diritto all'identità digitale nel contesto del diritto dell'informazione.

In quell'ambito la formula identità digitale riassume efficacemente «non solo la proiezione sulla rete dell'identità personale, ma anche la possibile creazione di una soggettività diversa dal sé, pur se ad esso riconducibile, un alter ego virtuale, c.d. avatar» (I. SIGISMONDI, 2008).

Invece, l'identità digitale nel diritto dell'amministrazione digitale assume rilievo con riferimento all'identificazione del cittadino per la fruizione dei servizi on-line ma anche nei procedimenti digitali.

Il rilievo dell'istituto emerge dopo l'entrata delle norme in materia di digi-

talizzazione contenute nel CAD e più precisamente a seguito delle modifiche ad esso apportate dal D.Lgs. n. 179/2016 attuativo della c.d. Legge Madia.

Prima della modifica decisiva del 2016, il CAD prevedeva che le pubbliche amministrazioni potessero consentire l'identificazione informatica dei cittadini per l'accesso ai servizi in rete da esse erogati, «anche *con strumenti diversi* dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'*individuazion*e del soggetto che richiede il servizio» (art. 64, comma 2, CAD). Nel 2013 fu poi precisato, nella stessa disposizione, che per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, fosse istituito, a cura dell'Agenzia per l'Italia digitale, «il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese» (SPID) (art. 64, comma 2-*bis*, CAD, come integrato dall'art. 17-*ter*, comma 2, D.L. 21 giugno 2013, n. 69 convertito in Legge n. 98/2013, per la cui attuazione è stato emanato il D.P.C.M. 24 novembre 2014).

È tuttavia solamente con l'entrata in vigore del D.Lgs. n. 179/2016 che viene inserita, all'interno del CAD, una definizione della nozione di "identità digitale" (art. 1, comma 1, lett. f), D.Lgs. n. 179/2016).

L'art. 1 CAD prevede infatti che per identità digitale si intenda «la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64» (art. 1, comma 1, lett. u-*quater*), CAD).

Dello SPID e della sua attuazione si tratterà nel prosieguo quando si esaminerà l'art. 64 CAD.

A livello generale, l'identità digitale è uno degli elementi essenziali della cittadinanza digitale proprio perché è il presupposto per la fruizione da parte dei cittadini dei servizi *on line* erogati dalle Pubbliche amministrazioni e dai gestori dei servizi pubblici (ad esempio l'*e-health* fornito dalle strutture sanitarie oppure l'*e-learning* somministrato da alcuni Atenei) (cfr. art. 1, comma 1, lett. n-*quater*), CAD).

In questo senso, l'art. 3-*bis*, comma 1, CAD prevede che chiunque ha il diritto di accedere «tramite la propria identità digitale» ai servizi *on-line* offerti dai Soggetti pubblici di cui all'art. 2, comma 2, lett. a) e b), CAD (Pubbliche Amministrazioni in senso tradizionale e gestori di servizi pubblici).

La norma è stata recentemente modificata dal D.L. n. 76/2020, che ne ha esteso l'applicazione anche ai soggetti di cui all'art. 2, comma 2, lett. c), e cioè le società a controllo pubblico come definite dal D.Lgs. n. 175/2016.

Esaminando ora gli strumenti a disposizione del cittadino per permetterne l'identificazione, va considerata, innanzitutto, la correlazione tra identità digitale, servizi in rete (art. 64 CAD) e procedimenti digitali (art. 65 CAD).

Il CAD collocava l'identità digitale, e dunque il sistema SPID (Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese) ad essa funzionale, come strumento privilegiato di identificazione rispetto alla carta di identità elettronica e alla carta nazionale dei servizi. Tant'è che l'art. 65, comma 2, lett. b) CAD prevedeva – prima della modifica di cui si dirà – che, ai fini della presentazione di istanze e dichiarazioni in via telematica, il cittadino fosse identificato «attraverso il sistema pubblico di identità digitale (SPID), *nonché attraverso uno degli altri strumenti di cui all'articolo 64, comma 2-novies*, nei limiti ivi previsti», dando dunque rilievo meramente residuale alla carta nazionale dei servizi e alla carta di identità elettronica.

Di recente, tuttavia, il D.L. n. 76/2020 è intervenuto in controtendenza, attribuendo "pari dignità" agli strumenti alternativi rispetto allo SPID, ed in particolare, alla carta di identità elettronica. In questo senso, va interpretato, sia il richiamo all'art. 65, lett. b) alle due carte, sia i reiterati richiami alla carta d'identità elettronica contenuti all'art. 64, commi 2-*quater* e 2-*quinquies*, per l'accesso ai servizi in rete. Decisiva è poi la norma inserita dal predetto D.L., all'art. 64, comma 3-*bis*, CAD, in cui si è stabilito che a decorrere dal 28 febbraio 2021 le pubbliche amministrazioni di cui all'art. 2, comma 2, lett. a), utilizzeranno esclusivamente «le identità digitali e la carta di identità elettronica ai fini dell'identificazione dei cittadini che accedono ai propri servizi on-line».

In ogni caso, «la verifica dell'identità digitale con livello di garanzia almeno significativo, ai sensi dell'articolo 8, paragrafo 2, del Regolamento 2014/910/UE del Parlamento e del Consiglio europeo del 23 luglio 2014, produce, nelle transazioni elettroniche o per l'accesso ai servizi in rete, gli effetti del documento di riconoscimento equipollente» (art. 64, comma 2-*duodeces*, CAD, come mod. D.L. n. 76/2020 convertito, con mod., dalla Legge n. 120/2020).

In altri termini, l'identità digitale viene equiparata, in termini di efficacia, agli altri strumenti di riconoscimento "equipollenti" alla carta di identità, previsti dall'art. 35 D.P.R. n. 445/2000.

L'intento del legislatore è chiaramente quello di emancipare il cittadino digitale che accede ai servizi in rete, consentendogli il superamento del fastidioso onere amministrativo della trasmissione della copia del documento di identità ai fini di identificazione.

Il legislatore ha previsto inoltre che l'accesso ai servizi in rete, di cui all'art. 64, comma 2-*quater*) CAD, è possibile al cittadino anche «attraverso il punto di accesso telematico di cui all'articolo 64-*bis*» (art. 24, comma 1, lett. a), punto 1, modificato dal D.L. n. 76/2020 conv. dalla Legge n. 120/2020).

Anche questa disposizione ha indubbiamente ampliato la cittadinanza digitale, così come l'art. 64-*bis* CAD. La disposizione, del tutto revisionata dal

D.L. n. 76/2020, ha inserito, infatti, l'obbligo delle pubbliche amministrazioni di rendere i servizi accessibili e fruibili «tramite applicazione su dispositivi mobili», salvo impedimenti di natura tecnologica attestati dalla Società costituita dallo Stato per la gestione della piattaforma tecnologica per l'interconnessione e l'interoperabilità (art. 64, comma 1-*ter*, CAD). A carico delle pubbliche amministrazioni sussiste a questo proposito uno specifico onere di avviare progetti di trasformazione digitale entro il 28 febbraio 2021 (art. 64, comma 1-*quater*, CAD come modificato dal D.L. n. 76/2020).

Tornando all'esame della nozione di identità digitale al comma 2-*bis* dell'art. 64 – rimasto inalterato rispetto alle recenti modifiche – il CAD ha innanzitutto previsto l'istituzione del sistema che rende operativa l'identità digitale, e cioè del *sistema pubblico per la gestione dell'identità digitale di cittadini e imprese* (SPID), a cura dell'Agenzia per l'Italia digitale.

Le disposizioni attuative di questa norma sono contenute nel D.P.C.M. 24 ottobre 2014. Tra di esse, figura la definizione stessa della nozione di "identità digitale" che, come già esposto, è stata poi replicata all'interno del CAD nel 2016 con l'introduzione, all'art. 1, del comma 1, lett. f).

La disposizione del D.P.C.M., che dunque contiene la definizione originaria, prevede che l'identità digitale è «la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi *attributi identificativi*, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale» (art. 1, comma 1, lett. o), D.P.C.M.).

Per «attributi identificativi» si intendono il nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché il codice fiscale o la partita IVA e gli estremi del documento d'identità utilizzato ai fini dell'identificazione (art. 1, comma 1, lett. c) D.P.C.M.).

Si consideri, ulteriormente, che il D.P.C.M. prevede la possibilità per il cittadino di far sì che l'identità digitale fornisca ulteriori informazioni e qualità riguardanti se stesso, oltre agli attributi identificativi: si tratterebbe di «attributi secondari» (come il numero di telefono) oppure «attributi qualificati» (come il titolo professionale).

In attuazione dell'art. 64 CAD, l'art. 2 del D.P.C.M. prevede che lo SPID consenta agli utenti di avvalersi di «gestori dell'identità digitale» affinché i fornitori di servizi on line possano identificarli.

I «gestori dell'identità digitale» sono le persone giuridiche accreditate dall'AgID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, «assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica». Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di acces-

so, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti.

In questo senso, chi presenta un'istanza all'Amministrazione ai fini della fruizione di un servizio, secondo questo sistema, dovrebbe farsi rilasciare un'identità digitale di gestori, al fine di rendere possibile una identificazione sicura da parte della Pubblica Amministrazione (e non solo, come si dirà oltre).

I gestori assicurano la corrispondenza del soggetto con l'identità digitale che gli è attribuita, assicurando certezza nei rapporti tra cittadino e soggetti pubblici. Essendo indubbia la loro importanza all'interno del sistema SPID i gestori dell'identità digitale accreditati sono iscritti in un apposito elenco tenuto da AgID, consultabile anche in via telematica (art. 64, comma 2-*undecies*, CAD come modificato dal D.L. n. 76/2020).

In conclusione allo SPID partecipano:

a) i gestori dell'identità digitale;
b) i gestori degli attributi qualificati;
c) i fornitori di servizi (pubbliche amministrazioni o gestori di servizi pubblici);
d) l'AgID;
e) i cittadini utenti.

Si tratta quindi di un sistema "aperto" e "misto". Misto giacché in esso interagiscono sia soggetti privati che pubblici. I primi sono ad esempio chi usufruisce del sistema per identificarsi (utente), i gestori dell'identità digitale (c.d. *identity provider*), ma anche, come si vedrà, gli operatori privati che vogliano appoggiarsi al sistema – e alle garanzie che dà – per offrire i propri servizi (i fornitori, secondo la dizione del D.P.C.M.).

Il soggetto pubblico è, invece, l'Amministrazione che fornisce i propri servizi (fornitore di servizi) nel contesto dello SPID: infatti l'art. 64, comma 2-*octies*, CAD prevede che le pubbliche amministrazioni consentono mediante SPID l'accesso ai servizi in rete da essa erogati.

Un soggetto pubblico, che sembrerebbe esterno allo SPID giacché gioca il ruolo determinante di "garante" dell'intero sistema è l'AgID.

Con riferimento a quest'ultimo aspetto, l'evoluzione normativa fa emergere sempre di più l'importanza del ruolo dell'AgID che esercita una funzione di certificazione sui requisiti di chi opera nel sistema pubblico di identità digitale.

La natura "aperta" dello SPID è data, come si è accennato, dal fatto che ad ogni impresa privata che fornisce servizi è riconosciuta la possibilità di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti.

L'adesione di un'impresa al sistema SPID ha una rilevanza giuridica in quanto la esonera dall'obbligo generale di sorveglianza delle attività dei propri

siti ai sensi dell'art. 17 D.Lgs. 9 aprile 2003, n. 70 (art. 64, comma 2-*quinquies*, CAD). A sua volta, l'art. 17, avente ad oggetto «assenza dell'obbligo generale di sorveglianza», prevede che non sono soggetti ad un obbligo di sorveglianza sui contenuti delle informazioni che trasmettono o memorizzano via internet i soggetti che prestano servizi strumentali alla società dell'informazione.

Più precisamente: chi si limita a esercitare servizi di mera trasmissione su una rete di comunicazione, di informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione (art. 14 D.Lgs. cit.), chi trasmette, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, e le memorizza *temporaneamente* al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta (c.d. *catching* art. 15 D.Lgs. cit.), e, infine, chi memorizza informazioni fornite da un destinatario del servizio (c.d. *hosting*, art. 16 D.Lgs. cit.).

Dunque, chi si serve del sistema SPID è esonerato, come i soggetti sopra indicati, dall'obbligo di sorveglianza dei contenuti delle informazioni che trasmettono o memorizzano via internet.

Le figure centrali del sistema SPID, tra quelle sopra indicate, sono i soggetti che rilasciano e gestiscono le identità digitali.

Secondo il D.P.C.M. gestori dell'identità digitale sono le persone giuridiche accreditate allo SPID che, in qualità di «*gestori di servizio pubblico*», rendono disponibili e gestiscono gli «attributi» utilizzati dal medesimo utente al fine della sua identificazione informatica.

Si tratta dunque di soggetti privati che operano una funzione pubblicistica: a monte dell'esercizio di tale attività vi è il c.d. "accreditamento" da parte di AgID.

Tale procedimento è disciplinato dall'art. 29 CAD il quale stabilisce che i gestori di identità digitale – oltre che i soggetti che intendono avviare la prestazione di servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata – presentano all'AgID domanda di accreditamento, allegando alla stessa una relazione di valutazione della conformità rilasciata dall'Organismo di accreditamento riconosciuto ai sensi e in conformità del Regolamento 2008/765/CE e dell'art. 4, comma 2, della Legge 23 luglio 2009, n. 99. Il D.P.C.M. prescrive alcuni requisiti che devono essere posseduti dal soggetto che voglia ottenere l'accreditamento: tra gli altri, «avere forma giuridica di società di capitali e un capitale sociale non inferiore a cinque milioni di euro» (art. 10, comma 3, lett. a), D.P.C.M. 24 ottobre 2014).

A seguito dell'accoglimento della richiesta, l'AgID stipula apposita convenzione secondo lo schema definito nell'ambito dei regolamenti di cui all'art. 4 D.P.C.M. e dispone l'iscrizione del richiedente nel registro SPID, consultabile in via telematica (art. 10, comma 2, D.P.C.M. 24 ottobre 2014).

La verifica dell'identità del soggetto richiedente e la richiesta di adesione che stanno a monte del conferimento dell'identità digitale avvengono in modo che sia assicurata la certezza.

Dunque il sistema si regge sulla serietà degli *identity provider* nel verificare a monte l'identità del soggetto a cui attribuiscono l'identità digitale.

Le pubbliche amministrazioni che erogano in rete servizi qualificati, aderiscono allo SPID entro i ventiquattro mesi successivi all'accreditamento del primo gestore dell'identità digitale.

Le pubbliche amministrazioni, in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali.

Un cenno va svolto con riferimento alla "firma digitale".

Va osservato che l'istituto non è ricompreso nell'ambito della parte del CAD relativa alla carta di cittadinanza digitale.

Una tale scelta sembra riconducibile al fatto che, a parte la considerazione che la "firma digitale" possa essere uno strumento utile per il cittadino, essa costituisce istituto funzionale alla validità e valore probatorio del documento informatico.

La firma determina – con qualunque mezzo sia realizzata – l'autore del documento e l'assunzione di paternità (A. MASUCCI, 2004).

Per questa ragione, dunque, si rinvia per l'analisi di questo istituto e le diverse problematiche al capitolo relativo al Documento informatico (v. capitolo V, S. D'ANCONA).

5. Partecipazione democratica elettronica

All'art. 9 CAD il legislatore ha previsto che le pubbliche amministrazioni e i gestori di pubblici servizi favoriscano ogni forma di uso delle nuove tecnologie «per promuovere» una maggiore «partecipazione» dei cittadini, anche residenti all'estero, «al processo democratico» e «per facilitare l'esercizio dei diritti politici e civili» e «migliorare» la qualità dei propri atti, anche attraverso l'utilizzo, ove previsto e nell'ambito delle risorse disponibili a legislazione vigente, di «forme di consultazione preventiva per via telematica sugli schemi di atto da adottare» (art. 9 CAD).

La norma dà modo di riflettere su diversi possibili utilizzi delle nuove tecnologie nell'ambito dell'esercizio dei diritti civili.

Con il "voto elettronico" reso dai cittadini si perseguirebbero obiettivi più ambiziosi di quelli propri dell'automazione delle procedure elettorali. Il voto elettronico infatti consentirebbe al cittadino di manifestare la propria opinione rispetto alle più disparate proposte, siano esse di tipo politico od economi-

co, in qualsiasi momento, e da qualsiasi luogo alla sola condizione di disporre di un accesso alla Rete (P. COSTANZO, 2003).

Da una parte, quindi, le tecnologie digitali consentirebbero ai governanti la percezione delle opinioni dei governati orientando le decisioni pubbliche. Si pensi alla possibilità di avviare dibattiti tra i cittadini mediante internet, al fine di decidere alcuni aspetti di progetti pubblici, oppure al fine di decidere l'utilizzo di parte delle risorse finanziarie dell'Ente (la tecnologia potrebbe essere utile per avviare iniziative come il c.d. bilancio partecipativo).

Le applicazioni di rete, dall'altra parte, permetterebbero l'incontro di più opinioni ed un dibattito attivo tra la popolazione (democrazia *by discussion*) (P. COSTANZO, 2003).

Secondo una tesi condivisibile l'accesso ai mezzi informatici, in questo momento storico, diventa un «vero e proprio diritto sociale strumentale all'esercizio di altri diritti fondamentali» (opinione dell'Avvocatura dello Stato, nella causa per cui è stata emessa la sentenza Corte cost. 13-21 ottobre 2004, n. 307, punto 6.1, in www.cortecostituzionale.it).

Gli incentivi volti a promuovere la cultura informatica corrispondono a finalità di carattere generale il cui perseguimento fa capo alla Repubblica in tutte le sue articolazioni ai sensi dell'art. 9 della Costituzione (Corte Cost., cit., punto 3.1).

La pronuncia del Giudice delle Leggi traccia un importante "filo di congiunzione" tra l'art. 9 e la norma del CAD sulla alfabetizzazione informatica dei cittadini.

La disposizione prevede infatti che lo Stato e le altre Pubbliche amministrazioni promuovano iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete (art. 8 CAD).

Infine una breve riflessione non può mancare a proposito della tecnologia come strumento di promozione del diritto ad essere informati in merito alle decisioni pubbliche.

È evidente che il diritto ad essere informati è presupposto per il corretto esercizio del diritto di partecipazione cui fa riferimento l'art. 9 CAD appena esaminato.

Sia le norme del CAD in materia di dati pubblici sia le norme in materia di trasparenza (in particolare il D.Lgs. n. 33/2013) hanno imposto alle Pubbliche Amministrazioni l'obbligo di pubblicare sui siti web istituzionali molti "dati" che riguardano principalmente atti, provvedimenti e contratti adottati e stipulati dalle Amministrazioni stesse. I siti contengono anche i dati relativi ai pro-

cedimenti amministrativi con i soli limiti della tutela della riservatezza e della tutela di diritti di proprietà intellettuale (in argomento si veda il capitolo VIII, S. ROSSA).

A tutti questi dati i cittadini hanno accesso diretto proprio in virtù della connessione internet.

È evidente, dunque, che queste nuove disposizioni, a prescindere dalla loro potenzialità quali strumenti di controllo sull'operato delle Amministrazioni, abbiano delineato in capo al cittadino nuove possibilità di conoscenza.

Sulla questione della trasparenza e del diritto ad essere informati la dottrina ha osservato come non sia ancora chiaro se le nuove norme siano a presidio di un diritto fondamentale *pendant* del diritto a informare di cui all'art. 21 Cost., oppure se siano strumenti di garanzia della legalità contro la corruzione (D.-U. GALETTA, 2018).

Certo è che, proprio la tecnologia, la connessione ma anche la smaterializzazione dei dati dal supporto materiale cartaceo, è stata l'occasione per delineare tra cittadini e "dati" pubblici un rapporto inedito, ove i cittadini, parte attiva, possono apprendere l'informazione pubblica in maniera diretta ed elaborarla secondo la propria capacità.

Le tecnologie, in altri termini, giocano un ruolo determinante contribuendo nei processi dell'informazione (dalla sua generazione, alla elaborazione e diffusione) e di democrazia.

Si è a questo proposito osservato che i dati pubblici detenuti dalla Pubbliche Amministrazioni, costituiscono, nel contesto della società dell'informazione, una categoria specifica di "beni" (G. CARULLO, 2017).

D'altra parte, la dottrina civilistica ha affermato che per beni non si intendono solamente le "cose" in senso materiale, ma anche beni di diversa natura; quelli che pur avendo un'esistenza puramente ideale, hanno utilità (ad es. servizi, arg. *ex* artt. 2082, 2195 n.1) o valore (ad es. opere dell'ingegno, artt. 2575 ss.) (L. BIGLIAZZI-GERI, U. BRECCIA, F. D. BUSNELLI, 1996).

Anche i dati pubblici rientrano dunque nella nozione di "bene".

Con riferimento al regime proprietario, sembra che in considerazione delle norme in materia di trasparenza, i dati pubblici non possano essere considerati di proprietà delle Pubbliche Amministrazioni che li detengono.

Autorevole dottrina ha acutamente osservato che, anzi, nel custodire informazioni le pubbliche amministrazioni agiscono nell'interesse dei terzi, ossia i cittadini, in quali rappresentano i veri titolari del "bene" informazione (D.-U. GALETTA, 2018).

Ed allora, i dati pubblici trovano collocazione in un ambito ampio di beni "comuni" (sulla nozione, U. MATTEI, 2011) o "collettivi". D'altra parte, «l'appartenenza collettiva si estrinseca nella titolarità in capo ai singoli membri del-

la collettività (i *cives*) di diritti propri di godimento diretto del bene e di tutela dello stesso: i *cives* possono direttamente esercitare le azioni a tutela della proprietà e del possesso dei beni collettivi» (V. CERULLI IRELLI, 1997).

6. Diritto di effettuare i pagamenti con modalità informatiche

Tra i diritti di cittadinanza digitale enucleati dal CAD vi è anche quello, stabilito dall'art. 5, di effettuare i pagamenti alle Pubbliche amministrazioni e ai gestori dei servizi pubblici con «modalità informatiche». Il citato art. 5 dispone, infatti, a chiare lettere che detti ultimi soggetti «*sono obbligati ad accettare* (…) i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico, ivi inclusi, per i micro-pagamenti, quelli basati sull'uso del credito telefonico». Il tutto coerentemente con quanto previsto dalla Legge delega n. 124/2015 (c.d. Legge Madia), che invitava il legislatore delegato, chiamato a riformare il CAD, da un lato, a introdurre disposizioni volte a garantire «la piena disponibilità dei sistemi di pagamento elettronico» (art.1, comma 1, lett. c) Legge n. 124/2015), e dall'altro, a prevedere «che i pagamenti digitali ed elettronici effettuati con qualsiasi modalità di pagamento (…) costituiscano il mezzo principale per i pagamenti dovuti nei confronti della pubblica amministrazione e degli esercenti servizi di pubblica utilità» (art.1, comma 1, lett. d) Legge n. 124/2015).

In seguito alla riforma del 2018, e all'inserimento nell'art. 5 del comma 2-*ter*, occorre segnalare, tra i pagamenti elettronici che possono essere effettuati, anche quelli, ove spontanei, relativi ai tributi dei comuni e degli altri enti locali.

Chiarita la sussistenza di tale diritto, e di converso dell'obbligo in capo all'amministrazione e ai gestori di servizi pubblici di accettare dette modalità di pagamento, è necessario ora sottolineare che l'art. 5 disciplina nel dettaglio i sistemi di pagamento di cui può avvalersi chi intenda esercitare detto diritto.

La modalità principale consiste nell'utilizzo della «piattaforma elettronica» di cui al comma 2 dell'art. 5. Il quale prevede che la Presidenza del Consiglio dei ministri «mette a disposizione (…) una piattaforma tecnologica per l'interconnessione e l'interoperatività tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati».

Tale piattaforma, che prende il nome "PagoPA", consente ai «prestatori di servizi di pagamento abilitati» (si tratta delle banche, delle poste, ecc.) di eseguire, tramite essa e per conto di chi deve effettuare un versamento, i pagamenti in favore delle pubbliche amministrazioni e dei gestori dei servizi pub-

blici (comma 2-*quater*, art. 5, CAD) e ha, quale valore aggiunto, quello di essere strutturata in modo tale da garantire talune funzioni aggiuntive connesse ai pagamenti.

La piattaforma, ad esempio, mette a disposizione del Ministero dell'economia e delle finanze-Dipartimento Ragioneria generale dello Stato «le informazioni sui pagamenti» (comma 2-*quinques*, art. 5, CAD) e «può essere utilizzata per facilitare e automatizzare (…) i processi di certificazione fiscale tra soggetti privati» (comma 2-*sexies*, art. 5, CAD).

Bibliografia

BAVETTA G., *Identità* (diritto alla), in *Enc. dir.*, vol. XIX, Milano, 1970, p. 953.

BIGLIAZZI-GERI L., BRECCIA U., BUSNELLI F.D., NATOLI U., *Diritto Civile*, vol. II *Diritti Reali*, Utet, Torino, 1996, p. 3.

CARDARELLI F., *Amministrazione digitale, trasparenza e principio di legalità*, in *Diritto dell'informazione e dell'informatica*, II, 2015, p. 227 ss., in particolare par. 8.

CAMILLETTI F., *La responsabilità della pubblica amministrazione per violazione del diritto all'uso delle tecnologie*, in AA.VV., a cura di E. De Marco, *Accesso alla rete e disuguaglianza digitale*, Milano, 2008, p. 85 ss.

CARLONI E., *La riforma del codice dell'amministrazione digitale*, in *Giorn. dir. amm.*, 2011, pp. 469 ss.

CAROTTI B., *Il correttivo al codice dell'amministrazione digitale: una meta-riforma*, in *Gior. dir. amm.*, 2018, p. 131 ss.

CARULLO G., *Elezione del domicilio digitale per la ricezione di notifiche di atti giudiziari: dubbi in relazione alla diversa disciplina dettata per i privati e per le pubbliche amministrazioni*, in *Dir. proc. amm.*, 2019, p. 228 ss.

CARULLO G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2017.

CARULLO G., *Posta elettronica certificata e domicilio digitale: futuro e incertezze in una prospettiva europea*, in *Riv. it. dir. pubbl. com.*, 2016, pp. 51 ss.

CERULLI IRELLI V., *Corso di diritto amministrativo*, Torino, 1997, p. 668.

CERULLI IRELLI V., *Proprietà pubblica e diritti collettivi*, Padova, 1983, p. 16.

COSTANZO P., *La democrazia elettronica*, in *Dir. informatica*, 3, 3, p. 465 ss.

CREPALDI G., *Efficacia temporale del provvedimento amministrativo e le sue vicende*, in *Foro amm. C.D.S.*, 2013, p. 449 ss.

D'ORLANDO E., *Profili costituzionali dell'amministrazione digitale*, in *Diritto dell'informazione e dell'informatica*, 2011, 1, p. 216.

DE CUPIS A., *Diritto all'identità personale, diritto ai segni distintivi personali, diritto morale d'autore*, Milano, 1961.

DE GRAZIA D., *Informatizzazione e semplificazione dell'attività amministrativa nel nuovo codice dell'amministrazione digitale*, in *Dir. pubbl.*, 2011, 2, p. 611 ss.

FALCO G., *Identità personale* (Voce), in *Nuovo dig. it.*, VI, Torino, 1938, p. 649.

FINOCCHIARO G., *L'equilibrio titolare/users nel diritto d'autore dell'Unione Europea*, in *Diritto dell'Informazione e dell'Informatica (Il)*, 2016, 3, p. 499.

FINOCCHIARO G., *Identità personale* (diritto alla), in *Dig. disc. priv.*, Agg., Torino, 2010, p. 721 ss.

FLICK C., AMBRIOLA V., *La cittadinanza amministrativa telematica fra previsioni normative ed effettività*, in *Dir. inform.*, 2006, 6, 825 ss.

FROSINI T.E., *Liberté, egalité, internet*, Napoli, 2019.

GALETTA D.-U., *Accesso (civico) generalizzato ed esigenze di tutela dei dati personali ad un anno dall'entrata in vigore del Decreto FOIA: la trasparenza de "le vite degli altri"*, in Federalismi.it, maggio 2018.

MANTELERO A., *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Diritto dell'informazione e dell'Informatica*, 2012, p. 136.

MARINELLI F., *Beni comuni* (Voce), in *Enc. dir.*, Annali, VII, Roma, 2014, p. 160.

MASUCCI A., *Il documento informatico*, in *Riv. dir. civ.*, 2004, 5, p. 10749 ss.

MATTEI U., *Beni comuni. Un manifesto*, Bari, 2011.

PANATO M., *"Carta di internet" e diritto della comunicazione: il riconoscimento dell'accesso alla rete internet quale diritto fondamentale della persona e rapporto con gli enti pubblici*, in *Diritto & Diritti – Rivista giuridica elettronica*, pubblicato il 4 settembre 2015, in http://www.diritto.it/docs/37283-carta-di-internet-e-diritto-della-comunicazione-il-riconoscimento-dell-accesso-alla-rete-internetquale-diritto-fondamentale-della-personae-rapporto-con-gli-enti-pubblici.

PIRAS P., *Il tortuoso cammino verso un'amministrazione nativa digitale*, in *Dir. inform. e inf.*, 2020, p. 43 ss.

PROVENZANO P., *Decreti Madia e nuova disciplina del c.d. "domicilio digitale": quali prospettive?*, in Federalismi.it, 2016.

RESTA G., *L'identità digitale e l'identità personale*, in *Dir. inform. e inf.*, 2007, p. 511 ss.

RODOTÀ S., *Il diritto di avere diritti*, Bari, 2012, p. 384.

SARZANA DI SANT'IPPOLITO F., *Il digital divide e le telecomunicazioni: potenziali soluzioni tecnico regolamentari*, in A.A. MARTINO (a cura di), *Aspetti giuridici di Internet. Quaderni dell'Internet italiano*, 2007, p. 67 ss.

SIGISMONDI I., *Telematica* (Voce), in *Enc. giur.*, Roma, Postilla di aggiornamento, 2008, p. 2.

VITERBO A., CODIGNOLA A., *L'informazione e l'informatica nella società della conoscenza*, in *Dir. informatica*, 2002, 2, p. 23.

VIII.

TRASPARENZA E ACCESSO ALL'EPOCA DELL'AMMINISTRAZIONE DIGITALE

Stefano Rossa

SOMMARIO: 1. Introduzione. La trasparenza: coordinate sistematiche di un principio cardine della Pubblica Amministrazione. – 1.1. La c.d. strategia di *Open Government* e il ruolo centrale della trasparenza. – 2. La trasparenza "debole" della fase di "protodigitalizzazione" dell'amministrazione. – 2.1. L'accesso alla documentazione amministrativa nella Legge n. 241/1990. – 2.2. Conseguenze ed effetti della trasparenza "debole". – 3. La trasparenza "difensiva" della prima fase della digitalizzazione dell'amministrazione. – 3.1. L'accesso alle informazioni come strumento per realizzare maggiore efficienza dell'attività amministrativa e combattere i fenomeni corruttivi. – 3.2. L'accesso civico come strumento di controllo sociale. – 3.3. Conseguenze ed effetti della trasparenza c.d. "difensiva". – 4. La trasparenza "ragionata" dell'attuale fase della digitalizzazione dell'amministrazione. – 4.1. L'accesso civico generalizzato. – 4.2. Conseguenze ed effetti della trasparenza "ragionata" e il collegamento con il riutilizzo dei documenti contenenti dati pubblici della Pubblica Amministrazione (cenni). – 5. Il contributo della digitalizzazione dell'amministrazione per una concezione più ampia del principio di trasparenza.

1. Introduzione. La trasparenza: coordinate sistematiche di un principio cardine della Pubblica Amministrazione

L'aggettivo "trasparente", secondo il vocabolario Zingarelli, si riferisce innanzitutto alla capacità di un corpo di lasciar passare la luce (cfr. M. DOGLIOTTI, L. ROSIELLO, 1996, 1867): tale lemma concerne, dunque, qualità estrinseche e concrete. Il collegamento concettuale di tale aggettivo all'azione amministrativa, in realtà solo apparentemente astratta, si deve a una metafora coniata da Filippo Turati all'inizio del XX secolo.

Turati, all'epoca Deputato del Regno d'Italia, affermò con eloquenza come la Pubblica Amministrazione dovesse essere intesa quale una casa di vetro

(cfr. ATTI DEL PARLAMENTO ITALIANO – CAMERA DEI DEPUTATI, 1908, 22962). In tal modo, ben quarant'anni prima dell'entrata in vigore della Costituzione, si iniziò a ripensare la Pubblica Amministrazione, immaginandola come una casa per il cittadino, con le pareti di vetro e che permettesse dunque a chi è fuori di vedere cosa accade nell'edificio e a chi è dentro di vedere cosa accade fuori.

Quella turatiana è una metafora che avrà molta fortuna negli anni a venire, sebbene non sarà esente da critiche (cfr. A. ROMANO TASSONE, 1995, 342). Critiche che chi scrive ritiene di condividere, per le ragioni che saranno espresse in seguito, in quanto tale espressione non appare più utile a comprendere appieno il concetto di trasparenza così come essa è da intendersi oggi (*infra* par. 5).

Nonostante il dibattito sulla trasparenza fosse sorto, dunque, all'inizio del secolo scorso, il testo della Costituzione che entrato in vigore nel 1948 non contiene alcuna norma esplicita in riferimento al principio di trasparenza – contrariamente a quelli di imparzialità e buon andamento enunciati all'art. 97 Cost.

Come sottolineato dalla dottrina, la trasparenza amministrativa rappresenta «un modo di essere dell'amministrazione, un obiettivo od un parametro cui commisurare lo svolgimento dell'azione delle figure soggettive pubbliche» (R. VILLATA, 1987, 528). La trasparenza costituisce un vero e proprio principio democratico, risultando uno «strumento indispensabile a realizzare un effettivo e diretto rapporto tra governanti e governati» (così M.A. SANDULLI, 2000, 1). Non stupisce allora il fatto per cui, pur in assenza di una esplicita disposizione costituzionale, siano numerose le forme tramite cui tale principio è stato posto in essere, primo fa tutti il diritto di accesso.

Il legame fra trasparenza e accesso, emerso inizialmente proprio nei lavori dell'Assemblea Costituente, in particolare in quelli della "Commissione per gli studi attinenti alla riorganizzazione dello Stato" (c.d. "Commissione Forti" – cfr. MINISTERO PER LA COSTITUENTE, 1956, 156 ss.), si è concretizzato sul piano generale all'inizio degli anni '90, grazie alla promulgazione della Legge n. 241/1990 – rubricata, non a caso, "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi".

Il binomio trasparenza-accesso è così sorto in un contesto in cui risultavano molto più che avanguardistiche le timide applicazioni tecnologiche all'azione amministrativa, come testimoniato di riflesso dalla pioneristica monografia *L'atto amministrativo informatico*, scritta da Masucci all'inizio degli anni '90, relativa alle prime teorizzazioni sull'apporto dell'informatica alla Pubblica Amministrazione al (cfr. A. MASUCCI, 1993).

L'accesso, inteso come principale mezzo tramite cui concretizzare il prin-

cipio di trasparenza, nasce, dunque, in un contesto antecedente al processo di digitalizzazione dell'amministrazione. Tuttavia, proprio l'essenza, il cuore, dell'accesso, consistente nelle modalità pratiche che lo rendono azionabile nel mondo reale, è risultata inevitabilmente collegata e influenzata dal processo di digitalizzazione dell'amministrazione. Al crescere della diffusione delle ICT (*Information and Communication Technology*) nel settore pubblico, il legislatore si è trovato costretto ad affinare l'istituto dell'accesso, introducendone negli anni nuove tipologie tramite le quali poter garantire la trasparenza nel modo più adatto possibile ai cambiamenti delle condizioni dell'amministrazione. Di conseguenza, come vedremo, in qualche modo la trasparenza ha subito un processo di evoluzione che si è sviluppato in parallelo rispetto al processo di progressiva digitalizzazione della Pubblica Amministrazione.

1.1. La c.d. strategia di *Open Government* e il ruolo centrale della trasparenza

L'evoluzione della trasparenza in Italia, in particolare negli ultimi anni, è stata condizionata dall'elaborazione della c.d. strategia di *Open Government* a livello internazionale. In estrema sintesi, tale strategia si focalizza intorno all'obiettivo di realizzare un modello di amministrazione finalizzato a porre in essere una relazione più salda e stretta fra il settore pubblico, Pubblica Amministrazione *in primis*, e gli altri attori privati, in particolare i cittadini. Una relazione non più verticistica – che parte dall'amministrazione per poi discendere verso i cittadini – ma di natura (quasi) paritaria, nella quale il pubblico e il privato si trovino sul medesimo livello.

"Apertura" e "avvicinamento" sono infatti i due cardini sui quali ruota la strategia di *Open Government*, concretamente perseguita tramite l'attuazione dei principi di trasparenza, partecipazione e collaborazione (su tutti cfr. E. CARLONI, 2014; F. COSTANTINO, 2015; D.-U. GALETTA, 2019(a)) che è resa possibile proprio grazie all'impiego delle ICT.

Quanto alle origini della strategia di *Open Government*, questa è stata teorizzata per la prima volta sul piano politico-programmatico durante il suo primo mandato da Presidente degli Stati Uniti d'America da *Barak Obama*, che adottò il ben noto *Memorandum Transparency and Open Government*. Da questo documento emergeva l'intento di rendere l'amministrazione statunitense maggiormente aperta nei confronti dei cittadini (cfr. B. OBAMA, 2009). A seguito della chiara impostazione politica che Obama voleva imprimere con i propri atti, si verificarono due tipi di reazioni. Da un lato, le organizzazioni internazionali (già esistenti) iniziarono a interessarsi all'*Open Goverment* pub-

blicando rapporti specifici in punto di effettiva e realizzabilità: un esempio è costituito dal OECD, che nel 2016 pubblicò il report *Open Government. The Global Context and the Way Forward* (cfr. OECD, 2016 e per un commento D.-U. GALETTA, 2019(a), 666 ss.). Dall'altro lato, sorsero iniziative multilaterali di natura sovranazionale finalizzate a perseguire direttamente la strategia di *Open Goverment*, quali l'*Open Government Partnership* (cfr. OGP, 2011).

Quanto alle ricadute concrete di questa strategia, in Italia vi sono riferimenti espressi all'*Open Government* in atti giuridici cruciali adottati nel contesto delle politiche di digitalizzazione dell'Amministrazione Pubblica: quale ad es. il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021 (cfr. AGID, 2019, punto 1.3). Mentre riferimenti impliciti sono contenuti nello stesso CAD (cfr. art. 17, comma 1, D.Lgs. n. 82/2005). Sicché, il nesso fra trasparenza e digitalizzazione appare quanto mai evidente e rilevante, anche in concreto.

2. La trasparenza "debole" della fase di "protodigitalizzazione" dell'amministrazione

La Legge n. 241/1990 è nota principalmente per essere la normativa che ha introdotto nel nostro ordinamento nazionale la disciplina sul procedimento amministrativo (in argomento *ex multis* A. PUBUSA, 1993; A. SANDULLI, 2003; A. ROMANO, 2016; M.A. SANDULLI, 2017). Punto di sintesi di un processo di teorizzazione iniziato durante i lavori dell'Assemblea Costituente, nella già citata "Commissione Forti" (cfr. MINISTERO PER LA COSTITUENTE, 1956) e protrattosi fino alla fine degli anni '80, in particolare nell'elaborazione della "Commissione Nigro" del 1984 (cfr. M. NIGRO, 1989; in relazione anche G. MORBIDELLI, 2005, 550 ss.), la Legge n. 241/1990 ha introdotto, tuttavia, anche un diritto di accesso alla documentazione amministrativa.

Si tratta – è bene specificarlo subito – di un diritto di accesso *generale*, in quanto azionabile da ogni cittadino, alle condizioni stabilite dalla legge medesima e contrapposto rispetto alle poche e precedenti ipotesi di accesso *particolare* riservato a specifici soggetti e ambiti: si pensi all'accesso in materia urbanistica (cfr. art. 10, Legge n. 765/1967), in materia di autonomie locali (cfr. artt. 24, comma 1 e 25, comma 1, Legge n. 816/1985 e poi art. 7, comma 3 e 4, Legge n. 142/1990), o in materia ambientale (cfr. art. 14, comma 3, Legge n. 349/1985).

La portata innovativa della Legge n. 241/1990 non si riflette peraltro solo nell'allargamento di prospettiva compiuto in relazione all'accesso (da particolare a generale), bensì, anche e soprattutto, nella *ratio* stessa dell'istituto che,

per quanto qui direttamente ci concerne, nella sua concezione originaria aveva l'obiettivo proprio di favorire la trasparenza.

L'art. 22 della Legge n. 241/1990, sia nel testo attualmente in vigore sia in quello di originaria promulgazione, afferma come l'istituto dell'accesso documentale sia finalizzato ad assicurare (anche) il principio di trasparenza. Infatti l'attuale comma 2 dell'art. 22 precisa come l'accesso documentale abbia «rilevanti finalità di pubblico interesse» in quanto costituente un principio generale dell'attività amministrativa, mirato a realizzare cruciali principi, fra cui quello di trasparenza, appunto. Sicché, appare evidente come l'accesso documentale sia stato introdotto dal legislatore quale strumento per realizzare la trasparenza intesa quale fine pubblico (cfr. G. CLEMENTE DI SAN LUCA, 2006, 129 ss.).

Tuttavia, tale obiettivo, nei fatti, non è stato raggiunto. Infatti, sul piano concreto il diritto di accesso si è tradotto in un istituto talmente "diverso" da quello prefigurato nelle intenzioni del legislatore da rendere il suo legame con la trasparenza labile, o meglio, come affermato in dottrina, «debole» (cfr. S. FOÀ, 2017, 75).

Ma ecco che già qui emerge il legame chiaro (per ora in senso negativo) con la digitalizzazione: il contesto tecnologico nel quale è stata approvata la Legge n. 241/1990 rappresenta infatti, a parere di chi scrive, un fattore chiave che non ha contribuito a fortificare il summenzionato legame e ha coinciso con il contesto tecnologico nel quale è stata approvata la Legge n. 241/1990. All'epoca ci si trovava, infatti, in contesto protodigitalizzazione", nel quale solo da pochi anni si era iniziato a parlare di "teleamministrazione" (cfr. G. DUNI, 1993), di "informatica pubblica" (cfr. P. COSTANZO, 1997) e di "informatica amministrativa" (cfr. G. SARTOR, 2014, 64). Si trattava, cioè, dei primi deboli tentativi di applicazione alla Pubblica Amministrazione dell'informatica giuridica, nata dalle teorie di Frosini e Losano negli anni '60 (cfr. V. FROSINI, 1968; M.G. LOSANO, 1969); e tale applicazione era stata resa possibile dalla nascita del Web, da un lato, e dalle prime tecniche di compressione e registrazione di dati su supporti rigidi, di "dall'altro.

Questo contesto di "protodigitalizzazione" è identificabile chiaramente solo a fronte di un giudizio emesso ovviamente a posteriori e in base ad un paragone con quello odierno. Appare intuitivo, infatti, che, per l'epoca, la tecnologia di quegli anni fosse la più avanzata in assoluto. Si pensi che è nei primi anni '90 che fanno il proprio ingresso sul mercato i primi modelli di telefoni cellulari (ben diversi dagli attuali *smartphones)* e i CD-ROM. Il fatto, però, che quella tecnologia permettesse azioni esponenzialmente limitate rispetto a quelle attuali, unito a come è stato delineato nel concreto il diritto di accesso documentale, ha comportato, appunto, la realizzazione di una trasparenza che, a posteriori, è possibile definire come "debole".

2.1. L'accesso alla documentazione amministrativa nella Legge n. 241/1990

La legge generale sul procedimento amministrativo disciplina il diritto di accesso ai documenti amministrativi al Capo V (artt. 22-28, Legge n. 241/1990).

Come accennato nel paragrafo precedente, la legge generale sul procedimento ha introdotto un diritto di accesso *generale* (si badi bene: non *generalizzato*). *Generale* in quanto tale pretesa risulta essere esercitabile da ogni soggetto (e non più, per esempio, soltanto da specifici soggetti quali i Consiglieri degli enti locali *ex* art. 24, comma 1, Legge n. 816/1985), in base alle condizioni stabilite dalla legge.

Questa disciplina, infatti, nella versione attualmente in vigore stabilisce che tutti «i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso» (art. 22, comma 1, lett. b), Legge n. 241/1990) possano esercitare tale pretesa. Pretesa che, sebbene dal *nomen iuris* emerga quale diritto soggettivo, per la giurisprudenza è da ricondurre alla categoria dell'interesse legittimo (cfr. Cons. Stato, Ad. Plen., n. 16 del 1999, in www.giustizia-amministrativa.it) – tesi accolta anche dalla dottrina (cfr. *ex multis* F. FRACCHIA, 2003).

In ogni caso, l'accesso consta di due momenti coordinati e logicamente correlati: da un lato, quello della presa visione di documenti amministrativi, dall'altro, quello dell'estrazione della relativa copia (cfr. art. 22, comma 1, lett. a), Legge n. 241/1990). La presa visione è funzionale alla conoscenza del contenuto del documento amministrativo, mentre l'estrazione di copia è mirata a consentire una eventuale difesa (innanzi all'amministrazione o in giudizio).

Da quanto fin qui ricostruito, emerge con chiarezza come l'oggetto dell'accesso ex Legge n. 241/1990 sia il documento amministrativo, intendendosi con esso «ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale» (art. 22, comma 1, lett. d), Legge n. 241/1990). Da tale definizione si evince come sia possibile prendere visione ed estrarre copia di un atto che sia già formato sul piano estrinseco (cfr. G. CLEMENTE DI SAN LUCA, 2006, 26, il quale fa riferimento all'«esserci dell'atto»), non risultando invece possibile l'accesso a meri dati e informazioni (sul punto v. *infra*).

Come sottolineato poc'anzi, la legge sul procedimento pone alcune limita-

zioni all'accesso documentale. Innanzitutto, pur possedendo l'accesso «rilevanti finalità di pubblico interesse» (art. 22, comma 2, Legge n. 241/1990), il legislatore ne fa oggetto di bilanciamento con altre situazioni giuridiche meritevoli di tutela, delineando in tal modo precise ipotesi sottratte all'accesso (es. Segreto di Stato – cfr. art. 24, Legge n. 241/1990). In secondo luogo, risulta necessaria la motivazione della richiesta di accesso (cfr. art. 25, comma 2, Legge n. 241/1990), la quale deve necessariamente riferirsi a una situazione personale del proponente, in considerazione dell'inammissibilità di «istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni» (art. 24, comma 3, Legge n. 241/1990).

Quanto ricostruito è l'impianto normativo base delineato dalla Legge n. 241/1990 in riferimento all'accesso documentale. Impianto che, nei fatti, ha comportato un ridimensionamento evidente della concretizzazione della trasparenza che esso avrebbe dovuto realizzare almeno nelle intenzioni del legislatore.

2.2. Conseguenze ed effetti della trasparenza "debole"

Quanto scritto poc'anzi conduce ad alcune riflessioni. La prima considerazione si riferisce all'impianto delineato dalla Legge n. 241/1990, mentre la seconda concerne il contesto tecnologico.

La prima riflessione discende dalla lettura coordinata dei due principali "paletti" normativi che il legislatore della legge sul procedimento ha imposto all'esercizio dell'accesso documentale, vale a dire, da un lato, l'obbligo di motivazione e, dall'altro, l'inammissibilità di istanze di accesso preordinate al controllo generalizzato sull'operato dell'amministrazione.

Da questi due elementi emerge come l'accesso documentale, in realtà, risulti essere uno strumento attraverso il quale il singolo può tutelare le situazioni giuridiche individuali nei confronti della Pubblica Amministrazione (cfr. S. COGNETTI, 2000, 44 ss. e D.-U. GALETTA, 2014(a)). Tesi che pare essere rafforzata sia dalla natura esoprocedimentale di tale accesso documentale – il cittadino si trova a doversi difendere dall'azione dell'amministrazione in quanto la richiesta di accesso può essere presentata soltanto alla conclusione del procedimento e, dunque, in un momento successivo all'azione amministrativa – sia dalla previsione di un rito *ad hoc* in materia di accesso ai documenti amministrativi (cfr. art. 116 D.Lgs. n. 104/2010).

L'esigenza di tutela individuale, dunque, si trova a prevalere sull'esigenza pubblica di concretizzazione del principio di trasparenza.

Sebbene, dunque, il primo intento del legislatore fosse la realizzazione sul

piano fattuale della trasparenza, nel diritto di accesso *ex* Legge n. 241/1990 tale principio si trova in secondo piano rispetto alla tutela di situazioni giuridiche soggettive.

Come già sottolineato, è per tale ragione che la dottrina ha qualificato come «debole» la relazione intercorrente fra l'accesso documentale, il mezzo, e il principio di trasparenza, il fine (cfr. S. FOÀ, 2017, 75).

Questa debolezza, tuttavia, discende altresì da un ulteriore aspetto, oggetto della seconda riflessione.

Pur ragionando a posteriori, non si può infatti non tener conto del contesto tecnologico esistente al momento dell'approvazione della Legge n. 241/1990. Contesto che, come già si è detto, ben può essere definito come di "protodigitalizzazione" della Pubblica Amministrazione, in conseguenza della presenza delle primissime sperimentazioni tecnologiche in relazione all'azione e all'organizzazione pubblica. Basti pensare che *Google* venne fondata sette anni dopo la promulgazione della legge italiana sul procedimento amministrativo, *Facebook* quattordici, mentre *YouTube* addirittura quindici. Risulta allora difficile pensare a che cosa dovesse essere la tecnologia digitale prima dell'uscita dei servizi di queste società; ed era dunque, evidentemente, quello il grado di digitalizzazione di riferimento, all'epoca.

La centralità che la legge sul procedimento riserva al documento amministrativo in relazione all'accesso deriva, dunque, sia dalle esigenze pratiche di tutela del singolo, come sopra evidenziato, sia, soprattutto, dal livello di digitalizzazione di quel periodo: era difficilmente immaginabile poter consentire la visione e l'estrazione di copia di dati e/o informazioni "esterne" al documento e prescindendo da esso, mentre era naturale considerare soltanto il documento in quanto supporto materiale contenente dati o informazioni (cfr. G. CARULLO, 2017, 33, il quale contrappone alla staticità dei documenti la dinamicità del dati). E proprio tale (basso) grado di innovazione tecnologica ha rappresentato una inevitabile zavorra, che ha contribuito a rallentare sul piano fattuale norme già di per sé di ardua attuazione, stante la portata innovativa della legge sul procedimento, definita dalla dottrina una vera e propria «rivoluzione copernicana» per l'azione e l'organizzazione della Pubblica Amministrazione (C.E. GALLO, S. FOÀ, 2000, 4).

Con quel grado di "protodigitalizzazione" dell'amministrazione sarebbe stato difficile ipotizzare una relazione meno debole fra l'accesso ai documenti delle Pubbliche Amministrazioni e l'attuazione della trasparenza posta in essere con la Legge n. 241/1990.

Tuttavia, pur a fonte dell'accelerazione dello sviluppo delle ICT, la modifica legislativa apportata alla legge sul procedimento in particolare dalla Legge n. 15/2005, e recentemente dal D.L. n. 76/2020 (D.L. 16 luglio 2020, n. 76,

Misure urgenti per la semplificazione e l'innovazione digitale, convertito con la Legge 11 settembre 2020, n. 120), non ha portato ad una modifica dell'impianto dell'accesso: che è rimasto un accesso documentale, risultando pertanto invariato anche il suo rapporto con il principio di trasparenza.

La ragione di ciò si ricollega alla scelta del legislatore di raggiungere l'obiettivo della trasparenza tramite una strada diversa dall'accesso documentale. Una via, come si vedrà nel paragrafo successivo, resa possibile, ancora una volta, dal mutato contesto tecnologico della seconda metà del primo decennio del Duemila.

3. La trasparenza "difensiva" della prima fase della digitalizzazione dell'amministrazione

Pochi giorni dopo la promulgazione della Legge n. 15/2005, di riforma della legge sul procedimento amministrativo, venne approvato il D.Lgs. n. 82/2005, il c.d. Codice dell'amministrazione digitale (CAD) – recentissimamente oggetto di modifiche apportate dalla Legge n. 120/2020.

In tale *corpus* vi è una norma, l'art. 54 CAD, che nella sua prima versione stabiliva l'obbligo, in capo alle amministrazioni, di pubblicare sui propri siti web istituzionali alcune categorie di dati relativi all'organizzazione e all'attività amministrativa. Questa norma imponeva, altresì, che tali dati dovessero essere accessibili agli internauti gratuitamente e senza la necessità di autenticazione sui siti delle amministrazioni. I dati presenti sui siti istituzionali, in ogni caso, dovevano essere conformi a quelli "contenuti" nei documenti cartacei cui si faceva riferimento (si badi che l'art. 54, comma 4, CAD versione originaria si riferiva, proprio su quest'ultimo punto, non tanto ai dati bensì alle informazioni, confondendo due concetti legati ma distinti).

Nonostante la summenzionata norma del D.Lgs. n. 82/2005 avesse chiaramente una natura programmatica, non imponendo sanzione alcuna rispetto alla mancata pubblicazione dei dati sui siti web, tale prescrizione si tradusse in un cambio di approccio al tema della concretizzazione della trasparenza.

In tal modo, il legislatore, percorrendo «una via tutta italiana alla trasparenza amministrativa» (M. SAVINO, 2016, 594), ha deciso di intraprendere una strada alternativa all'accesso alla documentazione amministrativa per attuare il principio di trasparenza. Ha scelto infatti di concretizzare tale principio tramite la previsione di obblighi di pubblicazione sui siti web istituzionali delle amministrazioni.

Questa scelta legislativa, che sposta l'accento dal diritto di accesso verso il

principio di pubblicità – considerato «l'altra faccia della trasparenza» (F. MERLONI, 2008, 3) sebbene per una parte della dottrina sia «un mero stato di fatto dell'atto dell'organizzazione o del procedimento» (F. MANGANARO, 2009, 4) – è stata confermata anche da altre norme di dettaglio di poco successive all'entrata in vigore del CAD (cfr. art. 44, comma 3, Legge n. 244/2007; art. 61, comma 4, D.L. n. 112/2008, conv. Legge n. 133/2008; art. 21, comma 1, Legge n. 69/2009), ed ha rappresentato l'*incipit* della trasparenza c.d. "difensiva".

La centralità degli obblighi di pubblicazione verrà, infatti presa a modello da tre importanti riforme: la c.d. Riforma Brunetta (D.Lgs. n. 150/2009), la legge Severino (Legge n. 190/2012) e il c.d. Decreto trasparenza (D.Lgs. n. 33/2013), che saranno analizzate successivamente (cfr. parr. 3.1. e 3.2.).

La pubblicazione sui siti istituzionali di specifici dati dell'amministrazione, alla quale di riflesso si innesta la consultazione e lo "scaricamento" in tempo reale degli stessi da parte degli utenti del web, è stata resa concretamente possibile dall'aumento della diffusione delle ICT fra i cittadini e, in particolare, nel settore pubblico. Pur qualificando, quella in questione, come la prima fase del processo di digitalizzazione dell'amministrazione, è indubbio come la realizzazione degli obblighi di trasparenza sia stata consentita, sul piano concreto, dalla maggior diffusione delle tecnologie informatiche (cfr. in tal senso M. SAVINO, 2013, 797).

Senza voler anticipare quanto trattato successivamente, nelle tre summenzionate discipline il principio di trasparenza viene attuato tramite il perseguimento del controllo sociale sull'operato della Pubblica Amministrazione, a sua volta reso possibile tramite lo strumento degli obblighi di pubblicazione.

In questa prospettiva appare evidente come l'idea di fondo del legislatore fosse che la trasparenza doveva essere raggiunta tramite un'azione "pungolatrice" posta in essere dalla cittadinanza: la quale verificava – anche grazie alla previsione di un relativo diritto soggettivo di accesso civico – se l'amministrazione fosse adempiente o meno agli obblighi di pubblicazione imposti dalla legge.

Sicché, in questo quadro normativo, l'amministrazione giungeva alla trasparenza soltanto per evitare di incorrere nelle sanzioni previste in caso di non adempienza all'obbligo di pubblicazione: da qui il concetto di trasparenza c.d. difensiva.

3.1. L'accesso alle informazioni come strumento per realizzare maggiore efficienza dell'attività amministrativa e combattere i fenomeni corruttivi

Pochi anni dopo, nel 2009, venne approvata la c.d. Riforma Brunetta con l'entrata in vigore del D.Lgs. n. 150 all'interno del quale la realizzazione del principio di trasparenza rappresentava uno dei pilastri fondanti.

La realizzazione dell'obiettivo della trasparenza veniva perseguita tramite lo strumento degli obblighi di pubblicazione sui siti istituzionali delle amministrazioni. Grazie alla pubblicazione online di informazioni ritenute dal legislatore centrali rispetto all'interesse dei cittadini (oltre a quelle concernenti l'organizzazione amministrativa e l'andamento della gestione, soprattutto le informazioni relative all'impiego di risorse pubbliche), lo scopo della Riforma Brunetta era, infatti, quello di realizzare la trasparenza intesa come «accessibilità totale», per potere giungere a concretizzare due diversi obiettivi: incrementare l'efficienza dell'azione e dell'organizzazione amministrativa, da un lato, e prevenire la corruzione, dall'altro (cfr. art. 11, comma 1, D.Lgs. n. 150/2009). Nell'idea del legislatore della Riforma Brunetta questi due fini potevano infatti venire realizzati grazie al controllo diffuso sull'amministrazione. Controllo diffuso che, è bene ribadirlo, è invece espressamente vietato in relazione all'accesso documentale *ex* art. 24, comma 3, Legge n. 214/1990.

L'amministrazione, in tal modo, veniva a trovarsi oggetto di una valutazione continua della propria *performance*. Valutazione dalla quale, inevitabilmente, tendeva a difendersi, e a fronte della quale essa era tenuta all'adozione e alla realizzazione di specifici Piani triennali per la trasparenza e l'integrità (cfr. art. 11, comma 2, D.Lgs. n. 150/2009).

Il cambio di prospettiva, tuttavia, emerge da un aspetto ben preciso: la valutazione sulla trasparenza, in realtà, era effettuata soltanto parzialmente da soggetti istituzionali preposti a tale compito (su tutti *ex* art. 13, comma 1, D.Lgs. n. 150/2009 la CiVIT, Commissione per la valutazione, la trasparenza e l'integrità delle amministrazioni pubbliche – le cui funzioni sono state ereditate dall'ANAC), in quanto il controllo più efficace, nell'idea del legislatore della Riforma Brunetta, era esercitato dai cittadini.

Dall'impianto generale della Riforma Brunetta emerge come la realizzazione della trasparenza sia un obiettivo cruciale, posto che essa viene innalzata a livello essenziale delle prestazioni ai sensi dell'art. 117, comma 2, lett. m), Cost. Ciononostante, alla mancata pubblicazione delle informazioni sui siti istituzionali, strumento tramite cui le amministrazioni sono in grado di attuare la trasparenza intesa come accessibilità totale alle informazioni, venivano ricondotte soltanto alcune disposizioni disincentivanti interne all'amministrazione,

quale il divieto di erogazione di retribuzione di risultato per i ruoli dirigenziali (cfr. art. 11, comma 9, D.Lgs. n. 150/2009).

Tale approccio deriva dal ruolo principe affidato al controllo sociale da parte della cittadinanza, in relazione al quale la previsione di sistemi sanzionatori vari passa in secondo piano. L'approccio inteso a privilegiare il controllo sociale da parte della cittadinanza rappresenta, peraltro, un ribaltamento totale di prospettiva sulla trasparenza rispetto all'accesso *ex* Legge n. 241/1990: la trasparenza diviene il risultato di un'azione positiva posta in essere dalla Pubblica Amministrazione, la quale «propone e non subisce l'acquisizione delle informazioni in suo possesso» (C. SILVESTRO, 2011, 711), come invece avviene nelle logiche dell'accesso ai documenti.

L'impostazione adottata dalla Riforma Brunetta in merito alla trasparenza ha costituito il punto di riferimento per la direzione della disciplina che il legislatore ha posto in essere pochi anni dopo con la Legge n. 190/2012, la c.d. legge Severino, nota altresì come legge anticorruzione. Intento principale della Legge n. 190/2012 è stato di contrastare la corruzione affiancando ai tradizionali strumenti repressivi di natura penale anche strumenti preventivi di carattere amministrativo (cfr. *ex multis* B.G. MATTARELLA, M. PELLISSERO, 2013. In relazione al tema della corruzione e dei possibili rimedi invece cfr. F. MERLONI, L. VANDELLI, 2010). Nelle intenzioni del legislatore, lo strumento anticorruttivo – o di lotta alla c.d. *maladministration* (cfr. F. PATRONI GRIFFI, 2013) – più adeguato sul piano della prevenzione fu identificato, appunto, nella trasparenza. La quale poteva essere attuata soltanto tramite la previsione di obblighi di pubblicazione e, dunque, grazie al controllo diffuso della cittadinanza (cfr. art. 1, commi 15 e 16, Legge n. 190/2012).

Nella realtà concreta, tuttavia, la trasparenza derivante dalla legge Severino è risultata essere uno strumento con portata piuttosto limitata. Questo sia sul piano della lotta alla corruzione: posto che, da un lato, tale strumento era incentrato (soltanto) sulla corruzione amministrativa senza interessarsi (anche) a quella politica, come messo in evidenza dalla dottrina (cfr. M. IMMORDINO, 2014, 406 ss.); e, dall'altro, la sua realizzazione non era affiancata all'implementazione di altri fattori cruciali per la lotta alla corruzione, quali i controlli amministrativi (cfr. S. ROSSA, 2018). Ma anche sul piano sistematico: poste le complesse condizioni politico-istituzionali che avevano portato all'insediamento del LXI governo della Repubblica (presieduto da Mario Monti), durante il quale venne approvata la Legge n. 190/2012.

A fronte di tali condizioni, al legislatore fu chiesto di intervenire tempestivamente, con interventi normativi celeri, in diverse materie, fra cui la materia legata alla trasparenza, appunto. Si giunse quindi a prevedere, nel testo stesso della legge Severino, anche una delega all'esecutivo finalizzata all'obiettivo di

razionalizzare e omogeneizzare la disciplina in materia (cfr. art. 1, commi 35 e 36, Legge n. 190/2012). Tale delega è alla base dell'approvazione del D.Lgs. n. 33/2013, il c.d. Decreto Trasparenza.

3.2. L'accesso civico come strumento di controllo sociale

La delega per il riordino della disciplina sulla trasparenza contenuta nella Legge n. 190/2012 ha condotto all'approvazione del D.Lgs. n. 33/2013, c.d. Decreto Trasparenza (cfr. B. PONTI, 2013; M. SAVINO, 2013; A.G. OROFINO, 2013; G. GARDINI, 2014). In questa disciplina è evidente il legame con l'impostazione della legge Severino e, prima ancora, della Riforma Brunetta, relativamente all'inquadramento della trasparenza come «accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni» (art. 1, comma 1, D.Lgs. n. 33/2013 testo originario in G.U.). Trasparenza posta in essere tramite la previsione di obblighi di pubblicazione sui siti web istituzionali e finalizzata a realizzare forme diffuse di controllo in relazione all'esercizio delle funzioni e all'impiego delle risorse economiche pubbliche e pertanto qualificata come "principio generale" (cfr. il titolo dell'art. 1, D.Lgs. n. 33/2013 testo originario).

Nonostante questo legame come le normative del 2009 e del 2012, il Decreto Trasparenza si differenzia tuttavia da esse sotto alcuni aspetti.

Il primo aspetto è quello relativo all'oggetto della trasparenza. Il D.Lgs. n. 33/2013 allarga il raggio d'azione della trasparenza, non ricomprendendo più soltanto le informazioni (concernenti l'organizzazione e l'attività amministrativa e l'impiego delle risorse per perseguire le funzioni) (cfr. art. 11, comma 1, D.Lgs. n. 150/2009), ma facendo riferimento altresì a dati e documenti (attinenti all'attività e all'organizzazione dell'amministrazione) (cfr. art. 2, comma 2, D.Lgs. n. 33/2013 testo originario).

Il secondo aspetto riguarda la creazione di una posizione giuridica soggettiva funzionalmente contrapposta all'obbligo di pubblicazione. Si è sottolineato poc'anzi come sia nella Riforma Brunetta, sia nella legge Severino, il non ottemperamento degli obblighi di pubblicazione online fosse bilanciato da un sistema di disincentivi interni all'amministrazione (cfr. ad es. l'art. 11, comma 9, D.Lgs. n. 150/2009). La scelta compiuta dal Decreto Trasparenza va in una direzione invece diversa, grazie all'elaborazione del c.d. diritto di accesso civico.

Tale situazione giuridica soggettiva consta di due momenti. Da un lato, nel diritto di accedere ai siti istituzionali dell'amministrazione in modo diretto e immediato, con il relativo diritto di conoscere, fruire, usare e riusare gratuitamente i documenti, le informazioni e i dati oggetto di pubblicazione obbliga-

toria, espressamente individuati dalle norme del Decreto Trasparenza (cfr. art. 2, comma 2, e art. 3, D.Lgs. n. 33/2013 testo originario). Dall'altro lato, nel diritto di richiedere (e ottenere) quei documenti, quelle informazioni e quei dati oggetto di pubblicazione obbligatoria, nel caso di mancata loro pubblicazione (cfr. art. 5, comma 1, D.Lgs. n. 33/2013 testo originario).

Da questi rilievi emerge come la natura del diritto di accesso civico sia composita ed eterogenea, soprattutto sul piano strutturale delineato dall'impianto del D.Lgs. n. 33/2013. Ciononostante, pare logico ricondurre questi due momenti a due diverse sfaccettature di un unitario diritto di accesso civico (cfr. in tal senso C. CUDIA, 2013, 64).

Entrambe tali pretese giuridiche soggettive tutelate giuridicamente spettano a «chiunque», ovvero a ciascun singolo individuo, indipendentemente dal fatto che sia, o meno, portatore di interessi qualificati o sia o meno coinvolto nel procedimento (cfr. M. SAVINO, 2013, 801).

Questo aspetto si contrappone a quanto stabilito invece in relazione all'accesso documentale, così come anche la mancanza di motivazione della richiesta di accesso civico (cfr. art. 5, comma 2, D.Lgs. n. 33/2013 testo originario).

Nell'originario disegno del Decreto Trasparenza l'assenza di un obbligo di motivare la richiesta di accesso discendeva peraltro dalla circostanza che le ipotesi per le quali documenti, informazioni e dati devono essere pubblicati dall'amministrazione sui propri siti istituzionali sono preventivamente individuate dal legislatore nelle norme del Decreto Trasparenza. A fronte di tale impostazione, non soltanto sarebbe risultato pleonastico imporre l'obbligo di motivazione, ma sarebbe stato altresì illogico, stante la *ratio* di controllo sociale diffuso di questa originaria tipologia di accesso civico.

3.3. Conseguenze ed effetti della trasparenza c.d. "difensiva"

Dall'analisi condotta nel paragrafo precedente, emerge chiaramente la profonda distanza che esiste fra il diritto di accesso documentale e il diritto di accesso civico. Essa costituisce il riflesso della *ratio* sottesa a questi due accessi: da un lato, tutelare situazioni giuridiche soggettive individuali nella legge sul procedimento e, dall'altro, favorire un ampio controllo sociale sull'attività dell'amministrazione nel Decreto Trasparenza – così ampio che vi è chi ha visto nell'accesso civico una vera e propria «azione popolare correttiva» (cfr. V. TORANO, 2013, 797). In realtà, è proprio la *ratio* di questi due diversi istituti a tracciare la loro distanza, come ben sottolineato da quella parte della dottrina che ha visto in questi due accessi, rispettivamente, un «*need to know*» e un «*right to know*» (cfr. B. PONTI, 2013, 97).

Parallelamente, è possibile evidenziare una correlata trasformazione del concetto di trasparenza. Avendo messo al centro l'informazione, vale a dire il risultato dell'elaborazione di dati, a scapito del documento – al punto che la dottrina ha riferito di uno «spostamento dell'asse dell'accesso» (cfr. E. CARLONI, 2013) – il legislatore ha rafforzato questo principio tramite la sua riconduzione alla cura di interessi generali e non più, nei fatti, di quelli particolari. Tale aspetto è frutto di una progressiva apertura dell'amministrazione nei confronti dei cittadini elaborata, inizialmente, proprio dalla legge sul procedimento.

È evidente come, con il Decreto Trasparenza, il livello di apertura dell'amministrazione alle istanze dei cittadini sia incrementato notevolmente rispetto agli anni '90. Parimenti, è altrettanto chiaro come tale apertura sia stata, più che posta in essere, *imposta in essere* dal legislatore unicamente a scopi difensivi, a fini di controllo sociale diffuso sull'azione dell'amministrazione e sull'impiego delle risorse pubbliche – dimenticando forse che nell'ordinamento italiano vi è un giudice adibito a tale compito: la Corte dei Conti (sul ruolo della Corte dei Conti come organo di controllo dello Stato-Ordinamento e dello Stato-Apparato, cfr. Corte cost., sent. 12-27 gennaio 1995, n. 29, con nota di G. PASTORI, 1995).

Nelle intenzioni del legislatore vi era la convinzione che la cittadinanza, tramite la creazione del diritto di accesso civico, avrebbe potuto costituire una perfetta struttura sociale in grado di costringere l'amministrazione a comportarsi sempre correttamente nella consapevolezza di essere costantemente tenuta d'occhio, esattamente come in un «moderno Panottico di Bentham» (figura utilizzata da D.-U. GALETTA, 2017, 66 ss.).

In realtà, l'istituzione di un diritto soggettivo di accesso civico, che sul piano teorico avrebbe potuto rappresentare una forte novità, sul piano pratico appare assai più modesta di quanto desumibile dal dato normativo, poiché gli obblighi di pubblicazione individuati dal legislatore ne hanno ristretto l'ambito di azionabilità. Pertanto, la *declamatio* del Decreto Trasparenza relativa alla «accessibilità totale alle informazioni» (art. 1, comma 1, D.Lgs. n. 33/2013 testo originario) appare irrealizzabile e sgonfiata nella sua portata, posto che i cittadini possono richiedere soltanto quelle precise informazioni previste *ex ante* dal legislatore, e solo quelle e nulla di diverso.

La trasparenza "difensiva" appare dunque come una trasparenza "parziale", in quanto l'utilità della sua portata viene ridimensionata sul piano dell'attuazione. La trasparenza "difensiva" pare in tal modo un'arma spuntata, in particolare per due ragioni.

Da un lato, non soltanto l'obiettivo di contrastare la corruzione pare irrealistico ma, paradossalmente, come è stato sottolineato, l'aumento di nuove norme (e logicamente di soggetti, organi, competenze ed eccezioni), non favorisce

certamente la chiarezza e la trasparenza dell'amministrazione e dell'ordinamento in generale, ma produce un vero e proprio aumento dell'entropia normativa. (cfr. A. PAJNO, 2015, 245, il quale scrive di una «iperregolamentazione puntuale, che provoca inflazione normativa e con essa non trasparenza, ma confusione ed opacità»).

Dall'altro lato, la previsione di obblighi di pubblicazione di particolari informazioni, quali, ad esempio, la retribuzione annua dei dirigenti pubblici, non ha comportato un controllo dei cittadini orientato a verificare che l'attività e l'organizzazione dell'amministrazione fossero effettivamente finalizzate al raggiungimento dell'interesse pubblico. L'accesso a queste informazioni si è trasformato, in realtà, in quello che è stato polemicamente qualificato in dottrina quale «vouyerismo amministrativo» (D.-U. GALETTA, 2014(b), 6). Un accesso, vale a dire, basato su interessi personali, e non pubblici, e mosso da sentimenti individuali assenti nelle intenzioni del legislatore, come nel caso evidente delle informazioni relative alla retribuzione annua dei dirigenti, la cui conoscenza da parte del cittadino ben poco ha a che vedere con l'interesse pubblico quanto, invece, con la curiosità (nel migliore dei casi, l'invidia in quelli peggiori) di venire a conoscenza di informazioni scollegate con la vera attività dell'amministrazione e della sua organizzazione.

Con tutti i *caveat* del caso, l'interesse degli azionisti di una società diretto unicamente a conoscere la retribuzione degli amministratori apparirebbe irrazionale e illogico nel mondo imprenditoriale, specie se ciò fosse accompagnato da un totale disinteresse in merito all'utile d'esercizio. Evidentemente, in relazione alla Pubblica Amministrazione, tale irrazionale illogicità non è stata altrettanto avvertita, almeno per i primi anni.

4. La trasparenza "ragionata" dell'attuale fase della digitalizzazione dell'amministrazione

A seguito dell'approvazione del D.Lgs. n. 33/2013 è apparso chiaro come l'intento del legislatore fosse stato quello di introdurre una disciplina che tendesse ad avvicinarsi a quella relativa ai c.d. modelli FOIA, derivanti dal *Freedom of Information Act* statunitense del 1966 – a sua volta il punto di sintesi legislativo fra il diritto a conoscere (*Right to know*) e la libertà di stampa (*Freedom of Press*) nell'interpretazione evolutiva effettuata dalla Corte suprema USA in alcune importanti decisioni (sul punto cfr. D.-U. GALETTA, 2016(a), 1022 ss.).

La normativa del Decreto Trasparenza, infatti, non poteva essere considerata a ragione un FOIA italiano, in quanto l'impostazione seguita dal legislato-

re del D.Lgs. n. 33/2013 si distanziava notevolmente sotto alcuni aspetti fondamentali da quella del modello FOIA, adottato in molti Stati, europei e non (in argomento in chiave comparata cfr. H.J. BLAKE, R. PERLINGEIRO, 2018).

Nel modello FOIA la regola generale è la pubblicità, mentre l'eccezione è la riservatezza; e ciò a fronte del fatto che il fine da raggiungere è la trasparenza, attuabile tramite il mezzo dell'accesso. Nella disciplina italiana del 2013, invece, come detto in precedenza, la riservatezza è la regola e la pubblicità l'eccezione (dato che non è possibile accedere a quelle numerose informazioni non rientranti fra quelle poche espressamente oggetto di obblighi di pubblicazione), con la conseguenza che il fine ultimo diventa l'accesso, raggiungibile tramite la trasparenza. Nella disciplina del D.Lgs. n. 33/2013, rispetto al modello FOIA, vi è dunque una doppia inversione di rapporti fisiologici, essendo ribaltato sia il rapporto regola-eccezione sia quello mezzo-fine (cfr. M. SAVINO, 2013, 802 ss.; 2015, 683 ss.).

Se, dunque, è corretto sottolineare la grande distanza concettuale fra la disciplina dettata dal Decreto Trasparenza e il modello FOIA, è altrettanto esatto evidenziare il netto cambiamento di prospettiva effettuato dal legislatore, in merito alla trasparenza, rispetto alla disciplina nazionale precedente. Ecco perché si è detto poc'anzi di come D.Lgs. n. 33/2013 abbia rappresentato un tentativo di avvicinamento della normativa italiana a quella estera del modello FOIA.

Con la promulgazione della Legge n. 124/2015, la c.d. legge Madia, introdotta con l'obiettivo di operare una riorganizzazione generale di tutta la Pubblica Amministrazione, il legislatore ha introdotto anche una delega governativa per l'adozione di una disciplina che modificasse la disciplina vigente in materia di trasparenza. A seguito di detta delega, nel 2016 è stato approvato il D.Lgs. n. 97, c.d. decreto FOIA, il quale, oltre ad apportare numerosi emendamenti al testo originario del D.Lgs. n. 33/2013, rappresenta il culmine del predetto tentativo del legislatore di avvicinare la disciplina italiana al modello FOIA.

Come vedremo (cfr. par. 4.1), proprio questo ulteriore avvicinamento al modello del *Freedom of Information Act* statunitense ha inciso profondamente – ancora una volta – sulla concezione della trasparenza. Con il passaggio da una trasparenza (solo) "difensiva", quale quella delineata nell'originario D.Lgs. n. 33/2013, ad una trasparenza più matura, come quella disegnata dal D.Lgs. n. 97/2016.

Una trasparenza, adoperando una immagine coniata dalla dottrina statunitense, "ragionata": una «*reasoned transparency* (…) *that demands that government officials offer explicit explanations for their actions*» (C. COGLIANESE, 2009, 537). E che quindi, contrariamente a quella avente natura difensiva (che

nella ricostruzione a stelle e strisce è chiamata «*fishbowl transparency*»), non è posta in essere «*[to] disclosure of information about "what" government is doing [but] to promote an understanding of "why" government does what it does*» (C. COGLIANESE, D. LEHR, 2019, 19).

Questa trasparenza "ragionata" è appunto tale poiché l'amministrazione giustifica l'adozione di una determinata scelta, a scapito di un'altra, tramite il coinvolgimento dei cittadini, travalicando il "mero" obbligo di motivazione del provvedimento. In tal senso, l'attuazione del principio di trasparenza comporta la concretizzazione di quello di partecipazione.

Quanto al ruolo della tecnologia, esso è certamente cruciale e indispensabile in entrambe le concezioni di trasparenza, sia essa difensiva o ragionata, dato che, come vedremo, sono gli strumenti digitali a permettere sul piano pratico l'accesso alle informazioni. Tuttavia, nella trasparenza "ragionata" la mera digitalizzazione svolge una funzione cruciale ma secondaria. È la maturità dell'ordinamento, e dunque della Pubblica Amministrazione, il fattore imprescindibile per la realizzazione di questo tipo di trasparenza – maturità che viene potenziata dal processo di digitalizzazione (cfr. F. COSTANTINO, 2015, 278).

4.1. L'accesso civico generalizzato

Con l'entrata in vigore del D.Lgs. n. 97/2016 (c.d. decreto FOIA) sono state apportate sostanziali modifiche al testo del D.Lgs. n. 33/2013 (in argomento cfr. G. GARDINI, M. MAGRI, 2019; B. PONTI, 2016; E. CARLONI, 2016; D.-U. GALETTA, 2016(a)(b); M. SAVINO, 2016 e 2019). Ciò allo scopo di porre rimedio alla scarsa efficacia dello strumento dell'obbligo di pubblicazione per porre in essere il principio di trasparenza

In particolare, il D.Lgs. n. 97/2016 è intervenuto emendando l'art. 5, D.Lgs. n. 33/2013 ed introducendo il diritto di accesso civico generalizzato: ovvero, il diritto di chiunque di accedere anche a dati e documenti delle Pubbliche Amministrazioni per i quali non sia previsto un obbligo di pubblicazione ai sensi della disciplina dell'accesso civico (cfr. art. 5, comma 2, D.Lgs. n. 33/2013 mod. D.Lgs. n. 97/2016).

Più precisamente, dall'analisi del testo del Decreto Trasparenza così come emendato dal decreto FOIA, si evince la coesistenza di questo diverso tipo di accesso civico con quello introdotto nel 2013 (quest'ultimo è disciplinato nell'art. 5, comma 1, D.Lgs. n. 33/2013 mod. D.Lgs. n. 97/2016). Essi sono entrambi presenti e in vigore, sebbene il riconoscimento dei rispettivi confini sia un compito non sempre agevole e che spetta all'interprete. E ciò, a causa di una duplice scelta confusionaria del legislatore: da un lato, quella di introdurre e

disciplinare questo nuovo istituto nella medesima norma dell'accesso civico («un pasticcio nel pasticcio», G. GARDINI, 2017, 6); dall'altro, quella di non aver dato un nome all'accesso civico generalizzato («dal pasticcio (…) all'alta pasticceria», G. GARDINI, 2017, 8): difatti il *nomen iuris* di accesso generalizzato è stato attribuito a questo istituto successivamente, ad opera delle Linee guida ANAC del 2016 (cfr. art. 1 Delibera ANAC n. 1309 del 2016).

La scelta di nominarlo in questo modo, pur avvenuta *ex post*, rispecchia correttamente la natura di questo accesso, il quale è stato posto in essere espressamente «[a]llo 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» (art. 5, comma 2, D.Lgs. n. 33/2013 mod. D.Lgs. n. 97/2016). Esso appare "generalizzato", non tanto perché, come per l'accesso civico, non sia necessaria né la dimostrazione di un interesse giuridico qualificato né una motivazione per il suo esercizio (cfr. art. 5, comma 3, D.Lgs. n. 33/2013 mod. D.Lgs. n. 97/2016); quanto, invece, per la sua sottrazione al parametro degli obblighi di pubblicazione prestabiliti dalla legge, aspetto che riflette la *ratio* di partecipazione.

Al di fuori dei casi di esclusione dell'accesso civico generalizzato espressamente previsti (cfr. 5-*bis*, comma 2, D.Lgs. n. 33/2013 mod. D.Lgs. n. 97/2016), chiunque può richiedere potenzialmente qualsiasi dato e documento – poiché il Decreto Trasparenza modificato dal decreto FOIA non contempla più le informazioni. Il che conduce a ritenere, sul piano del formalismo giuridico, come l'oggetto dell'accesso civico sia più ampio rispetto a quello dell'accesso civico generalizzato (cfr. rispettivamente l'art. 5, comma 1 e comma 2, D.Lgs. n. 33/2013 mod. D.Lgs. n. 97/2016).

Quello che, dunque, a prima vista sembra essere un importante allargamento del raggio di azione del cittadino si traduce, nei fatti, in una sua potenziale restrizione. Se, infatti, come si evince dal paragrafo successivo, l'accesso civico generalizzato consente al cittadino di poter richiedere all'amministrazione qualsiasi dato e documento, non essendovi più limiti imposti dalla legge *ex ante*, in verità, nel decidere se accogliere o meno la richiesta, l'amministrazione si trova a dover bilanciare discrezionalmente la richiesta di accesso generalizzato con le altre situazioni giuridiche ritenute meritevoli di tutela, e contrapposte all'accesso, previste dalla normativa. A seguito di questo bilanciamento, che avviene *ex post*, le probabilità che la Pubblica Amministrazione rigetti la richiesta di accesso sono in realtà molto ampie. Con la conseguenza che, sul piano concreto, e pur apparendo sul piano formale come più ampia, la trasparenza potrà risultare in fin dei conti ridotta a seguito dell'accesso civico generalizzato versione post legge Madia.

4.2. Conseguenze ed effetti della trasparenza "ragionata" e il collegamento con il riutilizzo dei documenti contenenti dati pubblici della Pubblica Amministrazione (cenni)

L'accesso civico generalizzato si differenzia dall'accesso civico essenzialmente sulla base di tre macro aspetti.

Il primo è relativo all'abbandono dell'impostazione concettuale basata sugli obblighi di pubblicazione. L'accesso viene dunque concesso – potenzialmente – rispetto a tutti i dati e i documenti detenuti dall'amministrazione ed indipendentemente dalla circostanza che essi siano ricompresi fra quelli obbligatoriamente da pubblicare in base alla disciplina dell'accesso civico ex D.Lgs. n. 33/2013.

Il secondo aspetto concerne l'oggetto dell'accesso generalizzato, che ricomprende i dati e i documenti ma non anche le informazioni – le quali, invece, sono ricomprese (solo) nell'ambito dell'accesso civico.

La terza macro differenza riguarda la *ratio* dell'accesso generalizzato. Non tanto (*recte*: non solo) favorire forme diffuse di controllo sull'attività dell'amministrazione, quanto promuovere la partecipazione dei cittadini all'attività dei soggetti pubblici, e dunque anche della Pubblica Amministrazione. Proprio per raggiungere tale obiettivo di partecipazione, considerando altresì come non sia necessaria né la motivazione dell'accesso civico generalizzato né la dimostrazione di un interesse giuridico qualificato, il D.Lgs. n. 97/2016 ha previsto che *chiunque* possa potenzialmente richiedere *qualsiasi* dato o documento all'amministrazione: tramite l'accesso generalizzato, il legislatore sprona i cittadini a richiedere e utilizzare i dati, soprattutto, e i documenti per partecipare attivamente al dibattito pubblico.

Nonostante tale nobile intento, l'impianto normativo limita però fortemente, sul piano concreto, l'attuazione del principio di partecipazione (cfr. in particolare A. CAUDURO, 2017). Da un lato, infatti, le limitazioni stabilite espressamente dal decreto FOIA, che rappresentano il frutto del bilanciamento fra l'accesso generalizzato e gli altri interessi contrapposti ma coinvolti, appaiono «molto ampie e, soprattutto, troppo poco puntuali» (D.-U. GALETTA, 2016(b), 10): il che impone all'amministrazione di effettuare un importante lavoro interpretativo. Dall'altro lato, proprio la mancanza della necessità di motivare la richiesta di accesso generalizzato, nonché l'assenza di "paletti normativi" che stabiliscano *ex ante* in modo certo cosa sia pubblicabile e cosa no, conducono l'amministrazione a dover intervenire *ex post*, sul piano interpretativo, per porre in essere una contemperazione fra l'interesse dell'individuo all'accesso, nel singolo caso concreto, e quegli interessi contrapposti che impongo l'esclusione dell'accesso – in riferimento a cui le rispettive norme si è già sottolineato essere ampie e vaghe. In tal modo, il rischio che la discrezionalità dell'ammini-

strazione conduca a un bilanciamento restrittivo della richiesta di accesso appare decisamente più ampio di quanto si possa pensare.

Questi due aspetti, letti congiuntamente fra loro, evidenziano come l'effettività dell'attuazione dei principi di trasparenza e di partecipazione risulti, in verità, assai fragile.

Il solo accesso civico generalizzato non è in grado, per come delineato dal legislatore del 2016, di garantire una effettiva e piena partecipazione dei cittadini. Per poter giungere a tale risultato, pare necessario leggere la disciplina dell'accesso civico generalizzato insieme a quella del riuso dei dati pubblici.

Sul piano concettuale, infatti, il mero accesso a un dato comporta una trasparenza e – soprattutto – una partecipazione limitate e parziali. Se, invece, una volta ottenuto il dato, il cittadino fosse libero altresì di riutilizzarlo, anche a fini di attività di impresa, ecco che allora i due summenzionati principi risulterebbero concretizzati in modo pieno. Il cittadino è infatti messo realmente nelle condizioni di poter partecipare all'attività della Pubblica Amministrazione qualora, potendo riutilizzare il dato pubblico proveniente dall'amministrazione, questi ponga in essere un'azione finalizzata alla conoscenza. Una conoscenza che, quale che sia la sua finalità (di tipo meramente culturale o finalizzata allo sfruttamento economico), può costituire un vantaggio sia per il singolo individuo sia per tutta la collettività (sul punto v. *infra* par. 5).

La necessità di legare l'accesso al riutilizzo dei dati (o dei documenti contenenti dati) oggetto dell'accesso è si è avvertita inizialmente a livello europeo. Infatti già nel 2003 il Parlamento europeo e il Consiglio dell'Unione Europea avevano approvato la Direttiva 2003/98/CE, c.d. Direttiva PSI (*Public Sector Information*), il cui obiettivo era quello di incoraggiare gli Stati membri a consentire il riutilizzo dei documenti pubblici contenti dati pubblici, mettendoli digitalmente a disposizione di persone fisiche o giuridiche, di modo tale che il contenuto di tali documenti potesse essere impiegato anche per scopi diversi da quelli per i quali i documenti erano stati posti in essere. L'"incoraggiamento" si traduceva nella discrezionalità riconosciuta ai Paesi membri di consentire o meno, il riutilizzo. L'ordinamento italiano ha recepito la Direttiva 2003/98/CE con l'approvazione del D.Lgs. n. 36/2006 (cfr. B. PONTI, 2006 e 2007; P. PATRITO, F. PAVONI, 2012).

Nel 2013, poi, i legislatori dell'Unione Europea hanno deciso di aggiornare la disciplina della Direttiva PSI al mutato contesto tecnologico e sociale, procedendo ad un'armonizzazione delle diverse normative nazionali dei vari Stati membri (posto che ve ne erano alcune che avevano stabilito l'obbligo di riutilizzo, mentre altre no). Per tale ragione, è stata approvata la Direttiva 2013/37/UE, che ha rappresentato un notevole "cambio di passo" rispetto alla Direttiva 2003/98/CE, grazie all'imposizione, in capo agli Stati membri, dell'obbligo per tutti i Paesi

membri di rendere riutilizzabili i documenti delle pubbliche amministrazioni in base alle condizioni stabilite da apposite licenze di riutilizzo e dunque potenzialmente anche a fini commerciali. Il recepimento italiano della Direttiva 2013/37/UE è avvenuto tramite il D.Lgs. n. 102/2015 (modificativo del D.Lgs. n. 36/2006).

La disciplina italiana attuale è in tal modo dettata nel D.Lgs. n. 36/2006 così come modificato nel 2015.

A seguito, tuttavia, dell'approvazione nell'estate 2019 della Direttiva 2019/1024/UE – di rifusione delle precedenti Direttive 2013/37/UE e 2003/98/CE, che in particolare ha spostato l'oggetto del riuso dal documento contenente i dati pubblici al dato pubblico in sé – l'ordinamento italiano sarà chiamato entro il luglio 2021 a recepire tale direttiva, emendando nuovamente la normativa domestica.

Senza voler entrare nel dettaglio, a fronte delle summenzionate norme emerge come sussista ormai un vero e proprio obbligo, in capo alla Pubblica Amministrazione, di rendere riutilizzabili, in modo tendenzialmente gratuito e tramite le tecnologie digitali, i documenti contenenti dati pubblici delle Pubbliche Amministrazioni (i quali devono possedere un formato aperto e devono essere leggibili meccanicamente) anche per fini commerciali, grazie all'imposizione di una apposita licenza di riutilizzo (sul punto si rinvia a S. ROSSA, 2019(a); F. GASPARI, 2016; M. FALCONE, 2016). Ovviamente, le eccezioni al riutilizzo non mancano, ma quel che più conta, in questa sede, è sottolineare l'esistenza del riutilizzo come regola generale. E proprio il riutilizzo dei dati fra Pubbliche Amministrazioni, cittadini e imprese è visto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022 – elaborato e pubblicato nel luglio 2020 dall'Agenzia per l'Italia Digitale e dal Dipartimento per la Trasformazione Digitale – quale strumento per giungere a una consapevole valorizzazione del patrimonio informativo pubblico orientato sul «paradigma degli *open data*» (cfr. AGID-Dipartimento per la Trasformazione Digitale, 2020, p. 17).

Se appare chiaro come l'accesso ai dati sia reso possibile, sul piano concreto, dal processo di digitalizzazione, ancora più evidente è il legame logico che unisce il riutilizzo del dato all'impiego delle ICT e al grado di maturazione digitale della società, nella quale oggi risulta "normale", ovvero intuitivo e immediato, il *download* e l'*upload* di numerosi dati.

Il combinato disposto fra la disciplina dell'accesso civico generalizzato e quella sul riuso dei dati pubblici (contenuti o meno nei documenti) costituisce dunque un elemento chiave, da un lato, per attuare sul piano concreto il principio di partecipazione e, dall'altro, per riflettere sull'attualità o meno, oggi, della metafora turatiana quale paradigma di riferimento in tema di trasparenza.

5. Il contributo della digitalizzazione dell'amministrazione per una concezione più ampia del principio di trasparenza

Obiettivo di questo capitolo è stato delineare l'evoluzione dei mezzi posti in essere dal nostro legislatore nazionale al fine di attuare il principio di trasparenza. Occorre a questo punto precisare, tuttavia, come tale progresso sia avvenuto in parallelo rispetto all'evoluzione del processo di digitalizzazione dell'Amministrazione Pubblica. L'idea di fondo è, dunque, che il miglioramento dei livelli di digitalizzazione nella Pubblica Amministrazione ha comportato un affinamento degli strumenti di trasparenza (e non l'inverso!).

In realtà, come è testimoniato da varie indagini comparatistiche effettuate dalla dottrina, l'ordinamento italiano aveva previsto, già nel testo originario della Legge n. 241/1990, alcuni istituti in grado di garantire la trasparenza dell'azione amministrativa a prescindere dal contesto tecnologico. Da un lato, l'obbligo di motivazione del provvedimento, posto che l'amministrazione agisce in modo trasparente qualora le sue decisioni siano conoscibili e comprensibili (cfr. F. MANGANARO, 2014, 557). Dall'altro, la partecipazione endoprocedimentale al procedimento (cfr. D.-U. GALETTA, 2017, che evidenzia la centralità di questi due strumenti nell'ordinamento dell'Unione Europea, in quello tedesco e francese). Istituti che «paiono di recente del tutto passati di moda nel dibattito italiano sulla trasparenza» (D.-U. GALETTA, 2016(a), 1061), ma che, qualora rivitalizzati, potrebbero essere fondamentali per la concretizzazione del principio di trasparenza.

Ciò posto, se si riconosce nella tecnologia una natura catalizzatrice – caratteristica difficilmente negabile – risulta allora intuibile il fondamentale apporto del processo di digitalizzazione alla realizzazione della trasparenza. A parere di chi scrive, infatti, le tecnologie digitali hanno affiancato una strada complementare alla via tradizionale alla trasparenza, perseguibile tramite gli strumenti delineati nella legge sul procedimento (accesso documentale, partecipazione procedimentale e obbligo di motivazione dei provvedimenti amministrativi). Una strada complementare, e non alternativa, che si dirama parallelamente a quella tradizionale e che si fonda sul binomio "accesso e riuso" del dato.

In questo specifico contesto, l'oggetto non è più né il documento né l'informazione bensì il dato, posto che i dati rappresentano la base per l'elaborazione di numerose informazioni. Come è stato infatti sottolineato in dottrina «il dato di per sé non veicola alcun significato. Esso è solo l'elemento di partenza su cui viene elaborata l'informazione» (A. MASUCCI, 2004, par. 4; cfr. anche G. CARULLO, 2020, 137 ss.). In tal senso, un dato appare più utile di una informazione, in quanto da un singolo dato è possibile ottenere diverse informazioni, ovviamente dando per scontato di avere i mezzi per farlo.

Un semplice esempio può rendere evidente tale affermazione: da un singo-

lo dato, quale quello relativo alla distribuzione nel mondo del numero di persone di discendenza italiana, si possono ricavare diverse informazioni, fra le quali la ricostruzione delle ondate emigratorie, oppure la percentuale di conoscenza della lingua italiana nel mondo in rapporto alle altre lingue. Tuttavia, è molto più difficile ricavare i dati da informazioni. Per usare una similitudine, il dato è dunque la creta che, una volta modellata e cotta, dà vita al vaso. L'informazione è, invece, il vaso: da esso è difficilmente possibile ricavare la creta, ed è altrettanto difficile poterlo modellare in modo diverso.

Ponendo l'accento sul libero accesso ai dati, vale a dire l'accesso civico generalizzato, e sul loro libero riutilizzo, ovvero dando la possibilità ai cittadini di entrare in possesso dei dati aperti dell'amministrazione e di impiegarli per fini vari, anche a scopi di natura commerciale (a seconda della licenza attribuita, ovviamente), è possibile mettere i cittadini nella condizione di conoscere.

Questa conoscenza costituisce la base dello sviluppo sia di natura culturale (nell'ottica dell'*Homo Sapiens*) sia di natura economica (in quella dell'*Homo Oeconomicus*), a vantaggio del singolo e della società nel suo complesso (cfr. S. ROSSA(a), 2019, 1129).

È chiaro come tale processo di conoscenza sia reso attuabile sul piano della realtà proprio grazie alla concretizzazione del principio di trasparenza nell'ambito della Pubblica Amministrazione. Un'amministrazione che, "aprendo" i propri dati, li mette a disposizione dei cittadini, i quali hanno diritti di accedere a essi non più con logiche di controllo, bensì a fini di partecipazione e collaborazione con i soggetti pubblici («conoscere per partecipare», come titola un volume della collana dell'ANAC: cfr. A. CORRADO, 2018), si mostra come un'amministrazione trasparente, un'amministrazione aperta. D'altronde, come già evidenziato in precedenza, i principi di trasparenza, di partecipazione e di collaborazione costituiscono proprio i perni sui quali ruota la strategia di *Open Goverment*.

Tutto ciò è evidentemente possibile grazie all'impiego delle ICT nella società e al crescente livello di digitalizzazione dell'Amministrazione Pubblica.

Come si è avuto modo di mettere in luce nei precedenti paragrafi, all'incremento della digitalizzazione della Pubblica Amministrazione si è affiancato un progressivo affinamento della maniera di concretizzare il principio di trasparenza: da tutela di posizioni giuridiche soggettive individuali con l'accesso documentale, nella fase della trasparenza "debole", a strumento di lotta alla corruzione e di controllo sociale con l'accesso civico, nella fase della trasparenza "difensiva", a incentivo alla partecipazione con l'accesso civico generalizzato, nella fase della trasparenza "ragionata". Di riflesso è mutato anche l'oggetto della trasparenza, passando dai documenti, alle informazioni e infine ai dati, proprio a fronte del cambiamento tecnologico avvenuto nella realtà.

In questo cambio di prospettiva sulla trasparenza, il processo di digitalizza-

zione è stato in effetti determinante. Esso ha portato con sé nuovi strumenti tecnici in grado di consentire azioni difficilmente prospettabili solo pochi anni addietro (quale l'accesso istantaneo ai dati presenti sul web o la facilità di *download* e *upload* necessario al riuso dei dati, a cui si è accennato poc'anzi), saldando anche sul piano fattuale, oltre che su quello logico, il legame fra accesso ai dati e riutilizzo degli stessi e ponendo così le basi pratiche sia per un ulteriore incremento della digitalizzazione dell'amministrazione, sia per l'avvicinamento dell'accesso al diritto all'informazione nell'ordinamento italiano (cfr. S. ROSSA, 2019(b); già G. GARDINI, 2014, si interrogava sul punto in merito al D.Lgs. n. 33/2013).

In tal senso, pare evincersi una variazione del concetto di trasparenza fondato sulle tecnologie digitali. Grazie alla digitalizzazione, il principio di trasparenza tende ad avvicinarsi al principio di partecipazione (e a quello di collaborazione, seppur in modo più lieve), in piena attuazione del c.d. *Open Government* e distanziandosi all'ambito procedimentale in senso stretto.

Questa nuova declinazione della trasparenza, discendente dal processo di digitalizzazione dell'amministrazione, non si trova in contrapposizione con quella più tradizionale e riconducibile all'ambito procedimentale e connessa alla partecipazione al procedimento e all'obbligo di motivazione del provvedimento amministrativo. L'una non esclude, infatti, l'altra. Anzi, l'una fortifica l'altra, vicendevolmente.

A ben vedere, infatti, la trasparenza intesa in senso ampio, in quanto sintesi di queste due diverse declinazioni, si avvicina sempre di più alla "buona amministrazione", prevista dall'art. 41 della Carta dei diritti fondamentali dell'Unione Europea e che rappresenta un vero e proprio diritto fondamentale della persona (cfr. D.-U. GALETTA, 2005, 819 ss., 2013 e 2019(b). V. anche capitolo III, D.-U. GALETTA). In questo senso, appare determinante il contributo che la digitalizzazione dell'amministrazione ha apportato, e apporta, all'attuazione del principio di trasparenza.

Da quanto ricostruito poc'anzi, emerge con forza un concetto di trasparenza più ampio di quello che per decenni è emerso dalla figura della "casa di vetro" coniata da Turati (in questo senso già D.-U. GALETTA, 2016(a), 1059). E questo dipende ed è dipeso in massima parte, come si è cercato di mettere in evidenza, dall'apporto della digitalizzazione all'amministrazione. Ma è dipeso anche dalla prospettiva di un cambiamento nel rapporto fra amministrazione e cittadini: da una relazione basata sul sospetto (sul quale si è fondata la trasparenza "difensiva"), ad una relazione che dovrebbe invece basarsi sulla fiducia e che caratterizza la trasparenza "matura", correlata alla partecipazione.

Questo rapporto di fiducia per realizzarsi appieno necessita di condizioni sociali, ma soprattutto tecnologiche, le quali si stanno realizzando proprio nel corso degli anni più recenti: e sono proprio queste "condizioni tecnologiche"

a poter rappresentare la vera chiave di volta affinché il fiore della trasparenza possa sbocciare in tutta la sua complessità.

Bibliografia

AGID, *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021*, Roma, 2019, in https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2019_-_2021_allegati 20190327.pdf.

AGID, DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE, *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022*, Roma, 2020, in https:// www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pa_2020_2022.pdf.

ATTI DEL PARLAMENTO ITALIANO – CAMERA DEI DEPUTATI, sess. 1904-1908, Leg. XXII, I sess., II torn., 17 giugno 1908, 22962.

BLAKE H.J., PERLINGEIRO R. (a cura di), *The Right to Access to Public Information. An International Comparative Legal Survey*, Heidelberg-Dordrecht-London-New York, 2018.

CARLONI E., *Se questo è un FOIA. Il diritto a conoscere tra modelli e tradimenti*, in *Astrid Rassegna*, 2016, p. 4.

CARLONI E., *L'amministrazione aperta. Regole e limiti dell'open government*, Rimini, 2014.

CARLONI E., *I principi del codice della trasparenza*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33, Rimini*, 2013, p. 29 ss.

CARULLO G., *La gestione e lo scambio di dati nel settore pubblico nel contesto dell'Unione europea*, in D.-U. GALETTA (a cura di), *Diritto amministrativo nell'Unione europea. Argomenti (e materiali)*, Torino, 2020, p. 135 ss.

CARULLO G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2017.

CAUDURO A., *Il diritto di accesso a dati e documenti amministrativi come promozione della partecipazione: un'innovazione limitata*, in *Dir. amm.*, 2017, 3, p. 601 ss.

CLEMENTE DI SAN LUCA G., *Diritto di accesso e interesse pubblico*, Napoli, 2006.

COGLIANESE C., LEHR D., *Transparency and Algorithmic Governance*, in *Adm. Law Rev.*, 2019, 1, p. 1 ss.

COGLIANESE C., *The Transparency President? The Obama Administration and Open Government*, in *Governance – Intern. Jour. Pol., Admin., Inst.*, 2009, 4, 529 ss.

COGNETTI S., *Quantità e qualità della partecipazione. Tutela procedimentale e legittimazione processuale*, Milano, 2000.

CORRADO A., *Conoscere per partecipare. La strada tracciata dalla trasparenza amministrativa*, Napoli, 2018.

COSTANTINO F., voce *Open Government*, in *Dig. disc. pubbl.*, Agg., Torino, 2015, p. 268 ss.

COSTANZO P., *Aspetti e problemi dell'informatica pubblica*, in AA.VV., *Studi in onore di Victor Uckmar*, I, Padova, 1997, p. 291 ss.

CUDIA C., *Il diritto alla conoscibilità*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33*, Rimini, 2013, p. 57 ss.
DOGLIOTTI M., ROSIELLO L. (a cura di), *Lo Zingarelli 1996. Vocabolario della Lingua italiana di Nicola Zingarelli*, Bologna, 1996.
DUNI G., voce *Teleamministrazione*, in *Enc. giur. Treccani*, XXX, Roma, 1993, p. 1 ss.
FALCONE M., *Dati aperti e diritto al riutilizzo delle informazioni: la declinazione italiana del paradigma degli open data*, in B. PONTI (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni*, Rimini, 2016, p. 601 ss.
FOÀ S., *La nuova trasparenza amministrativa*, in *Dir. amm.*, 2017, 1, p. 65 ss.
FRACCHIA F., *Riti speciali a rilevanza endoprocedimentale*, Torino, 2003.
FROSINI V., *Cibernetica, diritto e società*, Milano, 1968.
GALETTA D.-U., *Open Government, Open Data e azione amministrativa*, in *Ist. fed.*, 2019, 3, p. 663 ss. [2019a].
GALETTA D.-U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in M.C. PIERRO (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Milano, 2019, p. 1 ss. [2019b].
GALETTA D.-U., *Trasparenza e contrasto della corruzione nella Pubblica Amministrazione: verso un moderno panottico di Bentham?*, in *Dir. soc.*, 2017, 1, p. 43 ss.
GALETTA D.-U., *Accesso civico e trasparenza della pubblica amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto legislativo n. 33/2013*, in Federalismi.it, 2016 [2016b].
GALETTA D.-U., *La trasparenza per un nuovo rapporto fra cittadino e Pubblica amministrazione: un'analisi storico-evolutiva in una prospettiva di diritto comparato ed europeo*, in *Riv. it. dir. pubbl. comunit.*, 2016, 5, p. 1019 ss. [2016a].
GALETTA D.-U., *Alcuni recenti sviluppi del diritto amministrativo italiano (fra riforme costituzionali e sviluppi della società civile)*, in *Giustamm.*, 2014, 11 [2014b].
GALETTA D.-U., *Transparency and Access to Public Sector Information In Italy: a Proper Revolution?*, in *Italian Journal of Public Law*, 2014, 2, p. 212 ss. [2014a].
GALETTA D.-U., *Riflessioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE sul diritto ad una buona amministrazione, anche alla luce di alcune recenti pronunce della Corte di giustizia*, in *Dir. UE*, 2013, 1, p. 133 ss.
GALETTA D.-U., *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione*, in *Riv. it. dir. pubbl. comunit.*, 2005, 3, p. 819 ss.
GALLO C.E., FOÀ S., voce *Accesso agli atti amministrativi*, in *Dig. disc. pubbl.*, Torino, 2000 (agg. cur. F. PAVONI), p. 1 ss.
GARDINI G., MAGRI M. (a cura di), *Il FOIA italiano: vincitori e vinti. Un bilancio a tre anni dall'introduzione*, Rimini, 2019.
GARDINI G., *Il paradosso della trasparenza in Italia: dell'arte di rendere oscure le cose semplici*, in Federalismi.it, 2017, p. 1.
GARDINI G., *Il codice della trasparenza: un primo passo verso il diritto all'informazione amministrativa?*, in *Giorn. dir. amm.*, 2014, 8-9, p. 875 ss.
GASPARI F., *L'agenda digitale europea e il riutilizzo dell'informazione del settore pubblico*, Torino, 2016.

IMMORDINO M., *Strumento di contrasto alla corruzione nella pubblica amministrazione tra ordinamento italiano ed ordinamento brasiliano. Relazione introduttiva*, in *Nuov. Auton.*, 2014, 3, p. 395 ss.
LOSANO M.G., *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Torino, 1969.
MANGANARO F., *Trasparenza e obblighi di pubblicazione*, in *Nuov. aut.*, 2014, 3, p. 553 ss.
MANGANARO F., *L'evoluzione del principio di trasparenza amministrativa*, in astridonline.it, 2009.
MASUCCI A., *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in *Riv. dir. civ.*, 2004, 5, par. 4.
MASUCCI A., *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Napoli, 1993.
MATTARELLA B.G., PELLISSERO M. (a cura di), *La legge anticorruzione. Prevenzione e repressione della corruzione*, Torino, 2013.
MERLONI F., VANDELLI L. (a cura di), *La corruzione amministrativa. Cause, prevenzione e rimedi*, Firenze, 2010.
MERLONI F., *Trasparenza delle istituzioni e principio democratico*, in F. MERLONI, (a cura di), *La trasparenza amministrativa*, Milano, 2008, p. 3 ss.
MINISTERO PER LA COSTITUENTE – COMMISSIONE PER GLI STUDI ATTINENTI ALLA RIORGANIZZAZIONE DELLO STATO, *Relazione all'Assemblea Costituente*, I, *Problemi costituzionali – Organizzazione dello Stato*, Roma, 1956.
MORBIDELLI G., *Il procedimento amministrativo*, in L. MAZZAROLLI, G. PERICU, A. ROMANO, F.A. ROVERSI MONACO, F.G. SCOCA (a cura di), *Diritto amministrativo*, I, Bologna, 2005, p. 531 ss.
NIGRO M., *Il procedimento amministrativo fra inerzia legislativa e trasformazioni dell'amministrazione (a proposito di un recente disegno di legge)*, in *Dir. proc. amm.*, 1989, 1, p. 5 ss.
OBAMA B., *Transparency and Open Government. Memorandum for the Heads of Executive Departments and Agencies*, Washington DC, 2009, in https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government.
OECD, *Open Government. The Global Context and the Way Forward*, Parigi, 2016, in https://read.oecd-ilibrary.org/governance/open-government_9789264268104-en#page1.
OGP, *Open Government Partnership*, 2011, in https://www.opengovpartnership.org.
OROFINO A.G., *Profili giuridici della trasparenza amministrativa*, Bari, 2013.
PAJNO A., *Il principio di trasparenza alla luce delle norme anticorruzione*, in *Giust. civ.*, 2015, 2, 213 ss.
PASTORI G., *Il controllo di gestione della Corte dei Conti fra controllo e collaborazione*, in *Le Regioni*, 1995, 6, p. 1095 ss.
PATRITO P., PAVONI F., *La disciplina del riutilizzo dei dati pubblici dal punto di vista del diritto amministrativo: prime riflessioni*, in *Dir. inf.*, 2012, 1, p. 87 ss.
PATRONI GRIFFI F., *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in Federalismi.it, 2013, p. 8.
PONTI B. (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni*, Rimini, 2016.

PONTI B. (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33*, Rimini, 2013.

PONTI B., *Il patrimonio informativo pubblico come risorsa. I limiti del regime italiano di riutilizzo dei dati delle pubbliche amministrazioni*, in *Dir. pubbl.*, 2007, 3, p. 991 ss.

PONTI B., *Il riutilizzo dei documenti del settore pubblico*, in *Giorn. dir. amm.*, n. 8/2006, p. 817 ss.

PUBUSA A., *L'attività amministrativa in trasformazione. Studi sulla l. 7 agosto 1990, n. 241*, Torino, 1993.

ROMANO A. (a cura di), *L'azione amministrativa*, Torino, 2016.

ROMANO TASSONE A., *A chi serve il diritto di accesso? (Riflessioni su legittimazione e modalità d'esercizio del diritto d'accesso nella l. n. 241 del 1990)*, in *Dir. amm.*, 1995, p. 315 ss.

ROSSA S., *Il diritto all'informazione come base per una amministrazione digitale: una comparazione fra Italia ed Estonia*, in *Dir. econ.*, 2019, 2, p. 543 ss. [2019b].

ROSSA S., *"Open Data" e amministrazioni locali. Riflessioni sul processo di digitalizzazione partendo dall'esperienza della Regione Piemonte*, in *Dir. inf.*, 2019, 4, p. 1121 ss. [2019a].

ROSSA S., voce *Controlli amministrativi (profili ricostruttivi)*, in *Dig. disc. pubbl.*, Banca Dati Ipert., Torino, 2018, p. 1 ss.

SANDULLI A., *Il procedimento*, in CASSESE, S. (a cura di), *Trattato di diritto amministrativo*, P. gen., Milano, 2003, p. 1083 ss.

SANDULLI M.A., *Codice dell'azione amministrativa*, Milano, 2017.

SANDULLI M.A., voce *Accesso alle notizie e ai documenti amministrativi*, in *Enc. dir.*, agg. IV, 2000, p. 1 ss.

SARTOR G., *Nozione e settori dell'informatica giuridica*, in G. PERUGINELLI, M. RAGONA (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Napoli, 2014, p. 59 ss.

SAVINO M., *Il FOIA italiano e i suoi critici: un dibattito scientifico meno platonico*, in *Dir. amm.*, 2019, 3, p. 645 ss.

SAVINO M., *Il FOIA italiano. La fine della trasparenza di Bertoldo*, in *Giorn. dir. amm.*, 2016, 5, p. 593 ss.

SAVINO M., *Le riforme amministrative: la parabole della modernizzazione dello Stato*, in *Riv. trim. dir. pubbl.*, 2015, 2, p. 641 ss.

SAVINO M., *La nuova disciplina della trasparenza amministrativa*, in *Giorn. dir. amm.*, 2013, 8-9, p. 795 ss.

SILVESTRO C., *Trasparenza e Riforma Brunetta*, in *Foro amm. – TAR*, 2011, 2, p. 706 ss.

TORANO V., *Il diritto di accesso civico come azione popolare*, in *Dir. amm.*, 2013, 4, p. 789 ss.

VILLATA R., *La trasparenza dell'azione amministrativa*, in *Dir. proc. amm.*, 1987, p. 528 ss.

IX.

LA REGOLAZIONE DI FRONTE ALLE SFIDE DELL'ICT E DELL'INTELLIGENZA ARTIFICIALE

Fabiana Di Porto

1. Premessa

Il presente capitolo intende fornire un contributo ad un nascente filone di studio, quello della *Law & Technology* (nel prosieguo anche *Law&Tech* o L&T), che si distingue dal Diritto dell'informatica o dell'innovazione o delle Tecnologie dell'Informazione e della Comunicazione (ICT), come pure da altri filoni di studio, noti specialmente nei paesi nord americani, quali gli *Empirical Legal Studies* (o ELS), ed anche dal cosiddetto *Legal Tech*. La *Law&Tech* è un

nuovo campo di ricerca che utilizza strumenti propri delle computer science, specialmente il Natural Language Processing (NLP) e il Machine Learning (ML), per analizzare temi giuridici. Classificheremo questo nuovo filone di indagine attorno a quattro aree di ricerca: (i) analisi, (ii) interpretazione (iii) applicazione ed *enforcement*, e (iv) *enhancement* del diritto (par. 2).

Nella seconda parte del capitolo approfondiremo specificamente la quarta (iv) sottocategoria, di *law enhancement*, per esplorare in che misura gli algoritmi di tipo predittivo possano essere impiegati per fare regolazione.

Articoleremo quindi una proposta per fare regolazione algoritmica. A tal fine impiegheremo l'esempio della regolazione degli obblighi informativi, o altrimenti denominata *disclosure regulation*. Per rendere operativa la proposta presenteremo un modello in due fasi, in ciascuna delle quali saranno impiegate tecnologie algoritmiche al fine di riformare questa strategia regolatoria prona al fallimento. Ciò rende ascrivibile la nostra proposta al filone di ricerca della *Law&Tech* (par. 3.1).

Nella prima fase, proporremo di utilizzare le tecnologie NLP e ML per combinare le norme (*de iure disclosure*) con i *disclaimer* di settore che ne sono attuazione (*de facto disclosure*), considerandoli come due database. A seguito di questa "combinazione" faremo una classificazione (*ranking*) in base ad indici di fallimento appositamente elaborati. Questo processo ci porterà a selezionare le *disclosure* che, sul piano testuale, "falliscono" meno: le BADs o *best available disclosure* (par. 3.2).

Nella seconda fase, utilizzeremo una *sandbox* regolamentare per testare le BADs con persone reali in un ambiente controllato prima della diffusione su larga scala dell'algoritmo regolatorio. Ciò ci consentirà di coniugare tre obiettivi: (i) costruire delle *disclosure* differenziate per gruppi di destinatari, aumentando la proporzionalità dell'intervento regolatorio; (ii) coniugare trasparenza e partecipazione con l'impiego di algoritmi nel procedimento normativo; (iii) integrare dati comportamentali a dati testuali in un "grafo della conoscenza" (*knowledge graph*) che si aggiorna automaticamente. Questo tipo di strategia regolatoria algoritmica ci consentirà di arrivare a selezionare quelle che enfaticamente definiamo le BEDs (o *best ever disclosure*, le migliori *disclosure* di sempre) (par. 3.3).

Tracciato il modello, altri impieghi in diversi ambiti giuridici saranno sempre possibili (par. 4).

2. La *Law and Technology*: modelli e finalità dell'integrazione tra *data science* e diritto

A seguito dei rapidi progressi dell'informatica, ed in particolare del NLP e del ML (su cui *infra* par. 2.1) registrati negli ultimi decenni, si sta affermando

una branca di studio interdisciplinare la cui denominazione è ancora in via di definizione, ma che potrebbe cogliersi nella locuzione *Law and Technology*, o anche *Law&Tech* (o L&T). Si tratta di un filone di indagine che combina metodologie proprie dell'informatica a studi giuridici, e che sta attirando negli Stati Uniti come in Europa crescente attenzione (M.A. LIVERMORE e D.N. ROCKMORE, 2019, K.D. ASHLEY e D. KEVIN, 2017, M. MEDVEDEVA, 2019). È indubbio che della *Law&Tech* esistano declinazioni giuspubblicistiche come privatistiche, di cui si darà conto, ove rilevante.

La *Law&Tech* va tenuta distinta dall'analisi giuridica delle nuove tecnologie (*Technology Law*) o dei mercati digitali, variamente definita come informatica giuridica, diritto dell'ICT o dell'innovazione tecnologica *et similia*. Mentre i problemi analizzati dagli studiosi di *Technology Law* potrebbero in parte sovrapporsi a quelli affrontati dai colleghi di *Law&Tech*, i primi si basano su metodologie giuridiche convenzionali (dottrinali) per esaminare nuovi fenomeni determinati dal progresso tecnologico (come i big data, gli algoritmi predittivi, l'Intelligenza artificiale, la *blockchain*, gli *smart contract*) (v. capitolo III, D.-U. GALETTA, e capitolo IV, R. CAVALLO PERIN e I. ALBERTI, nonché capitolo VI, G. CARULLO); mentre il *Law&Tech* impiega strumenti propri dell'informatica per svolgere questi compiti (v. capitolo I, A. SIMONICINI).

D'altra parte, l'utilizzo di algoritmi come mezzi di indagine è una caratteristica che il filone del *Law&Tech* condivide con l'industria della tecnologia legale (o *Legal Tech*). Nel *Legal Tech* vengono infatti utilizzati sofisticati software di *machine learning* per supportare pratiche legali quotidiane: si pensi ad esempio alla previsione dei «risultati dei casi giudiziari, o alla gestione dei dati per la *compliance* normativa» (C. DEVINS *et al.*, 2017). Altri ambiti nei quali il *Legal Tech* è impiegato sono quello della *discovery* probatoria svolta per via elettronica, ove gli studi legali si avvalgono di strumenti di apprendimento automatico per il recupero di informazioni; tali programmi sono altresì impiegati per ricercare casi giudiziari (precedenti) rilevanti. Si tratta di impieghi straordinari: basti pensare ai risparmi per le *law firm* derivanti dal poter analizzare in maniera automatica migliaia di casi, facendosi così una idea più precisa degli orientamenti delle corti e dei possibili esiti decisionali. Anche gli *smart contract*, spesso utilizzati nella pratica legale, rientrano in questa categoria; così come il cosiddetto "RegTech" nel settore finanziario (una tecnologia algoritmica che supporta i destinatari della abbondante regolamentazione informativa per adempiere ai propri doveri nel modo più economico possibile). Quello della *compliance* normativa è un altro settore straordinariamente in crescita (si pensi agli obblighi antitrust), ove le imprese possono usare algoritmi per fare previsioni sulle ispezioni ed altri adempimenti e, dunque, economizzare. A differenza del *Legal Tech*, tuttavia, la *Law and Technology* è un ambito di ricerca; e come tale

copre una gamma molto ampia di interessi scientifici (su cui *infra*).

Ancora. Sebbene contiguo e talvolta sovrapponibile, il *Law&Tech* va tenuto distinto dagli *Empirical Legal Studies* (o ELS) (L. EPSTEIN, A. MARTIN, 2010). I due impiegano metodologie di ricerca e talvolta studiano problematiche simili; tuttavia, ciò fanno perseguendo obiettivi scientifici diversi. Come il primo, anche i secondi utilizzano software per l'analisi del linguaggio come, appunto, il NLP ed il ML (si pensi, nel caso degli ELS, alla moderna criminologia o, nelle discipline umanistiche, alle *digital humanities*), e in entrambi i casi, molti dei compiti una volta svolti manualmente (come la classificazione dei testi in base ad indici, la ricerca statistica avanzata) sono ora eseguiti (automaticamente o semi-automaticamente) tramite software di apprendimento automatico (il ML appunto). Come nella *Law&Tech* anche negli ELS i casi giurisprudenziali sono oggetto di particolare attenzione. Ad esempio, le decisioni dei tribunali vengono esaminate per trovare prove di incoerenza, di *bias* o disaccordo tra i giudici su determinati argomenti giuridici. Fondamentali sono in tale ambito i lavori di Spaeth e Epstein, iniziatori del database delle decisioni della Corte Suprema (H.J. SPAETH e L. EPSTEIN, 2016), che rappresenta un modello per altre giurisdizioni, nonché, specie la seconda, attivista e seguita editorialista.

Tuttavia, nel caso degli ELS, l'obiettivo principale è quello di fornire supporto empirico alla ricerca nelle scienze sociali, più che indagare tematiche giuridiche in quanto tali. Il fine ultimo degli ELS è quindi diverso e talvolta giunge ad ispirare o sollecitare legislatori e politici ad adottare riforme o la società civile ad agire (interessanti e provocatori gli articoli della politologa Epstein in cui, dalle colonne del New York Times, dati empirici alla mano, propone riforme e "giudica" la Corte Suprema statunitense).

Esaurita la pur sintetica disamina di ciò che essa "non" è, procediamo ad individuare in positivo l'oggetto di studio della *Law&Tech*nology.

Sulla base degli interessi di ricerca che persegue, questa nuova disciplina può essere raggruppata attorno a quattro grandi aree di interesse: (i) analisi, (ii) interpretazione (iii) applicazione ed *enforcement*, ed (iv) *enhancement* (o rafforzamento algoritmico) del diritto.

2.1. Analisi algoritmica del diritto

L'analisi algoritmica del diritto può essere spiegata, almeno in parte, in analogia con l'analisi economica del diritto (o Law and Economics, L&E). Nessuna delle due è di per sé, unicamente, una metodologia, ma entrambe usano approcci che sono propri di discipline non giuridiche per svolgere i propri compiti.

Tuttavia, mentre la L&E, come noto, usa modelli economici per cercare di prevedere, spiegare e valutare normativamente il comportamento umano e le norme giuridiche, la L&T applica tecnologie informatiche per svolgere le proprie indagini.

In particolare, automatizzando il costoso e laborioso compito di leggere, classificare, organizzare e analizzare documenti giuridici (come norme, sentenze, ma anche rapporti di policy, come libri bianchi, minute, resoconti stenografici di commissioni parlamentari, ecc.), questa tecnologia consente di "leggere" e "studiare" enormi volumi di testo con grande rapidità.

Nell'ambito del ML, sono due le metodologie che oggi consentono la "lettura a distanza" di testi (o "distant reading": F. MORETTI, 2000): quella *supervised* e quella *unsupervised*. Nella prima l'uomo (il giurista nel nostro caso) annota a mano un certo numero di documenti (come norme, sentenze, o qualsiasi altro testo), ossia li classifica secondo indici quantificabili di proprio interesse, cui attribuisce dei pesi, fornendo in tal modo alla macchina delle istruzioni. Ad esempio, se intende istruire l'algoritmo a riconoscere quante istanze presentate negli ultimi cinquanta anni in una certa materia sono risultate inammissibili, dovrà fornire al programma documenti classificati in base a cause che producono vizi di inammissibilità, di modo che la macchina possa apprendere a riconoscerli. Dopodiché l'algoritmo apprende da questo gruppo di documenti a svolgere l'indagine fornendo risultati che saranno rielaborati dall'annotatore, onde verificarne la attendibilità. Maggiore il numero di documenti, migliore la *performance* e più preciso il risultato.

Nel secondo caso, dell'*unsupervised machine learning*, disegnato l'algoritmo secondo l'obiettivo, non si forniscono istruzioni né definiscono pesi, lasciando che sia l'algoritmo, in base a come è stato disegnato sulla base delle indicazioni fornite dall'esperto (il giurista), a ricercare le correlazioni rilevanti tra i documenti forniti.

È bene precisare che l'intervento umano non scompare neppure in questo secondo caso: sarà infatti sempre necessario che il giurista intervenga a "ripulire" i risultati forniti dalla macchina (sovrapposizioni, incongruenze, ecc.) in base alle proprie conoscenze scientifiche prima di potersene avvalere. In altri termini, in nessun caso è possibile escludere l'apporto umano dall'uso degli algoritmi (il cosiddetto *man in the loop*), a tecnologia data. Circa l'impiego in concreto della migliore tra le due, il dibattito tra gli addetti ai lavori è ancora aperto, essendovi vantaggi e svantaggi nell'impiego tanto della *supervised* quanto dell'*unsupervised* ML.

Da ultimo, occorre menzionare l'importante apporto della *Data Visualization*. Non si tratta, come potrebbe apparire a tutta prima, della mera resa grafica semplificata dei risultati di analisi algoritmiche complesse. La *Data Visualization*

certamente offre nuovi modi di visualizzare i risultati di un'analisi, rendendoli così più accessibili e facili da comprendere e interpretare. Ma essa permette altresì di accedere dalla interfaccia grafica direttamente alla sottostante parte analitica. Il che evidentemente abbrevia, agevolandole, le vie comunicative tra giuristi e ingegneri dei dati.

Diversi sono gli impieghi che gli studiosi di *Law&Tech* hanno fatto di tali applicazioni per l'analisi del diritto, come ad esempio: l'estrapolazione di *claims and arguments* (M-F MOENS *et al.*, 2007; O SHULAYEVA *et al.*, 2017), la semplice classificazione di norme (BIAGIOLI C *et al.*, 2005), o la creazione di tassonomie giuridiche basate sulla modellizzazione automatizzata di argomenti (SARNE et al, cit., p. 2). Alcuni sostengono inoltre che l'uso di algoritmi possa ridurre l'impatto dei *bias* cognitivi sulle scelte dei ricercatori (F. FAGAN, 2016). Tuttavia, a parere di altri questa obiettività potrebbe essere limitata e portare a nuovi errori cognitivi (R. KITCHIN, 2014). Ad esempio, se nel *dataset* che l'algoritmo considera la propensione a commettere un crimine è fortemente correlata alla etnia, il rischio di discriminazione nell'assumere decisioni diviene molto elevato (è quanto accaduto nel pluridibattuto caso Loomis: *Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis*, Case no. 2015AP157-CR, 5 April-13 July 2016).

2.2. Interpretazione giuridica a mezzo di algoritmi

In una seconda accezione, gli strumenti algoritmici possono essere impiegati per dare maggiore spessore all'interpretazione del diritto (o all'applicazione della norma al singolo caso) da parte delle corti o della dottrina. Ciò è particolarmente rilevante nei sistemi di *common law*, in cui l'identificazione della legge applicabile e dei precedenti è cruciale. Ne consegue (o se si vuole in linea di continuità), che l'uso dell'algoritmo può contribuire enormemente agli studi di diritto comparato e internazionale. È possibile, infatti, grazie all'analisi di enormi moli di casi, fonti dottrinali, arresti delle corti internazionali, chiarire con maggiore precisione le differenze di interpretazione tra giurisdizioni, o delinearne i chiaroscuri.

Ad esempio, Olsen e Küçüksu (2017) utilizzano la *quantitative network analysis* per identificare e analizzare la giurisprudenza della Corte europea dei diritti dell'uomo sul Regolamento 2016/679/UE (GDPR). Nel confrontare i risultati delle loro analisi con quelli conseguiti con l'approccio qualitativo convenzionale (dottrinale), essi dimostrano come l'indagine algoritmica riveli schemi interpretativi rimasti completamente inesplorati in passato.

Similmente, Derlén e Lindholm (2017) applicano i *network centrality mea-*

surement (ossia dei grafi che consentono di misurare l'importanza relativa di pagine web all'interno di una rete, come un *social network*) alle decisioni della Corte di giustizia dell'UE in tema di mercato interno, al fine di valutare «how accurately they capture the precedential and persuasive power of case law». Anch'essi giungono alla conclusione, che condivido, che la combinazione di metodi giuridici tradizionali e strumenti quantitativi di tipo algoritmico *sub specie interpretationis* (2.2) non potrà che rafforzarne gli esiti, dal momento che consentirà ai ricercatori di elaborare più dati documentali e quindi di individuare modelli eziologici diversi e sin qui inesplorati.

2.3. Uso di algoritmi per l'applicazione ed *enforcement* del diritto

Per quanto riguarda *l'enforcement* e l'applicazione della legge, molto è stato scritto in merito a quali misure, in quali ambiti e procedimenti, sia amministrativi sia giurisdizionali, gli algoritmi predittivi (v. capitolo III, D.-U. GALETTA, e capitolo IV, R. CAVALLO PERIN) potrebbero essere utilizzati. Ad esempio, Lowden (2018) discute l'uso degli algoritmi nei procedimenti di valutazione del rischio da parte dei tribunali penali statunitensi per le decisioni di messa in libertà provvisoria. Egli sottolinea il grande potenziale degli algoritmi nel poter rendere queste decisioni meno discrezionali ed anche efficienti. Tuttavia, mette anche in guardia contro i possibili *bias* e i problemi di trasparenza nell'uso di tali strumenti; problemi evidenziati anche da Brayne e Christin (2020), secondo cui l'uso di algoritmi creerà semplicemente modi diversi di esercizio della discrezionalità giudiziaria e, in ultima analisi, aumenterà i casi di discriminazione, semplicemente spostando le pratiche discriminatorie nelle "parti meno visibili" del processo giudiziario penale (ad esempio, nella composizione dei *database* e nella selezione degli algoritmi utilizzati).

Questioni simili sorgono riguardo all'uso di strumenti algoritmici da parte di amministrazioni e agenzie per quanto riguarda le attività di *enforcement* del diritto. Un esempio importante di tali applicazioni è quello degli *Automated Suspicion Algorithms* (ASA), che vengono utilizzati dalle forze di polizia statunitensi con l'obiettivo di prevenire il crimine (la cosiddetta polizia preventiva). Va notato, tuttavia, che il crescente impiego di algoritmi nell'*enforcement* e nell'applicazione della legge si estende oltre il contesto della giustizia penale: essi vengono anche utilizzati per «selezionare i contribuenti ai fini dell'audit da parte dell'IRS, per il rilascio o il diniego dei visti di immigrazione» (M.L. RICH, 2016) o per decidere quali ristoranti assoggettare a controlli da parte delle autorità locali (C. COGLIANESE, 2019).

In generale, sebbene si possano determinare efficienze sul piano decisiona-

le e risparmi in termini di costi (N. RANGONE, 2019), l'uso di questi strumenti appare ancora molto controverso, specialmente per ragioni inerenti la limitata trasparenza, la non chiara responsabilità e le possibili distorsioni al procedimento amministrativo (N. RANGONE, 2019).

2.4. "*Enhancement*" (o rafforzamento) di norme mediante algoritmi

Infine (e specialmente, ai fini del presente scritto), rileva la quarta sottocategoria della *Law&Tech*, ove gli strumenti algoritmici sono usati per "rafforzare", in senso migliorativo, il modo in cui leggi e regolazioni sono concepite sin dal loro disegno. Si tratta evidentemente di una modalità ancora in fase di esplorazione, in cui il potere analitico delle tecniche di ML e dei big data viene variamente impiegato per "anticipare" problematiche giuridiche prima che si materializzino.

Un esempio importante di questo approccio è l'idea del "diritto personalizzato" (o *perzonalized law*), che mira ad utilizzare i dati sulle preferenze individuali per progettare norme su misura, ovverosia norme che si adattano alle preferenze e alle esigenze dei singoli individui sì da evitare problemi di *over* o *under-inclusiveness* (quindi di proporzionalità). Si pensi ad esempio alle regole di *default* (A. PORAT, L. STRAHILEVITZ, 2013; O. BEN-SHAHAR, A. PORAT., 2016), o agli obblighi informativi personalizzati (C. BUSCH, 2016; P. HACKER, 2017; F. DI PORTO, 2017; F. DI PORTO, M. MAGGIOLINO, 2019) inseriti automaticamente nei contratti e/o presentati nel momento in cui i consumatori ne hanno bisogno e secondo formati congeniali alle loro preferenze.

Gli strumenti algoritmici offrono quindi nuove opportunità ai legislatori e regolatori in quanto consentono l'analisi automatizzata di enormi quantità di informazioni che devono essere considerate in un processo normativo di *future-proof drafting* (S. RANCHORDÁS, 2019; European Economic and Social Committee (2016) explanatory Opinion on Future proof legislation, 2016/C 487/07, *GUUE* C 487/51, pp. 51-56).

Le prospettive di questa quarta linea di indagine del *Law & Tech* al fine di risolvere i possibili fallimenti della regolazione sono dunque enormi. Per fare un esempio, si pensi al tema della semplificazione normativa (oggi attuata con strumenti come il c.d. taglia-leggi e supervisionata da un apparato di apposite istituzioni). L'algoritmo può essere istruito ad individuare automaticamente i testi oscuri, i rinvii a norme vigenti confliggenti, quelli a norme abrogate implicitamente, e così via. A "segnalazione" ricevuta, esso può essere altresì istruito a "suggerire" gli interventi di semplificazione normativa (come le debite abrogazioni espresse di norme non più in vigore in quanto mai attuate) da inserire in testi da sottoporre all'attenzione dei competenti organi legislativi.

Onde comprendere più a fondo le potenzialità della regolazione algoritmica, ne illustreremo un caso specifico, quello degli obblighi informativi (o *algorithmic disclosure regulation*).

A questo dedicheremo maggiore spazio considerandolo paradigmatico di come in futuro potrà articolarsi la integrazione tra uso degli algoritmi predittivi e produzione di regole.

3. La regolazione algoritmica: un modello per la produzione degli obblighi informativi e non solo

È noto e ampiamente arato in dottrina il tema del fallimento della strategia regolatoria degli obblighi informativi (F. DI PORTO 2017). Questi sono presenti nel codice del consumo, nei contratti assicurativi, finanziari, nel GDPR. Ma sono anche oggetto di trasparenza e comunicazione amministrative, rispettivamente, in base al D.Lgs. n. 33/2013 e al D.Lgs. 7 marzo 2005, n. 82 (CAD), i quali obbligano tutte le PP.AA. a pubblicare sui propri siti web istituzionali e sportelli unici digitali ogni informazione sui servizi erogati (v. capitolo III, D.-U. GALETTA, e capitolo IV, R. CAVALLO PERIN e I. ALBERTI, nonché capitolo VI, G. CARULLO). La quantità di informazioni che gli individui ricevono per effetto di questi obblighi è tale che nessuno le legge più (*information overload*). Nel mondo digitale, caratterizzato da rapidità delle transazioni, e dei modi di aggiornarsi e socializzare, l'informazione è ancora meno rilevante per compiere le scelte (si pensi ai termini e condizioni contrattuali o ai formulari privacy resi visibili prima di "scaricare" una applicazione).

A ciò si aggiunga che dal lato delle imprese l'uso degli algoritmi e dei big data consente di tracciare il comportamento degli utenti e quindi di conoscerne le preferenze (in merito a prezzi, qualità dei servizi, abitudini di consumo, ecc.). Ciò tende a svuotare l'autonomia negoziale di una parte (tipicamente l'utente della piattaforma, sia esso consumatore finale o piccola e media impresa, PMI) a vantaggio dell'altra (oggi identificabile con l'intermediario o piattaforma digitale), senza che la condotta manipolatoria sfoci necessariamente in una pratica illecita (in quanto scorretta o ingannevole) (D. SUSSER *et al.*, 2019).

Ancorché superflua e sostanzialmente fallimentare la *disclosure regulation* continua ad essere massicciamente impiegata a livello europeo, financo nei mercati digitali. Ne sono esempi: la Direttiva 2019/2161/UE *New Deal for Consumers* e il Regolamento 2019/1150/UE sui rapporti tra piattaforme digitali e PMI (Platform-to-Business). Tutti introducono nuovi obblighi informativi, come ad esempio quello di informare i consumatori se i prezzi praticati sono personalizzati (cioè mutano automaticamente in base ai dati sulle abitu-

dini di consumo); di comunicare quali sono i parametri impiegati per costruire i *ranking* (le graduatorie di merito) con cui ci appaiono le offerte dei servizi (dando per scontato che questa informazione sia di per sé rilevante); dire se i rating dei servizi o beni (cioè le valutazioni espresse in modo sintetico con scale numeriche, stelle, punti, ecc. sulla base dei giudizi degli utenti) sono forniti dietro remunerazione (ad es., chi vende un bene su una piattaforma può pagare per aumentare la propria visibilità, specie se è appena approdato sulla stessa), e così via.

Ma la *disclosure regulation* è anche uno dei rimedi che la Commissione europea sta considerando di introdurre nel Digital Services Act (presentato a giugno 2020) come strumento per garantire maggiore concorrenza nel mercato digitale europeo (https://ec.europa.eu/digital-single-market/en/digital-services-act-package).

Pochi sono i riferimenti alla qualità dei dati o dei database impiegati: in un solo caso, infatti, si chiede espressamente che le informazioni fornite dalle piattaforme in esecuzione degli obblighi di *disclosure* siano leggibili dalle macchine (o *machine-readable*: requisito prodromico a che un algoritmo possa processarle, v. capitolo VI, G. CARULLO).

La domanda centrale di questo lavoro è: quali sono le soluzioni che la *Law&Tech* può fornire per "salvare" una strategia regolatoria che ha oramai esaurito ogni capacità di assolvere la propria funzione? (se si eccettua quella meramente simbolica, politica?).

3.1. Adottare una prospettiva di *Law&Tech* per rimediare ai fallimenti regolatori degli obblighi informativi significa assumere un "approccio onnicomprensivo"

Preliminarmente occorre chiarire cosa significa adottare un approccio *Law&Tech* per affrontare il tema del fallimento regolatorio. Si tratta evidentemente di un metodo estremamente innovativo, in quanto si propone l'impiego di algoritmi predittivi per intervenire sul disegno delle norme, al fine di renderle più efficaci.

In secondo luogo, come vedremo subito appresso, a tutt'oggi esistono numerosi diversi algoritmi che sono impiegati per il *distant reading* (*supra* par. 2.1), ognuno dei quali ha normalmente finalità proprie (in quanto viene elaborato *ad hoc* per scopi di ricerca specifici). Tuttavia, la circostanza che si debbano classificare i documenti in base ad indici, i quali sono elaborati secondo le esigenze di chi utilizza gli algoritmi, consente una certa flessibilità nel loro impiego.

Tornando così alla domanda iniziale, ovvero se la *Law&Tech* possa risolvere il fallimento della disciplina degli obblighi informativi, la questione diviene se possiamo tradurre i fallimenti di quella politica regolatoria in termini di indici che un algoritmo che "legge" documenti possa rilevare.

Questo passaggio è rilevante in quanto la letteratura *Law&Tech* ci offre moltissimi strumenti algoritmici pensati per semplificare i testi normativi, come pure i documenti prodotti dalle imprese (specialmente i *disclaimer* delle privacy) e renderli più intelligibili (*infra* par. 3.2.4). Parimenti, essa ha elaborato numerosi algoritmi per leggere ed estrarre conoscenza dalla giurisprudenza europea e financo nazionale (almeno per quella già resa *machine-readable*).

Le *disclosure*, come detto, non sono mero testo. Esse mirano ad informare al fine di rendere edotto, consapevole circa un qualche diritto (si pensi al diritto di accesso ai propri dati personali riconosciuto dall'art. 15 GDPR), posizione soggettiva che l'individuo può esercitare (nell'esempio fatto, l'accesso può essere finalizzato ad ottenere la cancellazione dei dati raccolti – lett. e) – ovvero l'intervento umano nel caso delle decisioni completamente automatizzate *ex* art. 22). Esse servono pertanto a far compiere una determinata scelta informata, qualunque essa sia.

Questo collegamento tra informazione ricevuta e comportamento, deve potersi cogliere anche nella traduzione del procedimento algoritmico che qui si propone. Detto altrimenti, la *Law&Tech* suggerisce un *enhancement* della normativa, che consente di anticipare problematiche che potrebbero sorgere nella fase attuativa.

Si tratta, potremmo dire, dell'equivalente (futurista) delle discipline *behaviorally informed* sperimentate sin qui dal legislatore europeo, cioè di quelle Direttive e Regolamenti ove riferimenti a che le informazioni vengano fornite «in modo chiaro, semplice, comprensibile» (riferimenti assenti fino a qualche anno fa), sono stati inseriti a seguito di indagini empiriche sul comportamento umano. Questi incisi servono ad anticipare problematiche (i testi sono scritti in maniera incomprensibile o sovrabbondante e non vengono letti) rese note al legislatore europeo da test comportamentali al momento del disegno della norma.

Occorre quindi che anche nel procedimento algoritmico possa darsi conto (o traccia) oltre che del *dato* testuale, anche del *dato* comportamentale.

Si pensi ad esempio alle *regulatory sandbox* impiegate nel settore finanziario: sia negli Stati Uniti, sia in Europa si utilizza un ambiente controllato (denominato *sandbox*) per testare alcuni prodotti finanziari e alcune regole prima della loro adozione su larga scala. Nelle *sandbox* partecipano normalmente il regolatore e l'industria e talvolta anche gli investitori (ESMA, EBA, EIOPA, 2019).

Il caso della *regulatory sandbox* è particolarmente interessante, perché può

costituire un ambiente ove raccogliere i dati comportamentali da integrare nell'algoritmo. In altri termini, i dati comportamentali possono servire a "confermare" o "smentire" se i testi che sono stati selezionati come i migliori (in base agli indici di fallimento) saranno anche quelli più efficaci a determinare scelte congruenti (ad esempio, in tema di privacy, determineranno maggiore consapevolezza sul diritto di accesso ai propri dati personali *ex* art. 15, GDPR). In ultima analisi, ciò darà modo di recuperare forza, pur in un ambiente digitale, alla autonomia decisionale individuale basata sull'informazione.

Un altro grande potenziale offerto dall'impiego delle tecnologie algoritmiche è la capacità di raccogliere e analizzare dati in tempo reale. Ciò può costituire un notevole passo avanti nelle politiche regolatorie cosiddette *evidence-based*, ovverosia basate su evidenze empiriche (di cui normalmente si ha traccia nei documenti di analisi di impatto della regolazione, di cui all'art. 14, Legge 28 novembre 2005, n. 246 e al D.P.C.M. 15 settembre 2017, n. 169). Si pensi alla disciplina sulle infografiche del packaging dei prodotti da fumo, preceduta da studi sul comportamento dei consumatori e su come questi reagiscono alla fornitura di informazioni testuali sintetiche e grafiche nei vari paesi europei. Per quanto queste evidenze empiriche possano essere diffuse e varie, esse rimangono occasionali. Cioè raccolte sulla base di indagini che non si aggiornano automaticamente, ma sono "date", e dunque possono perdere di attualità e di utilità.

Ne consegue che elaborare soluzioni normative sulla base di esse potrebbe avere dei limiti, poiché potrebbero emergere nuove evidenze che mostrano risultati opposti (ad esempio, i consumatori potrebbero cessare di essere reattivi ad alcuni tipi di informazioni; oppure le imprese digitali potrebbero iniziare ad offrire nuovi servizi, o cambiare strategie di marketing).

Ciò implica che al fine di sostenere l'intervento regolatorio sarebbe preferibile ripetere esperimenti utilizzando dati che restano sempre aggiornati. Qualcosa che le tecnologie algoritmiche consentono di fare.

Oltre al tema della "freschezza" dei dati empirici che supportano una strategia regolatoria, vi è quello del *locus* del fallimento regolatorio. Se si guarda alle proposte dottrinali e alle conseguenti strategie di semplificazione impiegate a livello europeo per migliorare la *disclosure regulation* (ad esempio fornire le informazioni «in modo conciso, trasparente, intelligibile e facilmente accessibile»: art. 12 GDPR) ci si avvede che per lo più si interviene sul fronte delle *de facto disclosure*, ovverosia sulle informazioni prodotte dall'industria, dando per scontato che lì si annodi il fallimento della *disclosure regulation*.

Invero, così facendo si tiene in ombra buona parte del problema: ovverosia che l'origine dei problemi possa essere nella "fonte" dell'obbligo informativo. Non è raro, infatti, che le norme siano scritte in modo oscuro o che gli obietti-

vi siano *self-defeating* (ad esempio, nel citato art. 12 GDPR l'obbligo per il «titolare del trattamento» di essere "conciso" e quello di essere "intelligibile" potrebbero, in certi casi, entrare in conflitto, perché alcuni utilizzi dei dati personali potrebbero essere complessi da spiegare e dunque richiedere ben più di un testo conciso).

Ne consegue che l'impiego di soluzioni algoritmiche dovrebbe seguire un "approccio onnicomprensivo" (o *comprehensive approach*), che valuti cioè gli obblighi informativi (e conseguentemente le soluzioni testuali adottate dalle imprese) come una strategia unitaria, che include sia i possibili fallimenti che attengono alla fonte normativa sia quelli relativi alla sua attuazione (da parte del mercato).

In terzo ed ultimo luogo, l'utilizzo di tecniche algoritmiche di semplificazione dei testi può essere molto utile, come vedremo, nel ridurne l'opacità o aumentarne la leggibilità (R. LEPINA *et al.*, 2019; I. AYRES, A. SCHWARTZ, 2014). Tuttavia, ciò non risolve ogni problema poiché, come anticipato, il fallimento della *disclosure regulation* può essere dovuto a fattori comportamentali. Pertanto, oltre a migliorare la qualità dei testi attraverso l'apporto degli algoritmi, occorre altresì essere in grado di stabilire se ciò aumenta le *chances* che questi testi siano anche compresi e, specialmente, impiegati per compiere delle scelte. Ad esempio, come regolatori avremmo bisogno di stabilire se una clausola di garanzia *algorithmically enhanced* (rafforzata algoritmicamente sul piano testuale) sia anche valutata dal destinatario in modo corretto oppure in modo eccessivamente ottimistico (un tipo di *bias* noto in letteratura). Ne consegue che, secondo un "approccio onnicomprensivo", le tecnologie algoritmiche debbano essere utilizzate per "misurare" e "graduare" i fallimenti delle *disclosure* sia sul piano testuale sia su quello comportamentale.

Per riassumere, adottare un "approccio onnicomprensivo" di *Law&Tech* significa riuscire ad individuare e misurare indici di fallimento in tutte le fasi: quella della redazione della *de iure disclosure*; della sua attuazione nella *de facto disclosure*; nonché i fallimenti comportamentali emergenti nel momento in cui il destinatario dell'informazione è esposto alla *de facto disclosure*, oltre alle loro interazioni. E suggerire "miglioramenti" (o *enhancement*) sia dal punto di vista testuale, sia comportamentale.

Come può la tecnologia algoritmica riuscire in tutto questo? E qual è la nostra proposta?

Nel prosieguo si delineeranno le due fasi procedimentali, documentale e comportamentale, in cui avviene quello che abbiamo definito l'*enhancement* normativo algoritmico.

3.2. Fase 1. *Enhancement* algoritmico del testo: le *Best Available Disclosures* (BADs)

Per poter utilizzare algoritmi è anzitutto necessario compiere un'operazione logico-ricostruttiva consistente nel concepire un testo come insieme di dati che la macchina possa leggere, inclusa la norma. «Law as Data» è il titolo di un bel libro curato da M.A. LIVERMORE e D.N. ROCKMORE (cit.), in cui si suggerisce che qualsiasi legge, regolazione sia un testo fatto di dati e, come tale, possa essere letto, annotato e analizzato da algoritmi per estrarre informazione utile all'analisi giuridica.

3.2.1. Costruzione del primo *dataset*: le *de iure disclosure*

Seguendo questo approccio, il nostro primo *dataset* è costituito dalle *de iure disclosure*, ovverosia dalle norme che pongono obblighi di trasparenza (si pensi da ultimo all'art. 6-*bis* della Direttiva 2011/83/UE sui diritti dei consumatori, emendata nel 2019, che obbliga le piattaforme digitali a comunicare i parametri utilizzati per il *ranking* dei risultati delle ricerche fatte online).

A livello europeo, tutte le normative sono reperibili mediante il canale di ricerca EurLex; esse sono altresì classificabili ed annotabili mediante strumenti di ML quali, ad esempio, il sistema ELI (European Legislation Identifiers). A livello interno, tutte le fonti normative risultano accessibili attraverso il portale Normattiva liberamente accessibile. L'esistenza di un database ad accesso aperto (*open access*) costantemente aggiornato e classificato secondo indici uniformi facilita notevolmente l'attività di ricerca di un algoritmo. Così ad esempio, BOELLA *et al.* hanno sviluppato un algoritmo in grado di estrarre le relazioni semantiche tra i testi giuridici, in modo da contribuire a migliorarne la chiarezza e la comprensibilità (BOELLA *et al.*, 2019).

3.2.2. Costruzione del secondo *dataset*: le *de facto disclosure*

Il nostro secondo *dataset* è costituito dalle *de facto disclosure*, ovverosia dai testi ('disclaimer') diffusi dalle imprese (o dalle amministrazioni) in attuazione degli obblighi informativi (si pensi agli obblighi di trasparenza *ex* D.Lgs. n. 33/2013). Si tratta, come detto, delle informazioni che gli individui tendono a non leggere online (come i termini e le condizioni contrattuali proposti prima di scaricare una qualsiasi applicazione). Normalmente anche questi testi sono disponibili in formato digitale (si v. da ultimo l'art. 34 del D.L. 16 luglio 2020, n. 76, Misure urgenti per la semplificazione e l'innovazione digitale, convertito con la Legge 11 settembre 2020, n. 120, che sancisce l'obbligo in capo alle pubbliche amministrazioni di condividere il patrimonio informativo di cui è in

possesso per ragioni istituzionali o in ragione dell'espletamento di un pubblico servizio mediante la istituenda Piattaforma Nazionale Digitale Dati) e possono essere letti, annotati ed analizzati da algoritmi (si veda ad esempio il funzionamento dell'algoritmo CLAUDETTE sviluppato dall'Istituto Universitario Europeo, che legge ed evidenzia le clausole "problematiche" dei termini e condizioni contrattuali delle principali piattaforme digitali: M. LIPPI *et al.*, 2018).

3.2.3. Il ruolo "legante" della giurisprudenza

Quanto alla giurisprudenza, occorre fare un discorso a parte. Chiaramente le sentenze, sia delle corti europee sia – seppur in misura minore – di quelle nazionali, sono accessibili *online* e codificate mediante la banca dati EurLex (laddove per la giurisprudenza nazionale esiste il sistema ECLI, che è ancora in fase di completamento). Ciò implica che tali testi sono conoscibili da parte della macchina in quanto insieme di *dati*. La giurisprudenza svolge un ruolo essenziale, in quanto consente di collegare i due *dataset* delle *de iure* e *de facto disclosure*. Le decisioni delle corti, infatti, servono a chiarire il significato da attribuire ai termini controversi; pertanto, al fine di sfruttare appieno il potenziale esplicativo ed eziologico della giurisprudenza, occorre avvalersi di strumenti algoritmici in grado di collegare stabilmente il modo in cui le corti interpretano una certa norma o clausola in entrambi i *dataset*. Da questo punto di vista, la dottrina (PANAGIS *et al.*, 2017) ha proposto di avvalersi della *citation network analysis*: uno strumento algoritmico che consente di stabilire quale caso giurisprudenziale utilizzare e a quale decisione dare prevalenza in caso di interpretazioni confliggenti tra diverse corti.

Riassumendo: la giurisprudenza, mediante lo strumento della *citation network analysis*, può essere utilizzata per collegare dinamicamente i due *dataset* delle *de iure* e *de facto disclosure*, tenendo al contempo in considerazione le interpretazioni fornite dalle diverse corti, così come del modificarsi nel tempo sia delle disposizioni normative sia dei testi delle *disclosure* prodotte da imprese o amministrazioni.

3.2.4. Costruzione degli indici di fallimento regolatorio e graduazione

Al fine di misurare le cause di fallimento delle *disclosure* in entrambi i *dataset* abbiamo elaborato cinque indici, di cui tre quantitativi e due qualitativi (F. DI PORTO, 2020). Tali sono: sovraccarico informativo; asimmetria informativa; inconsistenza e incoerenza (interna ed esterna). Per ciascuno di essi abbiamo proposto l'impiego di diversi algoritmi al fine non solo di individuarne la causa, ma anche di misurarla e quindi di graduare il testo della singola *disclosure* in base ad una scala da 0-5.

La Tabella 1 che segue sintetizza la metodologia, mentre per la discussione completa degli indici e dei relativi algoritmi, non possibile in questa sede, si rinvia ad altra sede (F. DI PORTO, 2020, cit.).

Tabella 1. – **Indici di fallimento delle *de iure* e *de facto disclosure* – Graduazione (per ambito/settore)**

Indice di fallimento	**Proxy**	**Metodologia per stabilire i casi di fallimento: *supervised* ML + varia a seconda dell'ALGO usato**
Information overload/ leggibilità	**Lunghezza del testo** (quantitativo)	***Ranking*** della clausola su uno spettro A-F, sulla base della lunghezza testo (es. se > X parole, ranking F) ALGO: SMOG, FRE, F-K
Information overload/ leggibilità	**Complessità del testo** (quantitativo)	**Sintattica**: si conta presenza di certe strutture grammaticali (nodi) e si attribuiscono punti. (es. avverbi congiuntivi, verbi modali – potrebbe, dovrebbe – ricevono più punti). ***Ranking*** della clausola su uno spettro A-F, sulla base del numero di nodi: più nodi più punti. **Semantica:** uso di termini complessi, difficili, tecnici o inusuali (detti *outliers*). ***Ranking*** su uno spettro A-F delle clausole. ALGO: LOF, CI, altro
Asimmetria informativa	**Mancanza di informazioni** (quantitativo)	Verifica assenza/presenza dell'informazione richiesta dalla norma (es. clausola di arbitrato deve identificare: autorità [A]; foro competente [LF]; giurisdizione [J]. ***Ranking*** spettro A-F (settoriale)
Consistency/ **Interna**	Collegamento tra clausole **all'interno dello stesso testo** (qualitativo)	Verifica presenza stesso lessico e riferimenti incrociati chiusi tra diverse clausole nello stesso documento. ***Ranking*** spettro A-F. ALGO: Sannier *et al.* 2017
Consistency/ **Esterna**	Collegamento tra clausole **tra diversi testi** (qualitativo)	Verifica ricorso allo stesso lessico e riferimenti incrociati chiusi tra diversi documenti. ***Ranking*** spettro A-F. ALGO: Sannier *et al.* 2017

Così costruiti gli indici di fallimento, si procede quindi a processare i documenti presenti nei due *dataset* e ad ordinarli secondo la scala ('grading') fornita. In tal modo, per ogni ambito settoriale identificato (ad esempio, *disclosure* nel settore della privacy, dei mercati finanziari, della cybersecurity,

ecc.), si otterranno coppie di testi (*de iure* e *de facto*) che, in base ai punteggi ottenuti, saranno quelli che "falliranno meno".

3.2.5. Collegamento dei dataset attraverso un grafo della conoscenza (*knowledge graph*). Graduazione ed elaborazione delle *Best Available Disclosures* (BADs)

Così preparati i testi, occorre procedere al loro collegamento. Questo passaggio rappresenta il fulcro del nostro "approccio onnicomprensivo": è pertanto necessario individuare una modalità tecnica che consenta di collegare in maniera dinamica le due *libraries*, e di procedere ad una ulteriore successiva graduazione. Allo stato ciò è possibile impiegando una ontologia/grafo della conoscenza (*knowledge graph*): questo rappresenta il modo migliore per fissare un legame tra testi che mutano nel tempo, come le norme o la giurisprudenza. Le «*legal ontologies*» (E. MONTIEL-PONSODA, V. RODRÍGUEZ-DONCEL, 2018), infatti, consentono di identificare, estrarre e formalizzare (ed anche visualizzare) concetti giuridici che sono tra loro collegati ma formalizzati in diverse fonti. Tali concetti sono visualizzati come nodi, mentre le connessioni ad altri concetti appaiono come legami tra i diversi nodi. A questi ultimi è possibile attribuire un diverso peso, in modo che la loro rilevanza possa aumentare o ridursi a seconda delle mutate circostanze (ad esempio, se una norma viene abrogata il peso del nodo diminuirà).

Nel nostro caso l'ontologia verrà usata per collegare la clausola della *de iure disclosure* con la corrispondente *de facto disclosure*, creando così una rete di nodi semantici collegati. Inoltre, il *knowledge graph* potrà essere ingrandito in qualsiasi momento mediante l'aggiunta di ulteriori nodi. In tal modo, la sua struttura risulterà costantemente aggiornata ed espansa per accomodare nuovi dati (ad esempio una nuova pronuncia giurisprudenziale) e riflettere sviluppi giuridici recenti.

Una volta ultimato il collegamento tra i due *dataset*, occorrerà attribuire i pesi ai nodi del *knowledge graph* che riflettano i "voti" assegnati agli indici di fallimento (*supra* par. 3.2.4). In questo modo, saremo in grado di classificare i testi collegati secondo un *ranking*, così da individuare, ancora una volta, quelli che, per ciascun indice di fallimento, ottengono il miglior punteggio (o, che è lo stesso, falliscono meno).

In altri termini, otterremo dei *linked-text* che denomineremo Best Available *Disclosure*s o BADs. Le BADs possono pertanto definirsi come una *legal ontology* costituita da testi collegati fatti da tutte quelle norme (obblighi informativi), collegate alle loro migliori attuazioni e chiarite dalla giurisprudenza che, secondo un approccio onnicomprensivo, falliscono meno (cioè determinano minore asimmetria informativa, sovraccarico informativo, e così via).

3.3. Fase 2. Integrare il dato comportamentale usando le *regulatory sandbox*: le *Best Ever Disclosures* (BEDs)

Come anticipato, la seconda fase della produzione normativa algoritmica consiste nell'integrare i dati comportamentali nell'algoritmo mediante la partecipazione di individui reali. La ragione di procedere a questa seconda fase è triplice. In primo luogo, occorre verificare l'efficacia della semplificazione dei testi operata nella Fase 1. In secondo luogo, non esiste allo stato una sola tecnologia che consenta di considerare dati comportamentali e testuali in un unico contesto, ma occorre procedere per fasi successive. In terzo luogo, occorre legittimare l'algoritmo a produrre norme, cosa che solo la presenza umana insopprimibile può fare.

3.3.1. Le *disclosure* prodotte attraverso l'algoritmo BADs non sono "*targeted*", differenziate, né proporzionate

In linea con l'approccio onnicomprensivo qui proposto, pertanto, le *disclosure* BADs debbono essere testate con persone reali per appurarne l'abilità a modificare il comportamento dei destinatari dell'informazione finale. Come detto più volte, gli esperimenti volti a determinare questa occorrenza non dovrebbero essere occasionali, ma condotti in tempo reale ed essere altresì ripetuti (come richiesto dallo European Data Protection Board – già Art. 29 Working Party, nelle linee guida sulle decisioni individuali automatizzate del 6 febbraio 2018).

Inoltre, un modo per aumentarne l'efficacia è usare *targeted disclosure*, ossia indirizzare diverse informazioni a diversi gruppi di destinatari che presentano capacità e preferenze omogenee al loro interno (F. DI PORTO, M. MAGGIOLINO, 2019). Le tecnologie algoritmiche si prestano infatti a supportare i regolatori nel disegno di simili *disclosure*. Esse possono infatti essere differenziate (anziché omogenee come sono ora) non solo in termini di contenuto grafico/testuale, ma anche in ragione di tempistica, ossia del momento in cui il messaggio viene rappresentato al destinatario (ad esempio: ciò può avvenire prima dell'inizio della transazione – come accade attualmente per termini e condizioni – prima della prima interazione e ripetuta al momento della conclusione della transazione, ecc.). Questa differenziazione mira a rendere le *disclosure* meno prone al fallimento (F. Di Porto, 2018). Tuttavia, perché non risulti capricciosa o arbitraria, essa deve farsi per gruppi omogenei e ampi di destinatari (escludendo cioè le *personalized disclosure*: STRAHILEVIZ, PORAT, cit.) e in maniera conforme al principio di proporzionalità.

3.3.2. Le BADs sono algoritmi e gli algoritmi non sono legittimati a produrre norme

In secondo luogo, ammesso che a livello teorico l'impiego di algoritmi per il disegno delle *disclosure* possa rafforzarne la proporzionalità (nella misura in cui esse siano indirizzate a gruppi omogenei e non ad individui), molto resta da dire sulla legittimità dell'uso di questi strumenti per produrre obblighi informativi, che sono norme. Poiché l'algoritmo non dispone di legittimazione democratica, non è possibile delegare ad esso *sic et simpliciter* poteri regolatori.

Per sopperire a tale carenza è tuttavia possibile ricorrere a quella procedurale, assicurando un certo grado di trasparenza e di partecipazione delle parti coinvolte nella produzione delle *disclosure* algoritmiche. Tradurre queste garanzie procedimentali di trasparenza e partecipazione in ambiente algoritmico significa che due cose sono insopprimibili: la presenza umana e, conseguentemente, l'integrazione dei dati comportamentali prodotti all'interno dell'algoritmo. Non si ritiene invece che la «piena conoscibilità del codice sorgente» dell'algoritmo (condizione di trasparenza richiesta, come noto, dalla giurisprudenza amministrativa nazionale: T.A.R. Lazio, sez. III-*bis*, 22 marzo 2017, n. 3769) sia di utilità a fini di legittimazione: qui si discorre infatti di algoritmi di *machine-learning*, che cioè auto-apprendono (a differenza del caso che ha dato origine alla sentenza menzionata: L. CASINI, 2020).

3.3.3. Esplorare le potenzialità delle *Regulatory Sandboxes*

Affinché ciò sia tecnicamente possibile, ovverosia per rispondere alle richieste di legittimazione della produzione normativa algoritmica nell'ambito che qui si discute, la proposta è quella di esplorare le potenzialità delle cosiddette *Regulatory Sandboxes* (o RS) (C.-Y. TSANG, 2019). Esistono diversi tipi di RS, ciascuna con proprie regole di funzionamento (P.G. PICHT, G.T. LODERER, 2018); tuttavia, esse hanno alcuni tratti comuni, come il fatto di pre-testare regole e tecnologie con individui reali in ambienti protetti prima della loro diffusione su larga scala (Commissione Europea, 2019).

Un altro tratto comune è il fatto di promuovere la collaborazione tra il regolatore, che normalmente prende l'iniziativa, e gli *stakeholder* per preservare l'innovazione e sperimentare nuove formule per produrre le regole (TSANG cit.; D. YANG & M. LI, 2018).

La proposta che intendo qui avanzare è dunque quella di usare il modello della RS dove, sotto gli auspici del regolatore (a livello Europeo, la Commissione o a una Autorità europea dei dati (qualora istituita); a livello nazionale, il singolo regolatore settoriale ovvero il legislatore, in entrambi i casi coadiuvati da AgID e dalla Presidenza del Consiglio dei Ministri competente per lo sviluppo della menzionata Piattaforma Digitale Nazionale Dati), imprese e desti-

natari delle informazioni si incontrano in gruppi sperimentali per "allenare" l'algoritmo BADs e sviluppare le *disclosure*.

Sul piano tecnico, la RS serve per raccogliere i dati comportamentali degli attori rilevanti (ovverosia del regolatore, dell'impresa – o amministrazione – che fornisce l'informazione, del destinatario della stessa, dei tecnici) affinché si possa testare l'efficacia dei diversi testi e formati delle *disclosure* nel supportare le decisioni degli individui reali. Questi dati saranno registrati e alimenteranno l'algoritmo al fine di elaborare le *disclosure* differenziate, le quali, come detto, saranno indirizzate ai diversi gruppi di destinatari in modo dinamico e significativo. Ovverosia: ciascun gruppo riceverà un tipo di messaggio diverso a seconda delle proprie preferenze; e al cambiare di queste muterà automaticamente il primo. Ad esempio, anziché visualizzare un solo modulo privacy prima di accedere ad un servizio, l'utente ne visualizzerà tre (solo grafico, solo testuale denso e un mix dei due), potendo scegliere quello che risulterà, in base alle proprie preferenze più semplice recepire.

A mano a mano che il BADs è alimentato con dati comportamentali (SUSSER *et al.*, cit., p. 6; C. GOANTA, J. SPANAKIS, 2020) sulle reazioni degli individui reali (in formato anonimizzato), sarà possibile selezionare i formati più efficaci per ciascun gruppo. Così facendo, cioè ripetendo sessioni successive di test comportamentali si giungerà a selezionare quei testi e formati non solo differenziati e "*targeted*" ma anche capaci di soddisfare i bisogni informativi dei destinatari prima di essere adottate su larga scala: si tratta di quelle che definiremo le *Best Ever Disclosures* o BEDs.

Per tornare al tema della legittimazione, l'impiego della RS ben si presta ad assicurare un certo grado di partecipazione dei soggetti coinvolti nell'intervento regolatorio e di trasparenza dello stesso. Per ciascuna clausola vi è infatti contraddittorio tra i partecipanti al procedimento di normazione algoritmica.

A ben vedere si tratta infatti di una declinazione del modulo del *notice and comment*, già impiegato per le autorità indipendenti. In primo luogo, la fase di *testing* delle BADs avviene in maniera cooperativa tra regolatore, operatori e destinatari (con l'assistenza di esperti tecnici *data scientist* indipendenti); in secondo luogo, poiché sia il procedimento regolatorio (cioè la definizione progressiva delle *disclosure* algoritmiche) sia la regola che ne costituisce il prodotto sono aperti alla partecipazione delle imprese, amministrazioni e individui, esso assicura una trasparenza, senza richiedere l'uso né la pubblicazione dei codici sorgente degli algoritmi di titolarità delle imprese.

Lo sviluppo di BADs e BEDs si basa difatti su algoritmi già disponibili (quelli che ho qui proposto) ovvero facilmente sviluppabili da parte dell'amministrazione (o del regolatore) sulla base di tecniche reperibili *online* (e spesso *open source*; si veda ad esempio l'elenco delle *legal ontologies* disponi-

bili: http://www.lynx-project.eu/data2/reference-ontologies).

A ciò si aggiunga la disposizione di cui all'art. 36, D.L. n. 76/2020 (DL-semplificazioni conv. in l. 120/2020, cit.) che, proprio al fine di incentivare «sperimentazione di idee e iniziative» innovative in ambito tecnologico e di digitalizzazione «volte al miglioramento della competitività, dell'efficienza e dell'efficacia di servizi a cui cittadini e imprese» consente di richiedere – in sede di presentazione del progetto – la temporanea deroga a norme che eventualmente impediscano la sperimentazione. Si tratta evidentemente di un'importante disposizione, che potrebbe tradursi in un incentivo per le imprese che intendano partecipare alla sperimentazione algoritmica (ad esempio, prevedendo un *safe harbor* dalle norme sulle pratiche commerciali scorrette).

3.3.4. Usare il Knowledge Graph/Ontologia per "allenare" l'algoritmo BEDs

Sul piano tecnico, come per le BADs, anche per arrivare a selezionare le BEDs, ci si avvarrà di un *knowledge graph* (R. BENJAMINS, 2005). Il processo inizia pertanto con tre *library*: due saranno i *database* testuali ('linked-database') collegati nel BADs, i quali verranno arricchiti con i dati provenienti dalla RS (per avere un'idea di come funzionano i grafi della conoscenza, si v. D. CAVAR, J. HERRING e A. MEYER, 2018). Nel *knowledge graph*, i dati testuali e comportamentali saranno integrati avvalendosi della esperienza degli utilizzatori: in pratica i partecipanti alla RS forniranno risposte (dati comportamentali) che confermano (o negano) una certa clausola o testo, in tal modo rinforzando i nodi e via via i legami all'interno del grafo.

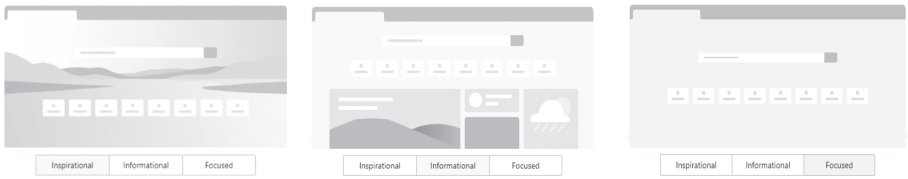
Nella pratica, la tecnologia del *knowledge graph* sarà impiegata per raffinare l'algoritmo BADs svolgendo i seguenti task:

i) si parte dai testi collegati presenti nel BADs,
ii) li si memorizzano,
iii) li si annotano (attraverso una ontologia),
iv) si costruisce una griglia di concetti giuridici, specifici di un settore (ad esempio, trasparenza nel settore finanziario, i modelli della privacy).

Questo processo deve essere ripetuto per più sessioni finché si giunge al punto in cui tutti i partecipanti alla RS sono il più possibile soddisfatti (o meno insoddisfatti possibile).

Il risultato di questo procedimento regolatorio potrebbe somigliare a quello rappresentato in Fig. 1, ove l'obbligo informativo è diverso in base a tre gruppi omogenei di soggetti, indicati come "Creativo" (gruppo intermedio); "Informativo" (gruppo che riceve informazioni dettagliate e complete); "Focalizzato" (che riceve informazioni essenziali e super-semplificate).

Figura 1. – **Esempio di format di *disclosure* algoritmica differenziata e *targeted***



Creativo
Puoi sempre cambiare questa scelta nelle Impostazioni

Informativo
Puoi sempre cambiare questa scelta nelle Impostazioni

Focalizzato
Puoi sempre cambiare questa scelta nelle Impostazioni

Fonte: *Microsoft Edge*, Agg.to giugno 2020.

3.4. Adozione delle *Best Ever Disclosures* – BEDs su larga scala

A conclusione della fase di *testing* nella RS, l'algoritmo BEDs sarà in grado di produrre obblighi-*disclosure* dinamici, differenziati e targettizzati a differenti gruppi, pronti per essere attuati su larga scala. Una volta lanciato sul mercato l'algoritmo regolatorio (denominazione dal sapore tautologico, essendo di per sé l'algoritmo un insieme di istruzioni o regole, ma al giurista potrà non suonare tale), i destinatari dell'informazione (in ipotesi i consumatori) saranno collocati automaticamente nel gruppo intermedio (quello "Creativo" nella Fig. 1). Tuttavia, essi potranno liberamente cambiare gruppo e scegliere l'opzione di *disclosure* che preferiscono.

Abbiamo definito queste norme obblighi-*disclosure* perché in effetti le *disclosure* algoritmiche non necessitano di attuazione, almeno non nel senso tradizionale. L'esito principale di tutto questo procedimento è infatti il venir meno della fase attuativa da parte dell'industria o della amministrazione (nel caso della trasparenza amministrativa). Altrimenti detto, le BEDs sono automaticamente attuabili semplicemente trasmettendo le specifiche algoritmiche al destinatario (intermedio) dell'obbligo. Ciò sarà possibile tecnicamente ma anche giuridicamente, dal momento che il procedimento partecipato e trasparente che abbiamo descritto è settoriale (ve ne sarà uno per le *disclosure* finanziarie, con i relativi stakeholder, uno per quelle in campo energetico, o dei trasporti e così via) e che i dati testuali (le norme e le sentenze) e comportamentali di cui nutre si aggiornano continuamente.

Ciò chiaramente determina un enorme risparmio di tempo e costi tanto per il regolatore quanto per l'industria/amministrazione. Ma è altrettanto evidente che non ogni elemento delle *disclosure* sarà auto-esecutivo; sibbene solo ciò che, passando per la RS, ne riceve il *placet*.

Diverso il discorso per le "modifiche" alle *disclosure* algoritmiche. Queste infatti nasceranno in un'epoca in cui le *disclosure* algoritmiche saranno già una realtà. Giocoforza, esse potranno farsi direttamente nella *regulatory sandbox* (cioè nel solo procedimento normativo algoritmico) ed essere attuate in maniera automatica. In altri termini, tutti gli emendamenti che i partecipanti alla *sandbox* negoziando accetteranno – e il regolatore sugellandole certificherà – potranno diventare direttamente applicabili (mediante la pubblicazione delle specifiche) da parte delle imprese/amministrazioni, in quanto saranno pre-testate nella *sandbox*. Ancora una volta, ciò sarà in linea con le *best practice* individuate dalle Linee guida del European Data Protection Board (cit.), ad avviso del quale ogni modifica all'algoritmo deve non solo essere testata, ma i relativi dati devono «feedback into the algorithm to ameliorate it».

4. Discussione: incentivi ed effetti attesi dall'introduzione delle BEDs

Posto che la Fase 1 non richiede una partecipazione attiva delle imprese né dell'amministrazione interessata dall'obbligo informativo, le maggiori criticità per l'attuazione della regolazione algoritmica possono sorgere nella realizzazione della Fase 2.

Perché le imprese dovrebbero voler partecipare alle RS invece di continuare a produrre le (pur costose) *disclosure*? Potrebbe essere preferibile per esse mantenere segrete le proprie strategie informative (pur nei ristretti margini lasciati dagli obblighi informativi) anziché condividerle con propri concorrenti o coi regolatori. Inoltre, non tutte le imprese (per ora) fanno uso di tecnologie algoritmiche o sono presenti attivamente (fanno marketing) sui mercati digitali. Ciò ne impedirebbe la partecipazione attiva alle RS, con conseguente limitata rappresentatività e quindi perdita di legittimità della stessa *sandbox*. Da ultimo, vi sono industrie nelle quali il bisogno informativo collettivo è incompatibile con la differenziazione e la targetizzazione, pure se per gruppi di individui o *cluster*. È questo il caso dell'industria farmaceutica: il "bugiardino", almeno nella parte delle indicazioni terapeutiche o delle controindicazioni non si presta a riduzioni testuali (ma solo eventualmente a semplificazioni semantiche e grafiche, già peraltro in atto) o a rese esclusivamente grafiche.

Se quest'ultima obiezione è (correttamente) insuperabile, molto si può fare sulle precedenti. Un modo per incentivare la partecipazione degli operatori digitali, non solo alla prima formazione dell'algoritmo BEDs, ma continuativamente, è quello di stabilire un *safe harbor* per tutte le imprese che accettano preventivamente i termini e le condizioni delle *disclosure* accettati dai partecipanti alla RS (oltre ai successivi emendamenti). Esse cioè non saranno ritenute

responsabili per questioni attinenti una clausola se questa è stata concordata dalla RS e l'impresa la ha recepita *telle quelle*. Chiaramente la prova contraria sarà sempre ammissibile. Ma è innegabile l'impatto deflattivo sulla giustizia di un siffatto meccanismo, almeno su questioni bagatellari.

Più in generale, sul piano reputazionale, l'impresa che partecipa al progetto BEDs può dimostrare di impegnarsi in attività pro-consumer. Non ultimo, le *disclosure* algoritmiche determinano un innegabile risparmio di costi per l'industria, non solo di scrittura, ma anche di aggiornamento continuo delle stesse, che diventerebbe automatico.

Per quanto attiene ai consumatori, un possibile rischio delle *disclosure* algoritmiche è che esse possano finire con «offering finite choices to users effectively forc[ing them] to guess the category under which their information falls» (D.K. CITRON, 2004). Inoltre, può ben accadere che, per ragioni che non siamo in grado di prevedere, le *disclosure* algoritmiche, ancorché differenziate e indirizzate a target di destinatari omogenei non producano alcuna modifica nelle scelte. Tuttavia, pur ammettendo che questo sia, avremmo bisogno di raccogliere evidenze empiriche di tale evenienza, ciò che è esattamente l'obiettivo di questo progetto.

Per quanto infine attiene al lato del regolatore, occorre stabilire quale sia l'autorità cui attribuire la responsabilità di (co-)disegnare e monitorare l'applicazione della regolazione algoritmica.

Come noto, in Italia non esiste una Autorità preposta alla *governance* dell'Intelligenza Artificiale o degli algoritmi, mentre sarebbe auspicabile la sua istituzione.

Si può tuttavia ragionare *medio tempore*. Nel modello proposto delle *disclosure* algoritmiche, essendo le stesse di tipo settoriale, il regolatore "principale" (cioè che prende l'iniziativa) sarà, ogni volta, quello responsabile del tema (ad esempio, dovendo definire le *disclosure* in campo energetico, l'iniziativa sarà assunta da ARERA, che convocherà la *regulatory sandbox*). In quello finanziario, la Consob; ove assente un regolatore settoriale, la responsabilità potrebbe ricadere, almeno in via istruttoria preliminare, su una commissione parlamentare. Resta fermo che gli altri regolatori (si pensi al Garante privacy, o all'AGCom) parteciperanno in ragione delle rispettive competenze. A ben vedere, tuttavia, se questa soluzione risolve i problemi a livello nazionale, dove è relativamente agile attribuire ai regolatori domestici la responsabilità di guidare il processo di produzione algoritmica delle *disclosure*, v'è da chiedersi se a livello europeo la Commissione goda del medesimo supporto politico per intraprendere l'iniziativa (posto che disporrebbe dei poteri).

Innegabili sono invece i benefici che deriverebbero al regolatore dal promuovere la regolazione algoritmica, primo fra tutti un recupero di fiducia da

parte dei consumatori e delle imprese/amministrazioni. Lo si è detto più volte, le *disclosure* algoritmiche hanno come obiettivo di massimizzare (o almeno recuperare terreno alla) autonomia individuale a fronte del rischio di delega "in bianco" alla macchina. E ciò fanno promuovendo schemi regolatori collaborativi, che passano attraverso moduli trasparenti e tracciabili.

I tempi sono maturi affinché il regolatore, che certo non può trasformarsi in un ibrido tecno-giurista, secondo i dettami della importante scuola del *Law&Tech*, che pure vanno seguiti attentamente e appresi, possa almeno guidare i processi tecnologici con umana sapienza.

Bibliografia

ASHLEY K.D., KEVIN D., *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in The Digital Age*, Cambridge University Press, 2017.

AYRES I., SCHWARTZ A., *The No-Reading Problem in Consumer Contract*, in *Law Stanford Law Review*, 2014, 66, p. 3.

BOELLA G., DI CARO L. & LEONE V., *Semi-automatic knowledge population in a legal document management system*, in *Artificial Intelligence and Law*, 2019, 27(2), p. 228.

BEN-SHAHAR O., PORAT A., *Personalizing Negligence Law*, in *New York University Law Review*, 2016, 91(3), p. 627.

BENJAMINS R. (a cura di), *Law and the semantic web: legal ontologies, methodologies, legal information retrieval, and applications. Lecture notes in artificial intelligence*, 1st ed., Springer, Berlin-New York, 2005, p. 116.

BIAGIOLI C. *et al.*, *Automatic Semantics Extraction in Law Documents*, in *Proceedings of the 10th International Conference on Artificial Intelligence and Law – ICAIL '05, 133. Bologna, Italy*, ACM Press, 2005, pp. 253-266.

BUSCH C., *The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data*, in C. TWIGG-FLESNER (a cura di), *Research Handbook on EU Consumer and Contract Law*, Edward Elgar Pub, 2016, p. 221.

BRAYNE S., CHRISTIN A., *Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. Social Problems*, 2020, 20(0), pp. 1-17.

CASINI L., *Lo stato nell'era di Google*, Mondadori, Milano, 2020.

CAVAR D., HERRING J., MEYER A., *Law Analysis using Deep NLP and Knowledge Graphs. Presented at the Proceedings of the LREC 2018 "Workshop on Language Resources and Technologies for the Legal Knowledge Graph"*, Miyazaki, Japan, 2018.

CITRON D.K., *Technological Due Process*, in *Washington University Law Review*, 2008, 85(6), pp. 1249-1314.

COGLIANESE C., *Transparency and Algorithmic Governance. Public Law and Legal Theory. University of Pennsylvania Research Paper Series No.* #18-38. April 18 2019.

COMMISSIONE EUROPEA, *30 Recommendations on Regulation, Innovation and Finance. Final Report of the Expert Group on Regulatory Obstacles to Financial Innovation* (ROFIEG), December 2019, p. 71.

DERLÉN M., LINDHOLM J., *Is it Good Law? Network Analysis and the CJEU's Internal Market Jurisprudence*, in *Journal of International Economic Law*, 2017, 20(2), pp. 257-277.

DEVINS C., FELIN T., KAUFFMAN S., KOPPL R., *The Law And Big Data*, in *Cornell Journal of Law and Public Policy*, 2017, 27, p. 366.

DI PORTO F., *From BADs to BEDs. Algorithmic Disclosure regulation. Theoretical Aspects for Empirical Application*, in The Hebrew University Legal Studies Research Paper Series, 2020.

DI PORTO F., *In Praise of an Empowerment Disclosure Regulatory Approach to Algorithms. IIC – International Review of Intellectual Property and Competition Law*, 2017, 49, pp. 507-511.

DI PORTO F., *La disciplina degli obblighi informativi. La sfida delle scienze cognitive e dei big data*, Edizioni Scientifiche, Napoli, 2017.

DI PORTO F., MAGGIOLINO M., *Algorithmic Information Disclosure by Regulators and Competition Authorities*, in *Global Jurist*, 2019, 19(2), p. 1.

EPSTEIN L., MARTIN A., *Quantitative approaches to empirical legal research*, in *The Oxford handbook of empirical legal research*, Oxford University Press, Oxford, 2010.

ESMA, EBA, and EIOPA, JC 2018 74, *FinTech: Regulatory Sandboxes and Innovation Hubs*, 2019.

FAGAN F., *Big Data Legal Scholarship: Toward a Research Program and Practitioner's Guide*, in *Virginia Journal of Law & Technology*, 2016, 20(1), pp. 1-81.

GOANTA C., SPANAKIS J., *Influencers and Social Media Recommender Systems: Unfair Commercial Practices in EU and US Law*, in *TTLF Working Papers No. 54*, 2020.

HACKER P., *Personalizing EU Private Law: From Disclosures to Nudges and Mandates*, in *European Review of Private Law*, 2017, p. 651.

KITCHIN R., *Big Data, new epistemologies and paradigm shifts*, in *Big Data & Society*, 2014, 1(1), April-June, pp. 4-5.

LEPINA R., CONTISSA G., DRAZEWSKI K., LAGIOIA F., LIPPI M., MICKLITZ H.-W., PAŁKA P., SARTOR G., TORRONI P., *GDPR Privacy Policies*, in *Proceedings of the Third Workshop on Automated Semantic Analysis of Information in Legal Text* (ASAIL 2019), 2019, pp. 1-7.

LIPPI M. *et al.*, *CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service*. arXiv preprint arXiv:1805.01217, 2018.

LIVERMORE M.A. e ROCKMORE D.N. (a cura di), *Law as Data*. SFI, 2019.

LOWDEN R., *Risk Assessment Algorithms: The Answer to an Inequitable Bail System?* In *North Carolina Journal of Law & Technology*, 2018, 19(4), p. 221.

MEDVEDEVA M., VOLS M., WIELING M., *Using machine learning to predict decisions of the European Court of Human Rights*, in *Artif. Intell. Law* (published online), 2019, https://link.springer.com/article/10.1007%2Fs10506-019-09255-y.

MONTIEL-PONSODA E., RODRÍGUEZ-DONCEL V., *Lynx: Building the Legal Knowledge Graph for Smart Compliance Services in Multilingual Europe*, in G. REHM, V. RODRÍGUEZ-DONCEL & J. MORENO-SCHNEIDER (a cura di), *Proceedings of the 1st Workshop on LREC (Language Resources and Technologies for the Legal Knowledge Graph) Workshop*, 12 May 2018, pp. 19-22.

MOENS M.F. *et al.*, *Automatic detection of arguments in legal texts*, in *Proceedings of the 11th international conference on Artificial intelligence and law. Association for Computing Machinery*, 2007, pp. 225-230.

MORETTI F., *Conjectures on World Literature*, in *New Left Review*, 2000, 1, p. 54.

OLSEN H.P. e KÜÇÜKSU A., *Finding hidden patterns in ECtHR's case law: On how citation network analysis can improve our knowledge of ECtHR's Article 14 practice*, in *International Journal of Discrimination and the Law*, 2017, 17(1), pp. 4-22.

PANAGIS Y., SADL U., TARISSAN F., *Giving every case its (legal) due. The contribution of citation networks and text similarity techniques to legal studies of European Union law. Paper presented at the 30th international conference on Legal Knowledge and Information Systems*, JURIX 2017, Luxembourg. December 2017.

PICHT P.G., LODERER G.T., *Framing Algorithms – Competition Law and (Other) Regulatory Tools*, in *MPI Research Paper*, No. 18-24, 2018.

PORAT A., STRAHILEVITZ L., *Personalizing Default Rules and Disclosure with Big Data*, in *Michigan Law Review*, 2013, 122, p. 1417.

RANCHORDÁS S. VAN M., *Future-Proofing Legislation for the Digital Age. University of Groningen Faculty of Law Research Paper Series No.* 36/2019.

RANGONE N., *Semplificazione ed effettività dei controlli sulle imprese*, in *RTDP*, 2019, 3, p. 883.

RICH M.L., *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, in *University of Pennsylvania Law Review*, 2016, 164(4), pp. 871-929.

SHULAYEVA O. *et al.*, *Recognizing cited facts and principles in legal judgements*, in *Artificial Intelligence and Law*, 2017, 25(1), pp. 107-126.

SPAETH H.K., EPSTEIN A.D. *et al.*, Supreme Court Database, Version 2016 Release 01 (http://scdb.wustl.edu/about.php?s=1).

SUSSER D., ROESSLER B., NISSENBAUM H., *Technology, autonomy, and manipulation*, in *Internet Policy Review*, 2019, 2.

TSANG C.Y., *From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of Fintech. Comparative Corporate Governance Conference, Singapore*, January 24, 2019, p. 359.

YANG D., LI M., *Evolutionary Approaches and the Construction of Technology-Driven Regulations*, in *Emerging Markets Finance and Trade*, 2018, 54(14), p. 3266.

X.

GLI *SMART LEGAL CONTRACTS*: PROSPETTIVE PER L'IMPIEGO NEL SETTORE PUBBLICO-PRIVATO

Benedetta Cappiello e Gherardo Carullo [*]

SOMMARIO: 1. Introduzione. – 2. *Smart contract* e *smart legal contract*: un confronto. – 3. Lo *smart legal contract* nelle legislazioni nazionali: tentativi di qualificazione. – 4. La normativa internazional-privatistica e lo *smart legal contract*. – 5. La Pubblica Amministrazione e lo *smart legal contract*: prospettive applicative.

1. Introduzione

Attualmente si sta assistendo all'ampia diffusione di un nuovo strumento, il c.d. *smart contract*, grazie al quale nel settore privato sono già state implementate numerose nuove soluzioni, quali ad esempio le c.d. Distributed Apps (DApps), ovvero strumenti di risoluzione alternativa delle controversie.

Gli *smart contract*s sono sviluppati con l'impiego della tecnologia blockchain, sicché tutti i relativi dati sono memorizzati su di un registro distribuito (v. capitolo VI, G. CARULLO). Concretamente, lo *smart contract* è un software che rende automatica l'esecuzione degli input-comandi sul medesimo prescritti. I comandi dovrebbero coincidere con le obbligazioni che le parti del rapporto si assumono; lo *smart contract* dovrebbe pertanto rendere automatica l'esecuzione di obblighi contrattualmente pattuiti.

Considerato il notevole rilievo che questa tecnologia sta avendo nel settore privato, ci si può senz'altro domandare se, ed in che misura, questo nuovo strumento possa essere utile anche per le pubbliche amministrazioni, e, in tal caso, quali applicazioni in concreto possano essere immaginate.

---

[*] Alla dott.ssa B. CAPPIELLO sono attribuibili i parr. da 1 a 4 inclusi. Mentre al dott. G. CARULLO si deve il par. 5.

Occorre tuttavia premettere che la natura giuridica degli *smart contract*s è ancora dubbia o, più propriamente, è dubbio se, e a quali condizioni, i predetti strumenti producano effetti giuridici. Ovviamente, ci si riferisce al quadro giuridico dell'ordinamento nel quale il regolamento contrattuale *smart* dovrebbe produrre i propri effetti. I dati del codice informatico dello *smart contract* acquisiscono infatti una propria idoneità giuridica nella misura in cui, a monte, si riconosce che i dati raccolti, e distribuiti, attraverso la blockchain producono effetti giuridici. Non è dunque scontato se, e in qual misura, i c.d. *smart contract* possano essere assimilati (e disciplinati) alla stregua di contratti tradizionali.

2. *Smart contract* e *smart legal contract*: un confronto

La diffusione dello *smart contract* è, come detto, correlata alla tecnologia blockchain nel senso che tale strumento ha avuto – e continua ad avere – largo impiego proprio grazie alla tecnologia alla base che ne permette lo sviluppo e l'esecuzione. La certezza, la trasparenza e l'immutabilità delle transazioni operate su blockchain parrebbero infatti rendere lo *smart contract* una risorsa assai idonea a rispondere alle necessità degli operatori economici.

Lo strumento è di sicuro interesse anche perché rappresenta un "fenomeno sociale": lo *smart contract* risulta particolarmente diffuso, pur nelle more di un intervento legislativo – nazionale e sovranazionale – che ne chiarisca i termini di utilizzo e gli effetti. La sicurezza nei processi operativi, così come l'affidabilità nel funzionamento della tecnologia, sembrano del resto essere condizioni sufficienti a indurre le parti a vincolarsi attraverso la sottoscrizione di uno *smart contract*. Il *medium* sembra dunque divenire strumento per superare la c.d. asimmetria informativa che è propria di ogni transazione economica (L. STOUT, 2010). Sarebbe quindi il senso di fiducia verso la tecnologia ad assumere un ruolo primario nell'indurre le parti medesime a stringere una relazione economica (R. POSNER, 1977). Le parti entrano in relazione prescindendo da chi è, da dove viene la "controparte", e da "chi" garantisce la prestazione. Ciascun utente può infatti impiegare la tecnologia blockchain rimanendo pseudo anonimo se non addirittura, almeno potenzialmente, anonimo. Si tratta del c.d. No-Party Trust (W. WERBACH, 2018).

Posto ciò, la questione sulla quale occorre soffermarsi è se, e in quale misura, uno *smart contract* produca effetti giuridici divenendo uno *smart legal contract*. Prima di procedere un *caveat*: le condizioni perché si possa parlare di *smart legal contract* cambiano, inevitabilmente, in ragione dello Stato all'interno del quale ci si pone. Ciascuno si dota, infatti, del proprio diritto contrattuale, definendo le condizioni in presenza delle quali si possa parlare di un

contratto. Con questa consapevolezza, esaminiamo la materia in termini generali, non trascurando qualche richiamo alla normativa interna, al sol fine di arricchire l'analisi di esempi concreti.

I primi modelli di *smart contract* diffusi sono stati implementati dalla piattaforma Ethereum i cui Sviluppatori, nel White Paper hanno sancito che lo *smart contract* non è necessariamente correlato al concetto classico di contratto, ma può essere qualsiasi tipo di programma per computer.

Per parte nostra, prima di procedere alla qualificazione dello strumento, è utile interrogarsi sulla natura dello *smart contract*, partendo proprio dalla scelta del nome.

L'appellativo "smart" deriverebbe dal fatto che la tecnologia sottostante a tale strumento ne permetterebbe l'esecuzione automatica (G. JACCARD, 2018; J. STARK, 2015). I codici che compongono lo *smart contract* contengono infatti, come detto, comandi che si auto eseguono in presenza di determinate circostanze. Si tratta della struttura condizionale basata sulla relazione "If-then" ("se-allora"). Proprio la possibilità di un'esecuzione automatica sarebbe la caratteristica idonea a rendere per gli operatori economici tali strumenti preferibili a quelli tradizionali. La auto esecuzione darebbe, infatti, alle parti la certezza che la prestazione da loro disciplinata si eseguirà nel modo prescritto nel software-*smart contract*, evitando così il sorgere di controversie e, per esse, l'intervento di un giudice.

Se il discorso si riducesse alla sola auto eseguibilità dello strumento, la nostra analisi dovrebbe fermarsi qui, tenuto conto che lo *smart contract* verrebbe semplicemente qualificato come uno strumento di esecuzione, non già di regolamentazione di una fattispecie contrattuale. Così non può però essere poiché, come detto, qualsiasi accordo liberamente assunto tra le parti produce effetti giuridici in tanto in quanto la disciplina di cui si compone è conforme al diritto dei contratti di un dato Paese. Sotto tale profilo il termine *smart contract*, sovrapposto al termine contratto, sembrerebbe essere abusato, tenuto conto che la effettiva giuridicità degli effetti dal primo prodotti è tutt'altro che certa.

La sovrapposizione, confusione, tra il contratto tradizionale e lo *smart contract* deriva dalla presunta corrispondenza tra gli elementi essenziali del primo e gli elementi di cui si compone il secondo (ovviamente, in un dato ordinamento giuridico). Tale conclusione ha origine in una, forse semplicistica, petizione di principio: i codici informatici di cui si compone lo *smart contract* equivarrebbero alle previsioni normative di un contratto tradizionale con la conseguenza che "Code is Law" (L. LESSIG, 2000) e che lo "*Smart contract* is a legal contract" (P. DE FILIPPI, A. WRIGHT, 2018).

A nostro giudizio questa conclusione poggia su un errore concettuale: gli effetti prodotti dallo *smart contract* nella sfera privata dei contraenti non hanno necessariamente un valore giuridico. In tema di qualificazione, si impone

dunque un'analisi rigorosa delle condizioni che ciascun legislatore, interno e sovranazionale, prescrive per la sussistenza di un valido rapporto contrattuale. Nel nostro ordinamento, ad esempio, un contratto è tale se contiene gli elementi di cui all'art. 1325 c.c.; sarebbe dunque la presenza del valido consenso, dell'oggetto (determinato e determinabile), della causa (lecita), così come della forma (quando prescritta *ad substantiam)* a rendere uno *smart contract* uno *smart legal contract*, se non altro per il legislatore italiano.

Operativamente, si rende però necessario un ulteriore passaggio: per valutare la sussistenza delle condizioni su elencate occorrerà traslare i concetti dal campo analogico-digitale a quello proprio delle tecnologie a registro distribuito. Si intende così affermare che, ferma la necessità della prestazione del consenso, uno *smart legal contract* può essere validamente concluso se il legislatore riconosce, ad esempio, che il consenso può essere validamente prestato anche attraverso un nuovo *medium* tecnologico.

Di poi, ammessa almeno potenzialmente la legittimità del consenso prestato con blockchain, si potrebbero porre problemi interpretativi: diversamente da quanto accade per il linguaggio naturale, i codici dello *smart contract* hanno solo un significante, predefinito, paralizzando così l'attività interpretativa della fattispecie disciplinata. Problemi interpretativi potrebbero sorgere anche con riguardo all'oggetto: potrebbe infatti essere messo in dubbio che il token (inteso quale rappresentazione digitale di valore e/o di bene fisico, G. GREFENSTETTE, P. TAPANAINEN, 1994), equivalga a un oggetto determinato o determinabile (come prescritto, ad esempio, in art. 1346 c.c. it.).

Vi potrebbero poi essere dubbi circa l'imputabilità di diritti e di obblighi in capo alle parti: le formulazioni dei codici dello *smart contract* non coincidono con il linguaggio naturale di prassi impiegato. Concretamente, "se succede A allora B" è diverso da "se tizio consegna X kg di grano, allora Caio paga €Y". Solo nel secondo caso, le parti sembrano adottare espressamente diritti e obblighi.

Correlativamente, potrebbero sorgere altri dubbi: la tecnologia blockchain, e la (presunta) auto eseguibilità dello *smart contract*, sembrano infatti favorire la costruzione di regolamenti contrattuali incompleti, quindi inidonei a produrre effetti giuridici (S. CERRATO, 2019). L'impiego della tecnologia blockchain parrebbe infatti rendere inoperanti l'istituto dei vizi del consenso (errore, dolo, violenza), così come le eccezioni di nullità e di annullamento. Il dubbio si pone poiché il software dello *smart contract*, una volta costruito, non è più modificabile sicché, in ipotesi di (presunto) inadempimento, ovvero di consenso viziato, i rimedi predisposti dal legislatore potrebbero operare solo attraverso la sottoscrizione di un nuovo *smart contract* che giuridicamente sostituisca il precedente, adottando il rimedio più opportuno (che, in ipotesi di

inadempimento accertato, potrebbe essere conservativo o liquidatorio). In nessun caso, pare però possibile prevedere già all'interno del codice dello *smart contract* originario i rimedi in caso di inadempimento o di vizi del consenso.

Posto ciò, sembra che nessuno dei dubbi su esposti sia tale da escludere la giuridicità degli effetti prodotti dallo *smart contract* potendo così parlare di *smart legal contract*. Si tratta, piuttosto, di adattare gli strumenti giuridici tradizionali a quelli diversi per forma ma non, necessariamente, per sostanza. Il legislatore, nazionale e internazionale, è dunque chiamato a interrogarsi sulle modalità attraverso le quali sussumere i nuovi strumenti nel quadro giuridico esistente.

3. Lo *smart legal contract* nelle legislazioni nazionali: tentativi di qualificazione

Lo *smart contract* manca di una definizione giuridica unanimemente accolta; le Organizzazioni Internazionali che ne avrebbero titolo, nonché interesse, (UNCITRAL, Conferenza dell'Aja di diritto internazionale privato) così come le Organizzazioni sovranazionali (si pensi all'Unione Europea) non hanno ancora assunto una posizione comune. Lo stesso vale per gli Stati: quelli che hanno sino ad ora adottato una politica nel settore delle tecnologie a registro distribuito, hanno infatti assunto posizioni difformi.

In estrema sintesi, è possibile distinguere due approcci: alcune normative hanno semplicemente assimilato lo *smart contract* a un software informatico in grado di auto eseguire i comandi nel medesimo registrati; altre vanno invece oltre, riconoscendo espressamente la natura giuridica contrattuale di tale strumento, presenti determinate condizioni.

Per quanto riguarda l'Italia, il legislatore ha introdotto nel D.L. n. 135/2018 l'art. 8-*ter* in cui al primo comma è prescritto che: «si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».

Il legislatore italiano ha quindi definito giuridicamente le tecnologie a registro distribuito, qualificando al contempo i dati nelle medesime registrati e conservati. Il legislatore avrebbe forse potuto essere più preciso nella scelta terminologica. Nel citato testo si legge, infatti, che il registro distribuito è "convalidato". Non è chiaro però, se la convalida riguardi il contenuto del dato ovvero il

meccanismo attraverso cui il dato è registrato (senza esser stato manipolato da terzi). In tale ultima ipotesi, il registro distribuito si limiterebbe a certificare il tempo e il modo in cui un dato è stato prodotto, non già il suo contenuto. Se così fosse, si tratterebbe di una evoluzione di scarso rilievo, tenuto conto che il legislatore ha già riconosciuto validità giuridica alla firma elettronica e digitale nonché alla posta elettronica certificata (PEC) (v. capitolo VII, S. D'ANCONA e P. PROVENZANO). Il legislatore italiano ha peraltro riconosciuto valore certo anche al contenuto della PEC, non solo alla data e all'ora, come viceversa sembra attualmente previsto nell'art. 8-*ter* in commento.

Il secondo comma della norma in commento prescrive invece che «si definisce "*smart contract*" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli *smart contracts* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto».

Lo *smart contract* è dunque identificato alla stregua di un programma informatico che, quando eseguito, vincola le parti. Tale affermazione solleva qualche quesito giuridico: se lo *smart contract* equivale a un programma informatico allora tale strumento sarebbe soggetto alla disciplina relativa alla tutela del software, vincolando in parte l'autonomia dei contraenti, che potrebbero essere chiamati a sottoscrivere una licenza per l'uso del software. Il comma in esame precisa poi che gli effetti prodotti dallo *smart contract* sono giuridicamente vincolanti; il limite della previsione è che essa si concentra sugli effetti, non già sulla validità del vincolo *inter partes* sottoscritto, ossia sullo *smart contract* medesimo. Rimane quindi dubbio se il dato formalmente inserito nello *smart contract* abbia validità giuridica.

Sempre a livello italiano, ricordiamo che il 28 giugno 2019 con Legge n. 58/2019, il legislatore ha convertito il D.L. 30 aprile 2019, n. 34, introducendo nell'art. 36.2 una novità fondamentale per il settore delle nuove tecnologie. La previsione dispone che nei giorni 90 successivi all'entrata in vigore del testo, dovrà essere predisposta una disciplina idonea a definire le condizioni e i metodi di esercizio per qualsiasi attività Fintech (purché circoscritta a un periodo di sperimentazione). Si tratta di un c.d. Sandbox ossia di una zona normativamente "franca", all'interno della quale determinati soggetti (persone fisiche o giuridiche) possono – d'intesa con il Governo dello Stato interessato – sperimentare progetti nel settore Fintech. All'interno del citato Sandbox possono operare anche le aziende che si occupano di sviluppare e così impiegare *smart contract*.

Nel Regno Unito è stata istituita la UK Jurisdiction Taskforce (UKJT) che,

il 9 maggio 2019, ha attivato una consultazione per definire e rendere pubblico l'orientamento del Governo nell'ambito delle nuove tecnologie e dello *smart contract*. La UKJT ha sancito che «The concept of a "*smart contract*" is a broader concept than a "*smart legal contract*". A *smart contract* may, or may not, have legal ramifications as it is merely computer code, whereas a "*smart legal contract*" refers to a *smart contract* that either is, or is part of, a binding legal contract. Whether English law recognises such a thing as a *smart legal contract* in this sense will be addressed in the Legal Statement. In any given case, this is likely to involve the application of established tests under English law for determining whether a binding legal contract arises. The concepts of offer, acceptance and consideration are likely to be relevant in this context» (LAW TECH DELIVERY PANEL, 2019).

La UKJT ha dunque chiarito se, e in che modo, lo *smart contract* produce vincoli con effetti giuridici. Ciò posto, la Taskforce ha sollevato due dubbi: in primo luogo, si domanda se occorra applicare anche allo *smart contract* le regole di interpretazione dei contratti tradizionali; in secondo luogo, la Taskforce si pone il dubbio circa le condizioni necessarie per sancire la compatibilità dello *smart contract* con le previsioni di legge che concernono la forma e la sottoscrizione dei documenti, analogici e digitali. A noi pare si tratti di dubbi assai legittimi; la Taskforce ha infatti chiaro che il nodo da risolvere concerna l'individuazione delle condizioni che rendono uno *smart contract* assimilabile a un contratto tradizionale e, come tale, soggetto alla normativa per il medesimo prevista.

In Australia, il legislatore ha deciso sin dal principio di rifarsi alle fonti normative già in vigore, emendandole all'occorrenza. Segnatamente, il legislatore ha ritenuto di applicare allo *smart contract* le previsioni dell'Electronic Transactions Act, 1999(Cth) (ETA): tale testo ha precisato che le transazioni elettroniche che possono essere equiparate, quindi che possono produrre i medesimi effetti giuridici, a quelle analogiche. Il legislatore ha dunque esteso l'analogia includendo anche le transazioni eseguite e registrate su blockchain.

Negli Stati Uniti d'America, gli Stati federali interessati hanno adottato politiche autonome, avendo il Governo di Washington mostrato un approccio distaccato. In particolare, Stati quali California, Delaware, Vermont, Nevada, Arizona, Hawaii, New Hampshire e Illinois, hanno introdotto (o sono in procinto di introdurre) una normativa volta a legittimare l'uso della tecnologia blockchain in generale, e dello *smart contract* in particolare. Le soluzioni sino ad ora adottate non sono però uniformi. Nello Stato del Vermont il legislatore ha adottato un approccio "timido" prevedendo quindi che un fatto, o un dato, verificato attraverso una corretta applicazione della tecnologia blockchain è autentico e si considera certa la data e l'ora in cui la registrazione della transa-

zione è avvenuta. La presunzione di certezza – così precisa la previsione – non si estende alla veridicità, validità o valore giuridico del contenuto del dato. In tal senso, il legislatore ha sì conferito certezza formale, ma ha ridotto il potenziale impiego delle nuove tecnologie: la tecnologia blockchain rimane infatti solo quale certificatore del momento temporale della registrazione del dato.

Parzialmente innovatore è stato invece il Governatore dello Stato dell'Arizona, D. Ducey, che, nel febbraio 2017 ha proposto modifiche alla legge HB 2417 introducendo una disciplina dedicata alle nuove tecnologie: la firma depositata su blockchain è stata così equiparata alla firma digitale. Correlativamente, è stato introdotto un emendamento a norma del quale un contratto memorizzato su blockchain equivale «to an electronic form and to be an electronic data». La fonte normativa in commento si spinge poi un po' oltre, disponendo altresì che lo «*smart contract* may exist in commerce. A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a *smart contract* term». La previsione è di sicuro interesse poiché chiarisce che se lo *smart contract* contiene gli elementi del contratto che lo Stato dell'Arizona considera essenziali allora, anch'esso può produrre effetti giuridici alla stregua di un contratto tradizionale.

Analogo approccio è stato adottato dal legislatore del Tennessee che il 22 marzo 2018 ha introdotto due previsioni volte a legittimare le nuove tecnologie. In particolare, a norma della nuova versione del Bill n. 1662 i dati raccolti e registrati su una piattaforma blockchain hanno valore giuridico e uno *smart contract* può produrre effetti giuridici. Inoltre, il legislatore del Tennessee, al pari di quello dell'Arizona, ha previsto che: «Smart contracts may exist in commerce. No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a *smart contract* term». Nei due ultimi predetti casi i legislatori U.S.A. dell'Arizona e del Tennessee, hanno in primis riconosciuto effetti giuridici ai dati raccolti e registrati su blockchain e, quindi, anche ai codici che formano lo *smart contract*. In secondo luogo, pur non riconoscendo una validità ex se allo *smart contract*, hanno escluso che la presenza di anche solo un termine contrattuale sviluppato in linguaggio smart privi lo strumento della qualifica di contratto. Ciò significa che, presenti tutte le condizioni prescritte dal diritto dei contratti dello Stato di riferimento, lo *smart contract* equivale a uno *smart legal contract*. Decisamente più innovativa è invece la normativa californiana che ha equiparato al contratto tradizionale lo *smart contract* – ovvero il contratto che contiene anche solo uno *smart contract* term. Segnatamente, nel settembre 2018 la California Assembly ha passato il progetto di Legge n. 2658 che modifica il California Civil Code. La Section 1633.2 così riformulata prescrive che «e) "Contract" means the total legal obligation resulting from the parties'agreement as

affected by this title and other applicable law. "Contract" includes a *smart contract*. (p) "Smart contract" means an event-driven program that runs on a distributed, decentralized, shared, and replicated ledger that can take custody over, and instruct transfer of, assets on that ledger». In buona sostanza, il legislatore californiano ha assimilato *smart contract* e contratto tradizionale chiarendo che il primo si distingue solo per forma.

Dal breve excursus tracciato sembra che i legislatori, sia di Stati membri UE sia di Stati extra UE abbiano adottato, salve rare eccezioni, un approccio di c.d. "timidezza regolamentare", limitandosi a definire previsioni di portata generale (T. SCHREPEL, 2018; F.A. HAYEK, 1945). L'approccio convince. La tecnologia alla base dello *smart contract*, ossia la blockchain, è infatti ancora in fase di evoluzione, sicché pare giusto che la stessa non sia frenata dall'introduzione di definizioni normative eccessivamente rigide e vincolanti (F. DI GIOVANNI, 2017). L'auspicio per il prossimo futuro è però riuscire a trovare un equilibrio simile a quello raggiunto in California dove il legislatore ha dato certezza giuridica ai rapporti conclusi con nuovi strumenti tecnologici, senza aggiungere nulla, quindi senza precludere eventuali e ulteriori evoluzioni tecnologiche. Vi è altrimenti il rischio, non peregrino, che l'impiego di termini analoghi induca a erronee qualificazioni giuridiche e, per esse, a illegittimi affidamenti.

4. La normativa internazionalprivatistica e lo *smart legal contract*

Il paragrafo precedente ha esaminato i più recenti – e attualmente gli unici – esempi di normativa nazionale introdotta per disciplinare le nuove tecnologie e gli strumenti normativi di cui esse permettono lo sviluppo. Le soluzioni adottate sono disomogenee e rendono quanto mai necessario un intervento chiarificatore da parte del legislatore europeo ed internazionale.

Nelle more, riteniamo comunque utile se le fonti europee e internazionali di diritto internazionale privato siano applicabili allo *smart legal contract*. Il problema si pone in quanto lo *smart legal contract* è sviluppato su blockchain pubbliche che corrispondono a una rete di computer (c.d. nodi) localizzati ovunque e privi di un'entità centrale che li coordini (M. FINCK, 2018) (v. capitolo VI, G. CARULLO). Conseguentemente, lo *smart legal contract* ha una natura transnazionale, salvo le parti non esprimano diversamente, radicando espressamente il contratto a uno Stato, o la blockchain impiegata sia prettamente nazionale. Da ciò consegue che in ipotesi in cui lo *smart legal contract* non si sia auto eseguito e sorgano controversie tra le parti, potrebbero derivare problemi di coordinamento, in particolare di individuazione del giudice

competente a dirimere la controversia, nonché della legge applicabile al contratto (trascuriamo in questa sede le questioni relative al riconoscimento e all'esecuzione delle decisioni in ragione dell'assenza di precedenti).

Per quanto concerne la dimensione europea, rileviamo che la scarsità e la disomogeneità delle soluzioni normative adottate dagli Stati membri, rende incerta l'applicabilità allo *smart legal contract* della disciplina internazionalprivatistica europea sulle obbligazioni contrattuali in materia civile e commerciale (F. MOSCONI, C. CAMPIGLIO, 2017). La questione meriterebbe uno studio autonomo sicché in questa sede ci limitiamo al primo passaggio del ragionamento. Segnatamente, ci interroghiamo sulle condizioni preliminari che potrebbero rendere applicabile la normativa internazionale privatistica europea, in particolare quella contenuta nei Regolamenti Bruxelles I bis e Roma I (che rispettivamente introducono una disciplina uniforme in tema di foro competente e legge applicabile alle obbligazioni contrattuali in materia civile e commerciale).

In primo luogo, occorre considerare i soli *smart legal contract* ossia quegli strumenti che, *prima facie*, contengono gli elementi essenziali del contratto. In altre parole, se l'ordinamento del foro adito esclude la validità giuridica degli effetti prodotti da qualsiasi *smart contract* – indipendentemente dal contenuto – il ricorso alla disciplina uniforme europea è ex se precluso. I citati Regolamenti si applicano infatti in presenza di fattispecie contrattuali. In secondo luogo, l'eventuale applicazione della disciplina uniforme europea deve ritenersi residuale, nel senso che essa interviene solo quando lo *smart legal contract* non è stato in grado di auto eseguirsi, inducendo così la parte presunta lesa a ricorrere all'intervento del giudice. Correlativamente, si pone la terza premessa: le parti devono fare ricorso al giudice nazionale solo dopo aver esperito i rimedi alternativi di risoluzione delle controversie, se previsti come obbligatori nello *smart legal contract* medesimo (dalla transazione, alle c.d. modalità ADR) e a patto che non sia stata inserita una clausola arbitrale.

Accertate le citate premesse, occorre verificare se sussistono i presupposti per cui lo *smart legal contract* sottoposto allo scrutinio del giudice, e la fattispecie nel medesimo disciplinata, rientrino o meno nel campo di applicazione temporale, materiale e personale dei regolamenti europei Bruxelles I bis e Roma I.

A questo proposito, e prescindendo dall'esame della normativa, ci pare di poter qui ribadire le conclusioni già raggiunte per la normativa interna: le norme dei citati Regolamenti potrebbero essere applicate se emendate sì da includere anche la fattispecie dello *smart legal contract* (G. RÜHL, 2020). Ad esempio, le categorie giuridiche del domicilio, della residenza, del luogo di consegna, che nei citati Regolamenti fungono da criteri di collegamento, do-

vrebbero essere interpretate sì da poter essere usate anche in ipotesi in cui le parti abbiano sottoscritto uno *smart legal contract* (B. CAPPIELLO, 2020).

Le incertezze applicative sollevate con riguardo alle norme di diritto internazionale privato europeo si pongono altresì con riguardo alle norme di conflitto, o materiali, contenute in alcuni strumenti di soft law o in convenzioni internazionali di diritto internazionale privato.

Con riguardo ai primi, ricordiamo la UNCITRAL Model Law on Electronic Transferable Records, 2017. Quest'ultima, nel rispetto del principio della neutralità tecnologica, legittima scambi di dati attraverso la tecnologia a registro distribuiti e riconosce che essa è idonea se non altro a certificare il momento in cui lo scambio è avvenuto. L' art. 1 dispone che «The Model Law provides generic rules that may apply to various types of electronic transferable records based on the principle of technological neutrality and a functional equivalence approach. The principle of technological neutrality entails adopting a system-neutral approach, enabling the use of various models whether based on registry, token, distributed ledger or other technology». Il successive art. 9 prescrive poi che «Certain electronic transferable records management systems, such as those based on distributed ledgers, may identify the signatory by referring to pseudonyms rather than to real names». Sempre con riguardo a strumenti di soft law, ricordiamo che nel settembre 2019 la ICC ha pubblicato gli Incoterms®2020, in vigore a decorrere dal 1° gennaio 2020. La Camera del Commercio Internazionale ha dapprima siglato un accordo con Perlin, una delle più influenti piattaforme di certificazione Blockchain, per poi elaborare «a customizable, self-executing digital sales agreements, incorporating the new Inconterms® rules. The incorporation of smartIncoterms® rules, or Smart INCOs, will help facilitate trade by reducing costs and barriers faced by importers and exporters worldwide, notably, small and medium enterprises». La ICC ha quindi riconosciuto che la tecnologia blockchain può facilitare gli scambi commerciali, rendendoli più sicuri e così ingenerando fiducia negli operatori.

Con riguardo alle convenzioni internazionali di diritto internazionale privato, anche in questo caso sorgono dubbi circa la loro applicabilità allo strumento *smart legal contract*. In particolare, per quanto concerne le convenzioni internazionali di diritto internazionale privato materiale si pongono dubbi circa l'applicabilità allo *smart legal contract* della Convenzione di Vienna sulla vendita di beni mobili, 1980 (L. TRIPODI, 2015; L. DI MATTEO, 2014; N. BOSCHIERO, 1990). A noi pare che l'applicazione agli smart (legal) contract non sia *ex se* preclusa; semplicemente, come già visto, occorre esaminare le condizioni in presenza delle quali la citata Convenzione, così come altre, troverebbero applicazione, per valutarne il possibile impiego in ipotesi di contratti sottoscritti ed eseguiti attraverso tecnologie a registro distribuito.

Per tutto quanto precede, risulta che il rapporto tra evoluzione tecnologica e diritto non impone necessariamente il superamento dei tradizionali paradigmi giuridici, e con essi dei più classici istituti del diritto; al contrario, ci sembra che l'integrazione tra i due settori sia possibile nella misura in cui il diritto legittimi i nuovi strumenti, se del caso emendando la disciplina esistente. Risulta dunque auspicabile qualificare correttamente gli strumenti in esame per poi sussumerli nel quadro normativo di volta in volta più idoneo. Solo in mancanza di fonti applicabili, anche attraverso una interpretazione estensiva, il procedimento di inclusione potrebbe richiedere un intervento *ad hoc* del legislatore. Si tratta in ogni caso di interventi necessari anche e soprattutto per tutelare i consociati che fanno uso dei nuovi strumenti. In altre parole, se un ordinamento prescrive per un contratto la forma scritta *ad substantiam*, occorre che il legislatore di quel dato ordinamento – ovvero il legislatore europeo – introduca una previsione che legittimi lo scambio di firma su blockchain ed equipari alla forma scritta la produzione, e successiva conservazione, di un documento su un blocco della blockchain. Si tratta del resto di un'elaborazione che si è già resa necessaria ogni volta che il legislatore si è trovato a dover fronteggiare una travolgente evoluzione tecnologica come è il caso della stampa e del digitale.

5. La Pubblica Amministrazione e lo *smart legal contract*: prospettive applicative

Alla luce delle innovative caratteristiche degli *smart contract*, e della loro idoneità a produrre validamente effetti giuridici nel nostro ordinamento – alle condizioni suddette –, ci si può domandare se e quale ruolo questi possano avere nel settore pubblico, specie nei rapporti con i privati. Vale sul punto ancora sottolineare che, secondo la ricostruzione proposta nei paragrafi precedenti, gli *smart contract* possono acquisire piena validità legale nel nostro ordinamento e, quindi, assurgere a veri e propri contratti. Per questo si è proposta l'espressione "*smart legal contract*", ad evidenziare la potenziale rilevanza giuridica del programma informatico che implementa lo *smart contract*.

Ciò premesso, non pare che, anche in mancanza di una norma *ad hoc*, vi siano preclusioni a che anche le pubbliche amministrazioni, nella loro capacità di diritto privato, si avvalgano di questo strumento.

In proposito occorre ricordare che in forza dell'art. 1, comma 1-*bis* della Legge n. 241/1990 «la pubblica amministrazione, nell'adozione di atti di natura non autoritativa, agisce secondo le norme di diritto privato salvo che la legge disponga diversamente». Come si è già da tempo riconosciuto in dottrina e

giurisprudenza, non vi è dunque dubbio che la Pubblica Amministrazione goda di una «capacità generale di diritto privato. Il che significa che, salvi i divieti espressamente previsti dalla legge, l'Amministrazione può stipulare qualunque contratto di diritto privato, tipico o atipico che sia» (G. GRECO e M. CAFAGNO, 2017, p. 317).

In mancanza dunque di espresse preclusioni all'utilizzo degli *smart contract* da parte dei soggetti pubblici, si può ritenere che a questi non sia precluso l'utilizzo di detto strumento. Anzi, in ragione delle evoluzioni legislative più recenti, tra cui il citato art. 8-*ter* del D.L. n. 135/2018 e quanto indicato nella relazione illustrativa del D.L. n. 76/2020 (D.L. 16 luglio 2020, n. 76, Misure urgenti per la semplificazione e l'innovazione digitale, convertito con la Legge 11 settembre 2020, n. 120), sembrerebbe che il legislatore voglia favorire il ricorso a strumenti basati sulle DLT anche nel settore pubblico (v. capitolo VI, G. CARULLO).

Si potrebbe tuttavia obiettare che non sia compatibile con i criteri di spesa pubblica, e soprattutto di selezione dei contraenti delle amministrazioni, il ricorso ad uno strumento che determina la conclusione automatizzata di accordi pattizi, od addirittura di più accordi simultaneamente.

A tale rilievo si può però agevolmente contestare anzitutto che la conclusione automatizzata di un contratto non impedisce che, per l'individuazione della controparte privata, l'amministrazione comunque svolga una procedura ad evidenza pubblica, solo a valle della quale venga effettivamente implementato lo *smart legal contract*. Senza contare che, nei contratti sotto soglia, un tale problema potrebbe *tout court* non porsi.

Ma v'è di più. Il ricorso agli *smart legal contract* potrebbe addirittura aumentare la trasparenza delle procedure selettive (v. capitolo XI, G.M. RACCA). Grazie all'automazione delle diverse fasi del contratto, si potrebbero addirittura rafforzare le garanzie procedimentali. Ad esempio, in relazione alla c.d. clausola di *stand still* sostanziale in forza della quale di norma l'amministrazione non può stipulare il contratto prima che siano trascorsi 35 giorni dall'aggiudicazione (v. art. 32, comma 9, D.Lgs. n. 50/2016), si potrebbe implementare un meccanismo che consenta la stipula solo trascorso tale periodo, ed in mancanza di azioni giurisdizionali volte a prolungare tale termine (v. art. 32, comma 11, D.Lgs. n. 50/2016). Il tutto con le garanzie di trasparenza e tracciabilità che la blockchain – sulla base della quale gli *smart legal contract* sono sviluppati – garantisce (v. capitolo VI, G. CARULLO).

Quanto poi all'automazione che sta alla base della logica degli *smart legal contract*, vale sottolineare che, a ben vedere, questa si esaurisce, sotto un profilo giuridico, nella mera automazione della verifica di condizioni sospensive stabilite dalle parti. La logica condizionale di cui si è detto sopra (if-then) può

essere inquadrata, da un punto di vista giuridico, quale mera verifica automatizzata dell'avveramento di una o più condizioni sospensive, al ricorrere delle quali si producono gli effetti giuridici voluti dalle parti.

Così impostata la questione, si può ritenere che la deviazione rispetto ad un normale contratto, da un punto di vista strettamente giuridico, sia fortemente ridimensionata. Anzi, a ben vedere, la conclusione automatizzata di un contratto al verificarsi di determinate condizioni registrate da un dispositivo elettronico non è cosa nuova. Si pensi al pagamento di una tariffa per la sosta di un veicolo su strada pubblica: in tali casi alla corresponsione di una determinata somma corrisponde automaticamente l'emissione di un titolo (cartaceo o digitale) che autorizza la sosta per un predeterminato periodo di tempo.

Ciò che muta con gli *smart contract* non è dunque l'automazione. Piuttosto, l'innovazione radicale che le DLT apportano in questo campo risiede nelle modalità con cui detta automazione è conseguita, ossia la memorizzazione degli eventi su di un registro distribuito con meccanismi di validazione dei dati crittografici. Tale registro distribuito può essere programmato in modo che, qualora i dati registrati sul database distribuito producano un determinato valore, gli effetti desiderati dalle parti si realizzino automaticamente, senza necessità che le informazioni siano validate da una terza parte certificatrice o comunque senza una qualche ulteriore attività da parte di terzi.

Ciò può essere di grande aiuto per le pubbliche amministrazioni, specie in relazione alle attività vincolate. In relazione a funzioni il cui contenuto è interamente predeterminato dalla legge si potrebbe infatti prevedere la predisposizione di *smart legal contract* che, al ricorrere delle condizioni predeterminate dalla legge, producano un certo risultato. Ciò potrebbe ad esempio essere applicato nel campo degli atti di assenso interamente vincolati, in supporto od in alternativa ad esempio all'istituto della segnalazione certificata di inizio attività (SCIA, art. 19, Legge n. 241/1990). Il privato non dovrebbe fare altro che allegare, attraverso un dato procedimento digitalizzato, l'integrazione dei requisiti previsti dalla legge per l'espletamento di una determinata attività, ed al ricorrere di tutti i presupposti potrebbe essere emesso in modo automatizzato – attraverso la registrazione sulla blockchain – l'atto richiesto.

Le applicazioni che si possono immaginare per questa tecnologia sono molte altre e non è possibile qui ripercorrerle tutte. Basti dunque evidenziare che, allo stato, non pare che sussistano fondate obiezioni di diritto a che gli *smart legal contract* possano essere utilizzati anche dalle pubbliche amministrazioni. Non resta dunque che attendere per verificare se e quale diffusione avranno gli *smart legal contract* nel settore pubblico.

Bibliografia

BOSCHIERO N., *Il coordinamento delle norme in materia di vendita internazionale*, Cedam, Verona, 1990.

CAPPIELLO B., *Dallo "smart contract" computer codallo smart (legal) contract. I nuovi strumenti (para) giuridici alla luce della normativa nazionale e del diritto internazionale privato europeo: prospettive de jure condendo*, in *Rivista del commercio internazionale*, 2020.

CAPPIELLO B., *Cepet Leges in Legibus, Crypto assets and Cryptocurrencies: interpretative and regulatory issues under the European and the member states "law" perspective*, in *Rivista del commercio internazionale*, 2019.

CAPPIELLO B., CARULLO G., *Blockchain, Law and Governance*, Springer-Verlag, Heidelberg, 2020.

CERRATO S., *Contratti tradizionali, diritto dei contratti e Smart Contracts*, in R. BATTAGLINI, M.T. GIORDANO, *Blockchain e Smart Contracts*, Giuffrè, Milano, 2019.

DI GIOVANNI F., *Macchine intelligenti e rapporti contrattuali, in Intelligenza Artificiale e Responsabilità*, in U. RUFFOLO (a cura di), *Atti del Convegno del 29 novembre 2017, Università per Stranieri di Perugia*, Milano.

DI MATTEO L., *International Sales Law. A Global Challenge*, Cambridge University Press, Cambridge, 2014.

FINCK M., *Blockchain Regulation and Governance in Europe*, Cambridge University Press, Cambridge, 2018.

GOLDWASSER S., MICALI S., *Probabilistic encryption and how to play mental poker keeping secret all partial information*, in *Proc. 14th Symposium on Theory of Computing*, 1982.

GOLDWASSER S., MICALI S., *Probabilistic encryption*, in *Journal of Computer and System Sciences*, 1984.

GRECO G., CAFAGNO M., *Pubblico e privato nei contratti, nei rapporti col personale e nella gestione di beni e servizi*, in G. GRECO, M. CAFAGNO, D.-U. GALETTA, M. RAMAJOLI e M. SICA, *Argomenti di diritto amministrativo*, vol. I, III, Giuffrè, Milano, 2017, p. 317.

GREFENSTETTE G., TAPANAINEN P., *What is a word, what is a sentence? Problems of Tokenization*, 1994, http://www.corpus.unam.mx/cursocorpus/mltt-004.pdf.

HAYEK F.A., *The use of knowledge in society*, in *American Economic Review*, 1945.

JACCARD G., *Smart Contracts and the Role of Law*, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885.

LESSIG P., *Code is law. On Liberty in cyberspace*, 2000, https://harvardmagazine.com/2000/01/code-is-law-html.

MARXWELL W., BOURREAU M., *Technological neutrality in internet, telecoms and data protection regulation*, in *Computer and Telecommunications Law Review*, 2014.

MOSCONI F., CAMPIGLIO C., *Diritto Internazionale privato e processuale*, vol. 1, *Parte generale e obbligazioni*, Giuffrè, Milano, 2017.

POSNER R., *The right of privacy*, in *Georgia Law Review*, 1977.

RÜHL G., *Smart (legal) contract, or: Which (contract) law to smart contracts?*, in B.

CAPPIELLO, G. CARULLO (a cura di), *Blockchain, Law and Governance*, Springer-Verlag, Heidelberg, 2020.

SCHREPEL T., *Is blockchain the death of antitrust law? The blockchain antitrust paradox*, in *Georgetown Law Technology Review*, 2018.

STARK J., *Making sense of Blockchain and Smart Contracts*, 2016, https://www. coindesk. com/making-sense-smart-contracts.

STOUT L., *Cultivating Conscience. How good law make good people*, Princeton University Press, Princeton, 2010.

TRIPODI L., *Towards a New CISG, The prospective Convention on the International Sale of Goods and Services*, Brill-Nijhoff, Leida, 2015.

WERBACH K., *Trustless trust, why the blockchain needs the law*, in *Berkeley Technologies Law Review*, 2018.

XI.

LA DIGITALIZZAZIONE DEI CONTRATTI PUBBLICI: ADEGUATEZZA DELLE PUBBLICHE AMMINISTRAZIONI E QUALIFICAZIONE DELLE IMPRESE

Gabriella M. Racca

SOMMARIO: 1. Digitalizzazione per l'integrità, l'innovazione e l'efficienza negli appalti pubblici. – 2. L'interoperabilità delle banche dati per un nuovo sistema di *e-procurement*. – 3. Contratti digitali: i sistemi dinamici di acquisizione, accordi quadro e aste elettroniche. – 4. La modellazione digitale per gli appalti di lavori e gli *smart contracts* (accordi collaborativi). – 5. La digitalizzazione per un rinnovato rapporto di collaborazione e fiducia tra amministrazioni e operatori economici nell'interesse pubblico.

1. Digitalizzazione per l'integrità, l'innovazione e l'efficienza negli appalti pubblici

L'Italia si colloca in una bassa posizione sia nelle classifiche internazionali di trasparenza e legalità (*Transparency International*), sia in quelle sullo sviluppo digitale (*Digital economy and society index, DESI*). La digitalizzazione dei contratti pubblici costituisce un presupposto essenziale per l'efficienza, l'integrità e l'innovazione della funzione appalti (ANAC, *Strategie e azioni per l'effettiva semplificazione e trasparenza nei contratti pubblici attraverso la completa digitalizzazione: le proposte dell'Autorità*, documento approvato il 27 maggio 2020; *Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia. Gli appalti pubblici tra istanze di semplificazione e normativa anticorruzione. Alla ricerca di un equilibrio tra legalità ed efficienza*, a cura di L. DONATO, 2020).

La digitalizzazione è necessaria per promuovere e rilanciare il mercato dei contratti pubblici superando le arretratezze, ormai insostenibili, nel confronto con le piattaforme private. L'efficienza della funzione appalti diviene infatti ne-

cessaria anche per evitare l'ingresso di operatori privati che, come già oltreoceano, si pongano come alternativi alla funzione pubblica di acquisto e riducano lo spazio pubblico di politica industriale nel settore. Il riferimento è alle piattaforme private del tipo "Amazon" che negli Stati Uniti stanno entrando sul mercato dei contratti pubblici di minor valore (GSA*, Awards Contracts to Commercial E-Marketplace Platform Providers*, 2020, https://interact.gsa.gov/blog/gsa-awards-contracts-commercial-e-marketplace-platform-providers; l'iniziativa avviata viene informalmente denominata come "Amazon.gov"). L'efficienza assicurata dalle piattaforme private di *e-commerce,* in particolare nel periodo emergenziale, fa emergere il rischio che esse tendano a sostituirsi alla "funzione appalti" delle pubbliche amministrazioni, con tutte le connesse implicazioni di strategia e politica industriale (Libro Bianco per l'Economia Digitale, 2020).

Come noto, la funzione appalti consiste nella programmazione e definizione dei fabbisogni di forniture, servizi e lavori, nella predisposizione delle procedure di scelta del contraente (ove si esauriscono le scelte discrezionali), nella conseguente gara pubblica per individuare il contraente e nella fondamentale fase dell'esecuzione. Infatti, a seguito del confronto concorrenziale e dell'aggiudicazione della gara sulla base dei criteri indicati nel bando, si stipula il contratto e si avvia la fase di esecuzione che, con un unico atto di consegna della fornitura, ovvero con anni di esecuzione del servizio o di realizzazione dei lavori, determina soddisfazione del bisogno, obiettivo primario della funzione appalti (Codice contratti pubblici, D.Lgs. n. 50/2016).

La trasformazione digitale della funzione appalti presuppone la capacità e l'adeguatezza organizzativa (art. 118, Cost.) e professionale delle amministrazioni aggiudicatrici. In Italia si contano ancora circa 32.000 amministrazioni aggiudicatrici ed è evidente che non possano essere tutte qualificate, ma si debbano individuare dei soggetti che svolgano le procedure di gara per le altre pubbliche amministrazioni. Il processo di qualificazione delle stazioni appaltanti avviato con il Codice non si è concluso, ma si sono tuttavia individuate centrali d'acquisto, (nazionali, Ministero dei Trasporti e Infrastrutture, Consip spa, Invitalia e 31 regionali) qualificate come "soggetti aggregatori" che svolgono funzioni di centrali di committenza e che dispongono di piattaforme sulle quali, con diverse modalità e consistenza, è stata avviata la digitalizzazione delle procedure. Vi sono anche forme di aggregazione differenti e minori (stazioni uniche appaltanti, centrali uniche di committenza, ecc.) che peraltro spesso hanno svolto gare per i relativi enti senza aggregare la domanda e senza soddisfare le esigenze di efficienza e semplificazione per mancanza di specifica formazione del personale.

Il processo di digitalizzazione si è, "sulla carta" avviato. Da tempo è stata intrapresa la prima fase di cosiddetta dematerializzazione dei documenti, di "informatizzazione", che spesso si è limitata alla scansione di documenti cartacei

caricati poi in rete, in particolare relativamente alla qualificazione degli operatori economici. Più di recente si sono previste le procedure selettive dell'asta elettronica, del sistema dinamico di acquisizione, del catalogo elettronico che consentono di avviare la digitalizzazione anche della fase di selezione.

Una effettiva digitalizzazione tuttavia richiede centrali d'acquisto digitalizzate con procedure "native digitali" e con documenti di gara (E-Forms) che contengano dati che possano essere direttamente prodotti per la forma dell'interoperabilità digitale in modo da permettere l'acquisizione e pubblicazione, nelle parti utili, nelle differenti banche dati, nazionali ed europee (Gazzetta Ufficiale Unione Europea, Tender Electronic Daily, Banca Dati Nazionale Contratti Pubblici, Amministrazione Trasparente, ecc.).

L'Unione Europea impone infatti la formazione "nativa digitale" dei documenti di gara con l'adozione (entro il 25 ottobre 2023) di nuovi atti digitali *standard* generati automaticamente per la pubblicazione di avvisi e bandi sulla Gazzetta ufficiale dell'Unione e per tutte le attività conseguenti (Regolamento di esecuzione 2019/1780/UE della Commissione del 23 settembre 2019). Tali formulari costituiranno modelli standard su cui inserire i dati rilevanti collegati, mediante sistemi di *software,* con le informazioni ricavate da precedenti avvisi e bandi, specifiche tecniche, offerte, contratti, registri amministrativi nazionali e altre fonti di dati. Tale disciplina assicurerà il rispetto del principio *once-only* nella pubblica amministrazione elettronica, in una prospettiva di favore per lo sviluppo di forme di cooperazione tra amministrazioni pubbliche europee (a livello nazionale e transnazionale) per la condivisione di informazioni con l'inserimento dei dati una sola volta ed il relativo richiamo e riutilizzo in differenti documenti e basi di dati, consentendo la riduzione degli oneri amministrativi e l'aumento dell'affidabilità dei dati. La pubblicazione potrà essere in tal modo agevolata e automatizzata, superando gli attuali estenuanti oneri di ricaricamento degli stessi dati da parte delle pubbliche amministrazioni e delle imprese. Con favore per la trasparenza e la pubblicità dei documenti di gara, senza aggravamento di oneri, anche degli avvisi e dei bandi di valore inferiore alle soglie UE e basati su accordi quadro.

La digitalizzazione e l'aggregazione dei contratti pubblici richiedono l'adeguatezza delle organizzazioni pubbliche deputate all'esercizio della funzione appalti. Adeguatezza, come principio costituzionale che si pone a fondamento della professionalità dei funzionari pubblici per assicurare la adeguata qualificazione di chi svolge le gare non individuali ma nell'ambito dell'esercizio di una funzione, pur sempre pubblica, a favore di terzi. Prospettazione che perciò legittima limitazioni della capacità giuridica di contrattare per assicurare la qualità delle prestazioni, senza limitare l'autonomia, in particolare degli enti territoriali nell'esercizio di poteri e funzioni (G.M. RACCA, S. PONZIO, 2019; A. ROMANO, 1987). Autonomia che, con riferimento alla funzione appalti, va

intesa come assegnata alla pubblica amministrazione nel suo complesso e non necessariamente in relazione alle sue diverse articolazioni.

L'impostazione è stata di recente affermata anche dalla Corte dei conti ritenendo indifferibile un programma di rafforzamento, professionalizzazione e specializzazione delle risorse umane interne alle pubbliche amministrazioni che operano nel settore degli appalti, in particolare per le figure tecniche, con l'aggregazione delle stazioni appaltanti accrescendone la competenza tecnica (Corte dei conti, *Referto in materia di informatica pubblica*, settembre-ottobre 2019, p. 115) riaffermando così quella simmetria tra amministrazioni e operatori economici imponendo a chi richiede una prestazione di saperla definire, selezionare e controllarne l'esecuzione.

L'aggregazione dei contratti pubblici va intesa, non come centralizzazione, ma come specializzazione per l'aggiudicazione degli appalti in modo efficiente, integro e innovativo, ripensando il modello organizzativo della centrale di committenza che compie gare per conto di terzi e attuandolo come sistema a rete fra la centrale di committenza nazionale (Consip) e i soggetti aggregatori regionali che possono specializzarsi su singoli settori (per es. sanità, infrastrutture) e aree merceologiche, anche per tutto il territorio nazionale.

L'aggregazione e la specializzazione nella funzione appalti richiedono la digitalizzazione e quindi interoperabilità specificamente programmata fra le banche dati rilevanti al fine di un'efficace conoscenza del settore contratti pubblici (G.M. RACCA, C. YUKINS, 2019).

La digitalizzazione dei contratti pubblici richiede un sistema di centrali d'acquisto specializzate coordinate fra loro in modo più strutturato rispetto all'attuale esperienza del Tavolo dei soggetti aggregatori. Ciò consentirebbe di assicurare un servizio di gare realizzate e messe a disposizione di tutte le amministrazioni utilizzatrici che non dispongono delle capacità, né potranno qualificarsi per poter svolgere adeguatamente le gare pubbliche. Una prospettiva che apre allo sviluppo di strategie di specializzazione anche superando i limiti territoriali e coprendo così più settori per lo sviluppo di politiche industriali per la crescita anche delle piccole e medie imprese innovative.

Gare elettroniche che mettono a disposizione dei fabbisogni delle amministrazioni utilizzatrici i beni e servizi necessari e che possono essere scelti "a scaffale", "già garati", secondo la quantità e qualità più appropriata rispetto al bisogno con una semplificazione della modalità di adesione e acquisto (modello "Amazon"), senza eludere le garanzie dello svolgimento di una procedura di gara (pubblica). Si supererebbe anche il modello del Mercato Elettronico della Pubblica Amministrazione (MEPA), che spesso induce la frammentazione abusiva e dovrebbe assicurare l'efficienza dei portali privati adottando un algoritmo pubblico che applichi i principi di imparzialità e rotazione, ove le

prestazioni siano equivalenti. L'analisi dati degli acquisti sul MEPA potrebbe consentire di distinguere gli acquisti di valore minimo e occasionali da svolgere direttamente, con l'efficienza e la valutazione reputazionale delle imprese. Per gli acquisti che si rinvengano come significativi e programmabili si potrebbe passare a gare elettroniche mediante sistemi dinamici di acquisizione.

Non si esclude che le amministrazioni possano realizzare autonomamente le proprie gare, ma la qualità e l'efficienza del servizio potrebbero soddisfare i bisogni, senza necessità di imporre obblighi. Le amministrazioni che si riterranno capaci di ottenere migliori risultati potranno ancora cimentarsi con i costi e tempi di una gara tradizionale.

Le recenti previsioni del D.L. 16 luglio 2020, n. 76, c.d. "Semplificazioni", convertito dalla Legge 11 settembre 2020, n. 120, inducono a ritenere la digitalizzazione essenziale per il rispetto dei principi non derogabili in materia di contratti pubblici che si ricollegano all'imparzialità e buon andamento (art. 97 Cost.). In assenza di un aperto confronto concorrenziale, gli affidamenti diretti o le negoziazioni dovranno assicurare comunque il rispetto dei principi e la forma digitale sarà necessaria per la tracciabilità delle operazioni. La digitalizzazione ed il monitoraggio, anche *ex post* di dati, tempi e costi sostenuti per i contratti potranno permettere di verificare se le misure di semplificazione avranno effettivamente raggiunto l'obiettivo della tempestiva esecuzione dei contratti nell'interesse pubblico. La previsione della qualificazione delle stazioni appaltanti, anche solamente per la fase di esecuzione e collaudo, apre alla attribuzione alle centrali di acquisto della progettazione e affidamento dei contratti mediante piattaforme ed adeguati strumenti digitali. Anche sulla qualificazione delle imprese si tende a superare l'attuale frammentazione. L'amministrazione digitale comincia a dimostrare la sua necessità ed il percorso verso l'adozione di evoluti strumenti di *e-procurement* pare avviato. L'evidenza dell'efficienza dei nuovi modelli, che pur vengono lasciati convivere in parallelo con quelli tradizionalmente frammentati, dovrebbe determinarne il progressivo volontario abbandono. La necessità di incentivare gli investimenti pubblici per far fronte alle ricadute economiche negative per la crisi in atto richiede la collaborazione ed il superamento delle arretratezze che solo la digitalizzazione dei contratti pubblici offre agli operatori economici alle amministrazioni pubbliche a vantaggio dei cittadini.

2. L'interoperabilità delle banche dati per un nuovo sistema di *e-procurement*

L'interconnessione delle differenti banche dati esistenti e la digitalizzazione possono semplificare la fase di selezione degli offerenti assicurando il rapido

reperimento di dati utili all'accertamento dei requisiti di partecipazione e dei possibili motivi di esclusione (sull'interconnessione delle banche dati, v. capitolo VI, G. CARULLO). Occorre integrare e rendere interoperabili i *database* esistenti, quali le banche dati dell'Autorità Nazionale Anticorruzione delle Infrastrutture e dei Trasporti, del Ministero dell'economia e delle finanze, ma anche quelle detenute da soggetti privati per l'acquisizione della qualificazione delle imprese digitalmente (una sorta di "bollino verde") con aggiornamenti in tempo reale sulla sussistenza dei requisiti di ordine tecnico, economico, finanziario e di ordine generale-morale, sfruttando la semplificazione proposta dalla digitalizzazione del documento unico di gara europeo.

Il mancato coordinamento dei dati nel settore degli appalti costituisce un forte limite alla semplificazione e allo sviluppo del settore. A fronte di una competenza esclusiva dello Stato sul «coordinamento informativo, statistico e informatico» (art. 117, comma 2, lett. r), Cost.) sono state riscontrate notevoli criticità connesse alla mancata razionalizzazione e coordinamento delle piattaforme di raccolta dei dati relativi alle fasi di programmazione, affidamento ed esecuzione dei contratti pubblici di rilievo regionale o sub-regionale che rimangono monitorati dalle Regioni e Province autonome (art. 29, commi 3 e 4, D.Lgs. n. 50/2016). Di qui la previsione del Codice dei contratti pubblici relativa alla definizione di un protocollo generale fra l'ANAC, il Ministero dell'economia e delle finanze, il Ministero delle infrastrutture e dei trasporti e la Conferenza delle Regioni e delle Province autonome, per la definizione delle regole di interoperabilità e delle modalità di interscambio dei dati e degli atti tra le rispettive banche dati, nel rispetto dei principi di unicità del luogo di pubblicazione e di unicità dell'invio delle informazioni (art. 29, comma 4-*bis*, D.Lgs. n. 50/2016).

Il Codice dei contratti pubblici prevede per l'acquisizione della documentazione comprovante il possesso dei requisiti di carattere generale, tecnico-professionale ed economico e finanziario, per la partecipazione alle procedure e per il controllo in fase di esecuzione del contratto della permanenza dei requisiti, l'utilizzo esclusivo della Banca dati centralizzata gestita dal Ministero delle infrastrutture e dei trasporti, denominata Banca dati nazionale degli operatori economici (art. 81 D.Lgs. n. 50/2016).

Manca ancora l'attuazione di tale disposizione e rimane pertanto operativo in via transitoria il precedente sistema AVCpass (art. 216, comma 13, D.Lgs. n. 50/2016), che peraltro risulta largamente insoddisfacente in quanto, per esempio con riferimento ai requisiti di ordine generale degli operatori economici, consente di scaricare i certificati del casellario giudiziale ad essi connessi ma non effettua in via automatica la verifica delle condanne riportate e dei carichi pendenti. Considerazioni analoghe riguardano anche la verifica dei requi-

siti di ordine tecnico-professionale e economico-finanziario sulla documentazione di altri enti certificanti.

Continua quindi a gravare in capo alla stazione appaltante tutta l'attività di analisi manuale della documentazione rinvenibile attraverso il sistema AVCpass rispetto ai requisiti di qualificazione degli operatori economici, come precisato dalla stessa Autorità Nazionale Anticorruzione (delibera ANAC n. 157 del 2016), che garantisce «il trasporto e la pubblicazione sicura dei dati» restando le valutazioni in merito ai contenuti di ciascun documento onere delle singole stazioni appaltanti, con evidente aggravamento della fase di selezione dell'offerente. La selezione dell'offerente nella procedura di appalto pubblico confluisce nella prima parte (cosiddetta busta A) sui requisiti di qualificazione dell'operatore economico e richiede ancora un complesso lavoro di verifica che assorbe molto del tempo necessario per giungere alla ammissione o meno al confronto competitivo che in seguito porterà alla valutazione delle offerte, normalmente nelle due componenti, tecnica ed economica (busta B). L'Unione Europea, sopra la soglia di rilevanza europea, impone la valutazione separata della qualificazione dell'operatore economico, rispetto alla valutazione dell'offerta per assicurare il rispetto del principio di non discriminazione fra operatori economici di Paesi europei differenti. Tale scelta vieta di attribuire un punteggio alla reputazione dell'impresa, ma permette di definire ed eventualmente elevare i requisiti di partecipazione per tutti gli operatori economici anche con riferimenti reputazionali. La digitalizzazione può assicurare significativi elementi di trasparenza e semplificazione soprattutto della fase di qualificazione delle imprese.

Con un nuovo sistema di verifica automatica dei requisiti di qualificazione e di semplificazione della fase di selezione degli operatori economici partecipanti, le centrali d'acquisto, ma anche tutte le amministrazioni aggiudicatrici, potrebbero invece velocizzare significativamente l'aggiudicazione dei contratti pubblici. Come accennato, il coordinamento delle banche dati esistenti e la loro effettiva interconnessione in una unica Banca dati degli operatori economici consentirebbe la rapida verifica ti tutti i requisiti (con sistema a "bollino verde" per le imprese qualificate) e permetterebbe di concentrare l'attenzione sulle strategie di gare la definizione di più lotti territoriali, merceologici adeguati ai mercati di riferimento, senza determinare un aggravamento della selezione e dei suoi tempi.

La mancanza di una adeguata banca dati pubblica ha determinato lo sviluppo delle attività delle SOA (Società Organismi di Attestazione, 19 in Italia che accreditano circa 30.000 imprese). Com'è noto le SOA sono soggetti di diritto privato, che svolgono la rilevante funzione pubblicistica di rilascio di una "attestazione" per la partecipazione agli appalti pubblici di lavori di im-

porto pari o superiore a 150.000 euro (art. 84 del D.Lgs. n. 50/2016). Nell'iter di qualificazione le SOA raccolgono una gran quantità di documenti che reperiscono o direttamente dall'impresa o da altri enti pubblici (Camere di commercio, Autorità giudiziaria, Prefetture, enti previdenziali, ecc.). Spesso le stazioni appaltanti richiedono nuovamente alle imprese lo stesso tipo di documenti già in possesso delle SOA. Per favorire l'attuazione del principio *once-only* è in corso di avvio l'applicazione delle metodologie di digitalizzazione mediante *blockchain* di tutta la documentazione tenuta dalle SOA (creazione di fascicoli virtuali delle imprese, interconnesso con le principali banche dati al fine di avere una qualificazione dinamica, sempre aggiornata) per consentire l'accessibilità alla stessa da parte dell'ANAC che vigila sul settore e di tutte le stazioni appaltanti che lo richiedano. Come ricordato, la semplificazione più significativa potrebbe determinarsi con il coordinamento pubblico delle banche dati esistenti relative agli operatori economici.

3. Contratti digitali: i sistemi dinamici di acquisizione, accordi quadro e aste elettroniche

Il servizio gare (come funzione pubblica) digitalizzato potrebbe in larga parte essere svolto da centrali d'acquisto pubbliche qualificate e specializzate che operino con sistemi dinamici di acquisizione della Pubblica Amministrazione – SdaPA (art. 55 del D.Lgs. n. 50/2016, nella sezione II, artt. 54-58 sulle: *Tecniche e strumenti per gli appalti elettronici ed aggregati*). Le centrali d'acquisto o soggetti aggregatori potrebbero mettere a disposizione le selezioni elettroniche che al loro interno contengono i beni e i servizi già "garati", assolti gli obblighi europei e nazionali di imparzialità e concorrenza tra i quali sia possibile scegliere da parte dell'amministrazione utilizzatrice della prestazione. Si potrebbe così assicurare l'esercizio dell'autonomia delle singole amministrazioni nel potere di scelta anche tra più aggiudicazioni già avvenute e rese disponibili, sulla base di previe convenzioni non vincolanti, con la cosiddetta «gara delle gare» (R. CAVALLO PERIN, G.M. RACCA, 2016).

I sistemi dinamici di acquisizione, interamente elettronici, consentono infatti agli acquirenti pubblici di consultare un gran numero di potenziali fornitori di lavori, beni o servizi standardizzati ("*off-the-shelf*"), le cui capacità sono già state verificate in sede di ammissione al sistema. Il sistema dinamico di acquisizione risulta particolarmente adatto per acquisti di uso corrente e ripetitivi, permettendo al tempo stesso adattamenti alle specifiche esigenze delle amministrazioni utilizzatrici.

Un sistema dinamico può essere predisposto per categorie definite di pro-

dotti, lavori o servizi sulla base delle caratteristiche del contratto da eseguire, che possono comprendere un riferimento al quantitativo massimo ammissibile degli appalti specifici successivi o a un'area geografica specifica in cui gli appalti saranno eseguiti.

Lo SdaPA gestito dalla piattaforma di un soggetto aggregatore consente a tutte le pubbliche amministrazioni di concludere, attraverso un processo completamente elettronico, gare d'appalto al di sopra delle soglie europee, invitando gli operatori economici che, ammessi al sistema (qualificati), hanno la possibilità di accedere alle gare in qualsiasi momento e formulare la relativa offerta.

Lo SdaPa è articolato in due fasi. La prima comprende la pubblicazione di un bando sulla Gazzetta Ufficiale dell'Unione Europea, che apre alla partecipazione di qualsiasi operatore economico che ne richieda l'ammissione e che soddisfi i criteri di selezione stabiliti senza limiti al numero dei candidati ammessi assicurando trasparenza, ampia partecipazione e concorrenzialità, rispetto ad un elenco di operatori economici "qualificati".

La seconda fase si caratterizza per l'indizione e aggiudicazione di appalti specifici a seguito di un confronto concorrenziale tra gli operatori economici ammessi al sistema applicando la disciplina prevista per la procedura ristretta (art. 61 del D.Lgs. n. 50/2016). Questa seconda fase potrebbe essere utilmente coordinata e gestita anche localmente dai soggetti aggregatori regionali. Si concilierebbe così l'esigenza di efficienza del sistema con le scelte di autonomia sulla strategia di gara sulla dimensione e articolazione dei lotti in ambito regionale.

La legge di bilancio 2019 ha infatti ampliato il numero dei soggetti invitati a fare ricorso agli strumenti elettronici e centralizzati di acquisto e negoziazione. In particolare, le amministrazioni statali centrali e periferiche – comprese le Università e le scuole di ogni ordine e grado – ove disponibili potrebbero approvvigionarsi attraverso gli accordi quadro stipulati da Consip oppure mediante lo SdaPa, anche in coordinamento con le Regioni.

Tali sistemi potrebbero essere istituiti anche al fine di promuovere l'acquisto di prodotti innovativi a favore delle amministrazioni italiane ed europee, in attuazione degli strumenti giuridici di cooperazione negli appalti tra amministrazioni di Stati membri differenti disciplinati dalle Direttive (art. 39 della Direttiva 2014/24/UE).

Attualmente, esempi di SdaPA attivi della centrale di committenza nazionale Consip includono ventuno principali categorie di prodotti, sei delle quali dedicate al settore sanitario e farmaceutico. In particolare, negli ultimi anni gli acquisti di farmaci sulla piattaforma elettronica hanno consentito alle pubbliche amministrazioni sanitarie di concludere 173 gare d'appalto per l'acquisto di 6.360 prodotti farmaceutici, per un valore di acquisto complessivo di 10,3

miliardi di euro e le potenzialità di sviluppo sarebbero notevoli con un migliore coordinamento nel Tavolo dei soggetti aggregatori. I soggetti aggregatori regionali spesso infatti aggiudicano gare negli stessi settori in cui è già presente una gara Consip, mentre un sistema di specializzazione potrebbe consentire, in particolari settori, che gli stessi soggetti aggregatori operino a favore di tutte o parte delle altre Regioni, con evidenti risparmi di spesa e vantaggi legati alla maturata conoscenza degli specifici settori di mercato di competenza.

Le potenzialità dello SdaPa sono state ampliate dalla legge di bilancio 2019 che ha consentito l'aggiudicazione di accordi quadro tramite sistema dinamico di acquisizione. In precedenza, l'utilizzo di tale strumento era limitato all'aggiudicazione di appalti specifici ad un unico concorrente, vale a dire il primo in graduatoria. Di conseguenza, le stazioni appaltanti non potevano acquistare sullo SdaPa ad esempio i farmaci biologici, per i quali – in base alla Legge di Stabilità 2017 – era previsto l'obbligo di ricorso allo strumento dell'accordo quadro, con l'esclusione del sistema dinamico. La novità della legge di bilancio 2019 apre nuovi e interessanti scenari per le centrali d'acquisto regionali, anche a favore delle aziende sanitarie nella scelta dei modelli di approvvigionamento più adatti a rispondere alle proprie esigenze.

In particolare, per acquisire tutte le tipologie di farmaci (inclusi, a partire dal 30 gennaio 2019, i farmaci biologici) le amministrazioni potranno, tramite lo Sdapa, scegliere autonomamente la struttura di gara, differenziandola, se opportuno, per singoli lotti merceologici o funzionali e secondo le tecniche di aggiudicazioni più funzionali allo strumento dell'accordo quadro (aperto, chiuso, con uno o più operatori, si tratta di uno strumento che permette di selezionare gli operatori economici in una prima fase, che a differenza del sistema dinamico si chiude, ed una seconda fase in cui si aggiudica il lotto a uno o più operatori che restano in graduatoria e che potranno essere interpellati dalle amministrazioni interessate alla prestazione, art. 54, aste elettroniche, art. 56 e cataloghi elettronici, art. 57, dello stesso codice, D.Lgs. n. 50/2016). Tali possibilità, oltre ad aumentare la flessibilità dello strumento dell'accordo quadro, si aggiungono ai già numerosi vantaggi offerti dallo SdaPa in termini di velocizzazione, razionalizzazione e coordinamento del processo di acquisto nonché di promozione dell'accessibilità e trasparenza delle informazioni contrattuali.

Come ricordato, i vantaggi della digitalizzazione e automatizzazione dei procedimenti si rivela utile anche nella fase di valutazione delle offerte con riferimento agli elementi di qualità misurabile e quindi valutabili oggettivamente in automatico, mentre l'intermediazione umana delle commissioni giudicatrici potrebbe restare a presidio e correzione degli esiti anomali e per le verifiche dei campioni necessari in settori come la sanità. Nello specifico, il ricorso agli al-

goritmi già in uso da parte delle centrali d'acquisto pubbliche consentirebbe di conoscere e standardizzare le migliori scelte, valide per amministrazioni omologhe, per i comuni più piccoli come per le aziende sanitarie o per i ministeri, distinguendo gli acquisti nei vari settori pubblici. Tramite i meccanismi di *machine learning* errori o prassi inefficienti potrebbero essere individuati e corretti rapidamente dando consistenza ai principi di efficienza e correttezza, fondamentali per rendere il fenomeno corruttivo in senso ampio (*maladministration, come incapacità e non solo corruzione in senso proprio*) un momento patologico e non così diffuso come oggi nella funzione appalti.

Consip S.p.A. gestisce anche l'*e-marketplace* "Mercato Elettronico della pubblica amministrazione – MEPA" normalmente impiegato dalle amministrazioni aggiudicatrici per gli acquisti di valore molto basso e che perciò si presta a soddisfare esigenze percepite come urgenti. L'introduzione del MEPA è stata certamente utile in quanto ha determinato risparmi sui processi e sulle risorse rispetto ai metodi di negoziazione tradizionali e la possibilità di un monitoraggio dettagliato della spesa pubblica tramite una costante acquisizione di dati. Tuttavia, le caratteristiche del portale si prestano ad un utilizzo improprio generando possibilità di frammentazione abusiva degli acquisti per rimanere sotto soglia.

Per evitare i limiti del MEPA, è necessario introdurre un portale elettronico di negoziazione, basato sul modello già testato dello SdaPa, per qualificare le imprese e per poter disporre di uno scaffale di beni (sul modello "*Amazon*") anche al fine di evitare che fornitori improvvisati possano acquistare sugli *e-commerce* privati per poi rivendere tali prodotti sul MEPA. Tale sistema, unendo i benefici della semplificazione e dell'immediatezza caratteristici dei portali privati, assicurerebbe la verifica dei requisiti già elaborata in seno allo SdaPa, consentirebbe di ottenere sistemi di gara digitalizzati con la verifica della qualificazione delle imprese istantanea e aggiornata, in tempo reale, e la selezione fra prestazioni già pronte per l'acquisto, escludendo la necessità di procedere con richieste di offerta.

La definizione di strategie di acquisto pubblico fondate sulle specifiche caratteristiche dei mercati di riferimento può favorire l'attivazione di sistemi dinamici di acquisizione, anche con lotti molto piccoli, da mettere a disposizione su piattaforme elettroniche, in relazione alle esigenze dei piccoli comuni e sotto il coordinamento dei soggetti aggregatori per favorire la qualità della contrattazione nell'interesse dei cittadini e delle imprese. Evoluzione che potrebbe perciò accompagnare il nuovo MEPA, trasformato in SdaPA sul modello tipo "*Amazon* pubblico" a sviluppare gare aggregate seppur con lotti anche di valore limitato, proprio a favore di piccole e microimprese e delle relative innovazioni sostenibili. L'adeguata pianificazione e verifica dei requisiti

oggettivi e soggettivi consentirebbe anche una più attenta analisi della domanda pubblica, evitando rischi di apertura a imprese private che intendano qualificarsi come centrali di committenza. La funzione appalti risulta infatti strategica al perseguimento di obiettivi di qualità in una visione sistemica di politica industriale che non pare opportuno cedere al mercato degli operatori privati, come di recente riconosciuto dalla Corte di giustizia (CGUE, sentenza del 4 giugno 2020, c-3/19, Asmel c. ANAC).

La digitalizzazione dei contratti pubblici richiede di coordinare le attività, in parte già intraprese, delle centrali di committenza nazionali con i soggetti aggregatori regionali specializzati e per taluni settori chiamati ad operare per l'intero territorio nazionale e per l'Europa, anche per promuovere le imprese più innovative. La contrattazione e l'acquisto avverrebbero direttamente su piattaforme elettroniche, consentendo agli amministratori pubblici di scegliere dal portale *online* i beni e servizi per i quali la gara è già stata svolta, a monte, e secondo le loro esigenze di quantità e qualità.

Una "funzione appalti" aggregata e qualificata che assicuri una effettiva autonomia nella scelta fra più "negozi elettronici" ove, con l'aggiudicazione di gare aggregate vengano selezionate (mediante accordi quadro o sistemi dinamici di acquisizione) le prestazioni di interesse e l'adesione sia semplificata, assicurando l'effettività dei principi della contrattazione pubblica, anche elettronica, ma basata su gare e algoritmi pubblici. Tali piattaforme potrebbero favorire la cooperazione europea e consentire l'accesso per valori e prodotti definiti anche ad amministrazioni di Stati membri differenti offrendo significative occasioni di sviluppo alle imprese inserite negli SdaPA. Anche le aste elettroniche, per singole specifiche prestazioni ed i cataloghi elettronici, sempre relativamente a beni in acquisto su portali elettronici potrebbero integrare il sistema. Un mercato europeo di adesione a gare svolte in Italia e messe a disposizione di altri Stati membri che assicurerebbe una nuova occasione di sviluppo per le imprese più innovative.

La disponibilità di piattaforme telematiche nella gestione delle procedure di gara è stata inserita fra gli elementi necessari e non più solo premianti per la qualificazione delle stazioni appaltanti (art. 8, comma 5, D.L. n. 76/2020, c.d. "Semplificazioni", che modifica l'art. 38 del D.Lgs. n. 50/2016). Come ricordato, il sistema di qualificazione non è ancora attuato, ma il riferimento alla necessità di disporre di piattaforme telematiche evidenzia una maturata consapevolezza verso la digitalizzazione dell'intero ciclo dei contratti pubblici.

4. La modellazione digitale per gli appalti di lavori e gli *smart contracts* (accordi collaborativi)

Come accennato, le tecnologie e metodologie digitali possono incidere in maniera significativa sulla domanda pubblica nella sua definizione e realizzazione in una prospettiva più integrata e collaborativa fra amministrazioni pubbliche, ma anche con gli operatori economici. Nel settore dei lavori pubblici una delle innovazioni più promettenti dal punto di vista giuridico, economico e tecnico pare riconducibile al *Building Information Modeling* (*BIM*).

La disciplina europea sugli appalti pubblici richiama con favore l'adozione di nuove tecnologie e richiede di ridefinire i modelli giuridici che possono disciplinare la cooperazione ed affrontare le difficoltà derivanti dall'uso della metodologia *BIM* ("*Legal BIM*"). La metodologia *BIM* negli appalti pubblici di lavori incide sulla definizione di tutti i documenti di gara, dai documenti preliminari alla progettazione fino a tutta l'esecuzione e la successiva gestione dell'opera (appalto di servizi, es. *facility management*) (G.M. DI GIUDA, G.M. RACCA, 2019).

La modellazione digitale può utilmente applicarsi anche agli appalti di servizi. Il codice dei contratti pubblici ha previsto «la razionalizzazione delle attività di progettazione e delle connesse verifiche attraverso il progressivo uso di metodi e strumenti elettronici specifici quali quelli di modellazione per l'edilizia e le infrastrutture» (art. 23, comma 1, lett. h), D.Lgs. n. 50/2016). Tali strumenti si caratterizzano per l'utilizzo di piattaforme interoperabili a mezzo di formati aperti non proprietari, al fine di non limitare la concorrenza tra i fornitori di tecnologie e per il coinvolgimento di specifiche progettualità adottate dai differenti progettisti.

La legge di bilancio 2019 ha previsto l'ampliamento dell'ambito operativo di Consip, estendendo anche al settore dei lavori pubblici l'utilizzo degli strumenti di acquisto e negoziazione, quindi con possibile aggregazione anche per i lavori, che potrebbe essere utilmente digitalizzata.

La transizione digitale per il settore delle costruzioni rappresenta un'opportunità di efficienza e sviluppo per un settore che vale oltre il 10% del Prodotto Interno Lordo nazionale e che ha ricadute significative anche sulla sostenibilità ambientale. Già il Codice dei contratti pubblici richiamava l'introduzione della metodologia della Modellazione Informativa (*Building Information Modeling*) con lo specifico obiettivo di migliorare la qualità progettuale per limitare ritardi, varianti, illegittimità e contenzioso nei contratti di lavori, sia in fase di progettazione, sia nella procedura di scelta del contraente (c.d. tempi di attraversamento), sia in fase di esecuzione del contratto. I dati relativi all'efficientamento dei tempi e dei costi derivanti dalla digitalizzazione dei progetti e dei processi definiscono risparmi intorno al 20% che, se rapportato

al PIL potrebbe assicurare un recupero intorno al 2%. L'introduzione del BIM nei processi delle costruzioni rappresenta un cambio di paradigma sostanziale, poiché ad oggi gran parte dello scambio di informazioni è ancora basato su carta, specialmente nelle fasi preliminari del procedimento.

Una graduale introduzione della modellazione digitale (*BIM*) nella progettazione di opere pubbliche va accompagnata da una adeguata formazione per il corretto impiego di queste tecnologie assicurando altresì incentivi ai Responsabili Unici del Procedimento ed alle relative unità di supporto (art. 31, comma 9 e art. 113, comma 4, D.Lgs. n. 50/2016). Si prevede l'obbligatorietà di tali strumenti solo per progetti complessi con un valore di gara pari o superiore a 100 milioni di euro, a partire dal 2019. Tuttavia, la disciplina non pare ancora chiarire in maniera esaustiva le conseguenze applicative del *BIM* negli appalti pubblici e le sue prime applicazioni nelle gare pubbliche hanno suscitato un primo contenzioso chiarificatore (T.A.R. Lombardia, sez. I, sentenza 29 maggio 2017, n. 1210).

L'utilizzo di tali innovative metodologie presuppone l'effettiva adeguatezza dell'amministrazione aggiudicatrice, che spesso potrebbe non coincidere con il destinatario dell'opera, come nel caso dei piccoli comuni, e la capacità del gruppo di operatori economici che potrebbe integrare differenti professionalità (anche Piccole e Medie Imprese) secondo modelli collaborativi innovativi. La modellazione delle informazioni costituisce pertanto uno strumento strategico volto allo sviluppo di forme di cooperazione tra pubbliche amministrazioni e soggetti privati nel perseguimento del comune obiettivo di realizzazione tempestiva e di efficiente gestione delle opere pubbliche.

Il *BIM* è stato descritto come una metodologia che consente *la rappresentazione digitale delle caratteristiche fisiche e funzionali di un edificio*. Può essere considerato una risorsa capace di offrire conoscenza condivisa e informazioni riguardo uno specifico edificio che funge da affidabile base dati di riferimento per il processo decisionale lungo tutto il ciclo di vita dell'edificio, dalla pianificazione e progettazione fino alla gestione (*National BIM Standard – U.S.*). Questa metodologia di progettazione consente all'utente di compiere valutazioni più analitiche ed efficaci rispetto a quelle possibili sulla base delle tradizionali metodologie di progettazione (*Computer – Aided Design, CAD*). Non di secondario rilievo appare la possibilità di ottenere una migliore qualità nella progettazione a costi ridotti e con tempi di esecuzione più brevi.

Il *Builiding Information Modeling* può essere inteso secondo differenti accezioni complementari. Il *BIModel* può costituire una rappresentazione digitale, perciò identificandone un modello, delle caratteristiche fisiche e funzionali di un edificio, individuando oggetti digitali capaci di fornire tutte le informazioni rilevanti.

In secondo luogo, può identificare uno strumento di E-*Modeling*. In questo senso, il *BIModeling* rappresenta una metodologia, dunque l'insieme dei processi collaborativi richiesti per creare ed utilizzare un modello elettronico di uno specifico edificio.

Da un terzo punto di vista, esso è inteso quale sistema gestionale delle informazioni. In questa prospettiva il *BIManagement* permette la gestione e il monitoraggio degli edifici mediante l'utilizzo di un modello digitale di scambio di informazioni tra tutti i soggetti coinvolti nell'intero ciclo di vita dell'opera. Gli strumenti digitali consentono di raccogliere informazioni più precise e di processarle meglio, aumentando il livello di efficacia e razionalità della risposta delle pubbliche amministrazioni ai bisogni nell'interesse pubblico. Sotto differente profilo è possibile ridurre le informazioni dubbie che potrebbero generare incertezze e problemi interpretativi, che spesso riguardano il completamento di edifici progettati con tecniche tradizionali, nonché le difformità e gli errori che potrebbero emergere nella fase esecutiva, con varianti, costi supplementari, ritardi e contenzioso.

Il *BIM* favorisce una pianificazione, progettazione, costruzione, gestione e manutenzione più efficienti mediante l'impiego di un modello informativo standardizzato in formato digitale per ciascun edificio, nuovo o esistente, che contiene tutti i dati sull'edificio in questione e li mette a disposizione in un formato utilizzabile da tutti gli interessati durante l'intero ciclo di vita dell'edificio.

Dal punto di vista giuridico è importante osservare che l'*Information Modeling* può assicurare una collaborazione ottimale tra i vari soggetti coinvolti nelle attività di progettazione, esecuzione e gestione del contratto, garantendo la predisposizione di infrastrutture di dati aperti e riutilizzabili in grado di assicurare un maggiore coordinamento e un migliore monitoraggio delle attività in tutte le fasi, dalla pianificazione alla definizione dei vari livelli progettuali da mettere a gara (*Alliance Frameworks*). Ciò consente di procedere ad una oggettiva e trasparente selezione e valutazione delle offerte e con la conseguente aggiudicazione ed esecuzione (*Alliance Management*). I sistemi di modellazione digitale consentono e tracciano soltanto modifiche specificamente individuate, che possano risultare utili in un quadro giuridico di collaborazione e cooperazione, contestualmente assicurando trasparenza e tracciabilità (G.M. DI GIUDA, S. VALAGUZZA, 2019).

Queste tecnologie favoriscono anche la redazione dei cosiddetti *smart contracts* (ossia i contratti redatti sulla base della tecnologia *blockchain*, v. capitolo X, B. CAPPIELLO e G. CARULLO), in cui dati e informazioni sono raccolti in una catena di blocchi e resi disponibili senza alcuna limitazione temporale. Tali contratti potrebbero assicurare quella certezza giuridica che con-

sente di registrare tutti i dati relativi alle parti coinvolte. La cosiddetta "transizione digitale" verso la modellazione informativa richiede un adattamento dal punto di vista procedimentale. Perciò gli strumenti di modellazione digitale devono integrarsi nei modelli organizzativi e trovare applicazione nei procedimenti amministrativi volti all'individuazione dei fabbisogni e in quelli relativi alla conseguente selezione del contraente ed esecuzione del contratto.

La modellazione informativa non introduce un mero strumento applicativo. Di qui le difficoltà connesse alla transizione digitale che per ciò stesso richiedono una profonda innovazione dei procedimenti amministrativi favorendo la trasparenza ed il superamento di molte delle criticità legate all'insufficiente precisione e qualificazione della domanda pubblica messa a gara. La definizione modellata della domanda pubblica richiede la trasformazione in dati di tutti gli elementi qualitativi per assicurare valutazioni oggettive, superando i rischi di arbitrio soprattutto con riferimento agli elementi di qualità non misurabile (D.I. GORDON, G.M. RACCA, 2014).

Dal punto di vista giuridico la possibilità di disporre e scambiare informazioni è la chiave per garantire trasparenza, efficienza e integrità lungo tutta la procedura d'appalto. In questa prospettiva, la modellazione informativa favorisce l'osservanza dei principi fondamentali che le pubbliche amministrazioni sono tenute a rispettare nel settore degli appalti pubblici, quali il principio di correttezza, trasparenza, concorrenza ed economicità. La trasparenza e condivisione dei dati permette di instaurare un accordo di cooperazione che, dopo l'aggiudicazione, individui gli obiettivi comuni e incentivi la tempestiva e corretta esecuzione del contratto, con conseguente superamento dei comportamenti opportunistici che tradizionalmente si instaurano dal giorno successivo all'aggiudicazione, per la massimizzazione del profitto dell'impresa ed il recupero con le varianti del ribasso proposto in gara.

Da segnalare che il menzionato D.L. n. 76/2020, c.d. Semplificazioni ha previsto la costituzione obbligatoria di collegi consultivi tecnici con funzioni di assistenza nell'esecuzione per tutti i lavori pubblici, obbligatori sopra soglia europea (e facoltativi sottosoglia e per la procedura selettiva), i cui componenti andranno scelti fra ingegneri, architetti, giuristi ed economisti esperti di appalti, anche con riferimento «alla specifica conoscenza di metodi e strumenti elettronici quali quelli di modellazione per l'edilizia e le infrastrutture (BIM)» (art. 6). Si evidenzia così una maturata consapevolezza sulla necessità della transizione digitale per assicurare efficienza nell'esecuzione, ma anche per impostare fin dell'inizio la realizzazione delle opere pubbliche, con la qualificazione della domanda pubblica e la chiarezza digitale del progetto che si intende realizzare.

La digitalizzazione dei requisiti è un aspetto fondamentale per garantire la

tracciabilità delle informazioni lungo tutto il processo e per passare dall'approccio *document-based* a quello *model-based*. La digitalizzazione delle specifiche progettuali dei capitolati tecnici e della conseguente fase di direzione lavori renderebbe trasparente il complesso della procedura. L'uso della modellazione informativa nella fase di scelta del contraente garantisce trasparenza, tracciabilità e oggettività nella valutazione delle offerte poiché si sviluppa a monte nella definizione di criteri, sub-criteri, modalità di valutazione, metodi e formule per l'attribuzione dei punteggi. In tali gare i ribassi sono minimi perché la domanda pubblica è precisa e, come anticipato, non vi è spazio successivo per il recupero del ribasso con le varianti: la procedura selettiva diviene così un momento di effettiva trasparenza e concorrenza fra gli operatori economici.

L'integrazione della metodologia BIM con forme contrattuali collaborative garantisce una maggiore efficienza dell'impiego dello strumento, aumentando la collaborazione tra committenti, imprese e filiera dei sub-contraenti, con una maggiore trasparenza di tutta l'organizzazione. Considerando la fase di costruzione del bene, l'integrazione della modellazione informativa con un *Document Management System* (DMS) assicura la tracciabilità delle informazioni e dei documenti tra le parti, facilitandone l'acquisizione, la condivisione e la consultazione da parte di tutti i soggetti coinvolti nella procedura.

La digitalizzazione dei processi potrebbe integrare l'approccio BIM con la tecnologia *Blockchain*, che tramite l'applicazione degli *Smart Contracts* potrebbe ulteriormente sviluppare una automazione certificata del procedimento e del ciclo del contratto assicurando il coordinamento tra le parti e l'efficienza nell'esecuzione, evitando come ricordato i comportamenti opportunistici connessi alla scarsa qualità e alle lacune del progetto, riducendo i tempi di esecuzione ed il contenzioso.

L'introduzione della modellazione informativa deve partire dall'analisi degli obiettivi specifici del committente e quindi dalla definizione dei risultati previsti. Per garantire la corretta strutturazione dell'approccio BIM, è opportuno predisporre modelli tipo, linee guida specifiche, a seconda del committente, basate sull'analisi dei procedimenti per la modellazione di edifici nuovi da realizzare, ovvero esistenti da gestire e manutenere. Le linee guida consentono di verificare i criteri di modellazione e quindi la validazione dei modelli e possono essere definite per la gestione di patrimoni esistenti, con l'obiettivo della gestione e della manutenzione dei beni, oppure per la modellazione di nuovi insediamenti, con l'obiettivo di creare uno standard specifico. Sarebbe così possibile strutturare e digitalizzare le procedure per la verifica semi-automatica dell'osservanza delle normative vigenti sulla sicurezza, antincendio, ecc. La definizione di un modello informativo consente inoltre di combinare dati geometrici e informazioni, facilitando simulazioni strutturate, combinando l'ap-

proccio BIM con i dati raccolti da sensori di vario tipo. In tal modo il modello diventa *repository* e facilita il tracciamento e l'aggiornamento costante dei dati, fornendo altresì una modalità di rappresentazione facilitata, consentendo di visualizzare i dati in uno spazio effettivo.

Simulazioni di *Post-Occupancy* consentono di migliorare l'uso e la gestione degli spazi, sulla base dell'effettiva occupazione e della qualità ambientale interna (*Indoor Environmental Quality* – IEQ) rilevata dai sensori. Le simulazioni tengono inoltre in considerazione anche gli spostamenti degli utenti all'interno degli edifici, simulando i flussi di ingresso, di uscita, e di spostamento. Il modello informativo può fornire una base costantemente aggiornata per la gestione degli edifici tenendo in considerazione in un approccio dinamico e *data-based* tutti gli aspetti caratterizzanti, quali geometria, condizioni interne, presenza e spostamento degli utenti.

Il modello si configura quindi come un gemello digitale (*digitaltwin*) dell'edificio reale, in grado di simularne qualsiasi fase del ciclo di vita (costruzione, logistica, ottimizzazione dei flussi, operatività, gestione delle emergenze), includendo dati in tempo reale provenienti dai sensori e tracciando la vita dell'edificio (G.M. DI GIUDA, 2019).

5. La digitalizzazione per un rinnovato rapporto di collaborazione e fiducia tra amministrazioni ed operatori economici nell'interesse pubblico

Come ricordato, anche a legislazione invariata, le gare "native digitali" possono già essere svolte dalle centrali d'acquisto (Consip e altri soggetti aggregatori) attraverso piattaforme elettroniche, con gli strumenti contrattuali già previsti e di recente riformati e sviluppati dall'ultima legge di bilancio, principalmente attraverso i sistemi dinamici di acquisizione, le aste elettroniche e i cataloghi elettronici.

La qualificazione digitale tecnica, economica, morale, finanziaria e reputazionale degli operatori economici, accertata in modo oggettivo attraverso il coordinamento delle banche dati pubbliche e private disponibili potrebbe fondare un nuovo patto di fiducia tra amministrazioni pubbliche e imprese.

Un accreditamento digitale nel sistema può consentire agli operatori economici di presentare le relative offerte in tempi molto rapidi ove il procedimento di valutazione delle stesse venga strutturato su criteri di qualità misurabile, perciò assicurando valutazioni largamente automatizzate, riservando alle commissioni giudicatrici un ruolo solamente in attività peculiari, ad esempio ove sia necessario testare dei campioni.

Le centrali d'acquisto potrebbero concentrarsi sull'analisi delle *supply chains*, sull'elaborazione delle strategie di gara, sulla definizione di lotti territoriali o merceologici, basati sulle caratteristiche specifiche dei mercati di riferimento – favorendo forme di cooperazione tra soggetti aggregatori per assicurare la qualità delle prestazioni e l'innovazione.

La trasparenza e tracciabilità connessa alla modellazione digitale permette di instaurare rapporti di collaborazione e fiducia con gli operatori economici nel comune obiettivo della qualità e tempestività delle prestazioni e del riconoscimento del corrispettivo con pagamenti celeri a tutta la filiera. La qualità della realizzazione delle opere sarà valorizzata anche nella successiva gestione, che vedrà ridotti i costi di manutenzione mediante la sensoristica e le valutazioni predittive per la sostituzione di parti obsolescenti.

Dalle opere pubbliche con i relativi servizi e forniture la digitalizzazione incide e si integra con il territorio e le città "intelligenti", o *smart*, che mirano a migliorarne efficienza e competitività, proprio sulla base dell'uso strategico di tecnologie digitali innovative.

L'uso delle tecnologie nei differenti contratti pubblici genera e integra i *big data* per la gestione dei flussi sino alla prospettazione di veri e propri meccanismi di monitoraggio anche predittivi dell'evoluzione delle città e dei territori. Poiché l'intelligenza della città può essere combinata con una «maggiore efficacia» della gestione delle questioni urbane, la raccolta della grande quantità di dati si collega alla trasparenza semplificata dell'uso degli stessi (G.M. RACCA, R. CAVALLO PERIN, 2019).

Tali approcci possono contribuire a sviluppare le strategie delle *smart cities* aprendo a nuove analisi giuridiche che si avvalgono del controllo pubblico sui dati e sulle tecnologie. La modellazione digitale insieme agli *smart contracts* operanti in connessione con gli strumenti di gestione del territorio e di sensoristica nella *smart city* assicura l'acquisizione di *big data* che consentono una visione capillare della realtà dei fatti che permettono di assumere decisioni pubbliche maggiormente rispondenti alle esigenze da soddisfare.

Il principio di trasparenza dell'informazione nel settore pubblico si riferisce, infatti, alla disponibilità universale dei dati che le nuove intelligenze gestiscono ed elaborano, permettendo di sviluppare analisi per sviluppare e proporre ai decisori le innovazioni più opportune. Le amministrazioni pubbliche digitalizzate possono agire come prime produttrici, con la ricerca e sviluppo e gli appalti pre-commerciali (PCP), prime acquirenti con gli appalti innovativi (PPI) da integrare nella pianificazione di tutti i servizi connessi (J.B. AUBY, 2019).

La modellazione digitale richiede qualificazione e integrazione sia dal lato della domanda, sia dell'offerta, richiama il superamento della singola stazione

appaltante che stipula i suoi contratti, sia del singolo operatore economico che partecipa alla gara pubblica, favorendo l'aggregazione fra amministrazioni in centrali d'acquisto, sia tra imprese tecnologicamente adeguate per collaborare alla sinergica e tempestiva esecuzione delle prestazioni (G.M. RACCA, S. PONZIO, 2019). La stessa condivisione dei dati mediante modellazione e sistemi di *blockchain* assicura un approccio collaborativo che supera i comportamenti opportunistici e conflittuali ancora esistenti fra amministrazioni, progettisti, esecutori dell'appalto. L'instaurazione di una filiera in cui tutti i soggetti apportano informazioni e accedono ai dati prodotti dagli altri accresce il valore complessivo della conoscenza condivisa e richiede una relazione di fiducia volta al comune obiettivo della realizzazione delle prestazioni.

La digitalizzazione dei contratti pubblici integrata nei territori può determinare un forte impatto sull'organizzazione pubblica che vedrà le infrastrutture tradizionali affiancate e supportate sempre più dalla corrispondente "meta-infrastruttura digitale" integrata nelle pianificazioni *smart* previste per la gestione dei territori e dei servizi per soddisfazione dei bisogni dei cittadini.

Bibliografia

AUBY J.B., *Conclusion en forme d'hypothèses*, in J.B. AUBY (a cura di), *Le futur du droit administratif*, LexisNexis, Paris, 2019, pp. 563-576.

AUBY J.B., *Public contracts and smart cities*, in G.M. RACCA, C.R. YUKINS (a cura di), *Joint public procurement and innovation: lessons across borders*, Bruylant, Bruxelles, 2019, pp. 187-194.

CAVALLO PERIN R., *Ordinamenti giuridici paralleli e necessità come fonte del diritto*, in R. CAVALLO PERIN, G. COLOMBINI, F. MERUSI, A. ROMANO (a cura di), *Attualità e necessità del pensiero di Santi Romano Pisa 14-15 giugno 2018*, Editoriale Scientifica, Napoli, 2019, pp. 41-55.

CAVALLO PERIN R., RACCA G.M., *Smart cities for an intelligent meeting of social needs*, in J.B. AUBY (a cura di) *Le futur du droit administratif*, LexisNexis, Paris, 2019, pp. 431-437.

CAVALLO PERIN R., RACCA G.M., *Administrative Cooperation in the Public Contracts and Service Sectors for the Progress of European Integration*, in F. MERLONI, A. PIOGGIA (a cura di), *European Democratic Institutions and Administrations*, Giappichelli, Torino, 2018.

DI GIUDA G.M. (a cura di), *Introduzione al BIM. Protocolli di modellazione e gestione informativa*, Società Editrice Esculapio, Bologna, 2019.

DI GIUDA G.M., RACCA G.M., *From Works Contracts to Collaborative Contracts: The Challenges of Building Information Modeling (Bim) in public procurement*, in G.M. RACCA, C.R. YUKINS (a cura di), *Joint public procurement and innovation: lessons across borders*, Bruylant, Bruxelles, 2019, pp. 223-271.

DI GIUDA G.M., VALAGUZZA S., *Gli accordi collaborativi come elemento cruciale per una regolazione strategica nel settore delle costruzioni*, Edizioni Scientifiche Italiane, Napoli, 2019.

DI GIUDA G.M., MALTESE S., RE CECCONI F., VILLA V., *Il BIM per la gestione dei patrimoni immobiliari. Linee guida, livelli di dettaglio informativo grafico (lod) e alfanumerico (loi)*, Hoepli, Milano, 2017.

DONATO L. (a cura di), *Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia. Gli appalti pubblici tra istanze di semplificazione e normativa anticorruzione. Alla ricerca di un equilibrio tra legalità ed efficienza*, 2020.

GORDON D.I., RACCA G.M., *Integrity Challenges in the EU and U.S. Procurement systems*, in G.M. RACCA, C.R. YUKINS (a cura di), *Integrity and Efficiency in Sustainable Public Contracts. Balancing Corruption Concerns in Public Procurement Internationally*, Bruylant, Bruxelles, 2014, pp. 117-145.

KOTSONIS T., *EU procurement legislation in the time of COVID-19: fit for purpose?*, in *P.P.L.R.*, 2020, 4, pp. 199-212.

LOCATELLI I., *Process Innovation Under the New Public Procurement Directives*, in G.M. RACCA, C.R. YUKINS (a cura di), *Joint public procurement and innovation: lessons across borders*, Bruylant, Bruxelles, 2019, pp. 31-63.

MERUSI F., *Integration between EU law and national administrative legitimacy*, in *Ius Publicum Network Review*, 2013, 2.

OROFINO A.G., GALLONE G., *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giur. it.*, 2020, 7.

OROFINO A.G., *La semplificazione digitale*, in *Il diritto dell'economia*, 2019, 3, pp. 87-111.

ORSONI G., D'ORLANDO E., *Nuove prospettive dell'amministrazione digitale:* Open Data *e algoritmi*, in *Ist. del Federalismo*, 2019, 3, pp. 593-617.

PONZIO S., *Joint Procurement and Innovation in the new EU Directive and in some EU-funded projects*, in *Ius Publicum Network Review*, 2014, 2.

RACCA G.M., *I contratti pubblici collaborativi e le prospettive innovative della modellazione digitale (*Building Information Modeling, *BIM)*, in G.F. FERRARI (a cura di), *Smart City. L'evoluzione di un'idea*, Mimesis, Milano-Udine, 2020, pp. 581-600.

RACCA G.M., *La modellazione digitale per l'integrità, l'efficienza e l'innovazione nei contratti pubblici*, in *Ist. del Federalismo*, 3, 2019, pp. 739-766.

RACCA G.M., YUKINS C.R. (a cura di), *Joint public procurement and innovation: lessons across borders*, Bruylant, Bruxelles, 2019.

RACCA G.M., PONZIO S., *La scelta del contraente come funzione pubblica: i modelli organizzativi per l'aggregazione dei contratti pubblici*, in *Dir. amm.*, 2019, 1, pp. 33-82.

RACCA G.M., YUKINS C.R. (a cura di), *Integrity and Efficiency in Sustainable Public Contracts. Balancing Corruption Concerns in Public Procurement Internationally*, Bruylant, Bruxelles, 2014.

ROMANO A., *Autonomia nel diritto pubblico*, in *Dig. Disc. pubbl.*, 1987.

SMITH C., PENAGOS N., MARCHESSAULT L., HAYMAN G., *Improving emergency procurement: an open data-driven approach*, in *P.P.L.R.*, 2020, 4, pp. 171-179.

XII.

IL PROCESSO AMMINISTRATIVO TELEMATICO

Federico Gaffuri

SOMMARIO: 1. La disciplina normativa del PAT. – 1.1. Il D.P.C.M. 16 febbraio 2016, n. 40, e le modifiche successive. – 2. Il Sistema Informativo della Giustizia Amministrativa. – 3. Il fascicolo informatico e il registro generale dei ricorsi. – 4. L'atto processuale informatico. – 5. La procura alle liti. – 6. Le notificazioni telematiche. – 7. Il domicilio digitale. – 8. Il domicilio digitale della P.A. – 9. Il deposito telematico. – 10. Le comunicazioni telematiche. – 11. Copie degli atti, verbale informatico e provvedimenti del giudice. – 12. L'Adunanza plenaria e il PAT.

1. La disciplina normativa del PAT

L'entrata in vigore, il 1° gennaio 2017, del processo amministrativo telematico (comunemente indicato anche con l'acronimo PAT) e cioè, in concreto, dell'obbligo di redigere gli atti e di eseguire gli adempimenti processuali inerenti ai giudizi di primo e secondo grado davanti all'autorità giudiziaria amministrativa con modalità telematiche è il punto di approdo di una complessa e, come si dirà, non sopita evoluzione normativa composta da disposizioni, di rango primario e secondario, interconnesse, anche se non sempre tra loro coordinate.

Il PAT deve essere considerato la naturale declinazione tecnologica del processo amministrativo (D. D'ALESSIO, 2017). L'uso degli strumenti informatici nel predetto rito ha, infatti, comportato una "dematerializzazione" pressoché totale degli atti processuali (ovvero la trasposizione della loro forma analogica in forma digitale e l'attribuzione di valore legale esclusivamente a quest'ultima modalità di predisposizione e deposito degli atti), ma ha lasciato in sostanza inalterate le norme di procedura e gli istituti da esse definiti. In linea di principio sono tre i capisaldi del PAT: la "neutralità" dello strumento telematico rispetto alla disciplina generale del processo amministrativo; il conferimento di

rilevanza ed efficacia formale unicamente agli atti digitali; l'utilizzo esclusivo dei mezzi di trasmissione elettronica.

Il giudizio amministrativo *paperless* – come si è osservato – non è stato concepito ed introdotto dal legislatore *ex abrupto* e con un solo provvedimento, ma è il risultato di una lunga "gestazione" durante la quale sono state, dapprima, poste le basi per l'applicazione nel sistema della giustizia amministrativa della tecnologia digitale e, successivamente, sono stati determinati i tempi per l'avvio del nuovo rito informatizzato e le relative regole tecniche ed operative.

Il primo intervento legislativo rilevante per lo sviluppo normativo innanzi descritto è stato realizzato con il D.P.R. 13 febbraio 2001, n. 123 (Regolamento recante la disciplina dell'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti). In tale decreto sono, innanzitutto, definiti (art. 1) i concetti di «documento informatico» (lett. a), di «duplicato del documento informatico» (lett. b), di «firma digitale» (lett. d) (v. capitolo V, S. D'ANCONA) e di «ricevuta di consegna» (lett. i) (v. capitolo VII, S. D'ANCONA e P. PROVENZANO). Gli artt. 12 e 13 del medesimo decreto prevedono, inoltre, la formazione del fascicolo informatico, in aggiunta al fascicolo cartaceo, e ne disciplinano il contenuto e l'accesso in via telematica (art. 13, comma 6) (v. capitolo V, S. D'ANCONA); gli artt. 9 e 14 attribuiscono poi alle parti la facoltà di redigere e depositare gli atti e i documenti di causa con modalità digitale o attraverso strumenti di supporto elettronici; infine, l'art. 6 consente di eseguire le comunicazioni e le notificazioni con l'ausilio dei mezzi informatici.

Un'ulteriore importante tappa di avvicinamento al processo amministrativo telematico è rappresentata dall'entrata in vigore del Codice dell'amministrazione digitale (CAD), approvato con il D.Lgs. 7 marzo 2005, n. 82, e successivamente modificato dal D.Lgs. 26 agosto 2016, n. 179 (emesso sulla base della legge delega n. 124/2015, c.d. "legge Madia"). Ivi sono stabiliti i principi e gli istituti fondamentali relativi alla dematerializzazione e digitalizzazione dell'attività amministrativa. Detti principi ed istituti trovano attuazione anche nel processo amministrativo telematico: si avrà modo di segnalare nella seguente esposizione che le nozioni e le regole enunciate nel CAD in materia di firma digitale, posta elettronica certificata (PEC), fascicolo informatico, copia informatica di originale analogico, sono esplicitamente richiamate dalla normativa sul PAT. Inoltre, l'art. 2, comma 6, CAD, prescrive, in generale, che i precetti dettati nel D.Lgs. n. 82/2005 si estendono, in quanto compatibili e salvo diversa disposizione espressa, al processo civile, penale, amministrativo, contabile e tributario.

Tuttavia, il testo legislativo essenziale per l'operatività ed il funzionamento del PAT è, senza dubbio, il Codice del processo amministrativo (c.p.a.), emanato con il D.Lgs. 2 luglio 2010, n. 104: come si è già ricordato, le innovazioni ap-

portate dal PAT non hanno inciso (se non per la dematerializzazione degli atti e degli adempimenti processuali) sulla struttura e sulle caratteristiche fondamentali del giudizio amministrativo, né hanno modificato gli istituti e le regole valevoli per tale rito. Rispetto alla disciplina delineata nel D.Lgs. n. 104/2010 il regime del PAT assume, quindi, una funzione meramente attuativa ed integrativa.

Appare utile ricordare che il legislatore aveva già previsto nella delega al Governo per la predisposizione del nuovo codice del processo amministrativo il futuro, progressivo adeguamento del rito in esame alle esigenze di modernizzazione e di informatizzazione della giustizia: infatti, tra i criteri direttivi fissati dalla Legge delega 18 giugno 2009, n. 69, vi era quello di «assicurare la snellezza, concentrazione ed effettività della tutela, anche al fine di garantire la ragionevole durata del processo, anche mediante il ricorso a procedure informatiche e telematiche, nonché la razionalizzazione dei termini processuali, l'estensione delle funzioni istruttorie esercitate in forma monocratica e l'individuazione di misure, anche transitorie, di eliminazione dell'arretrato» (così recita l'art. 44, comma 2, lett. a), della legge innanzi ricordata).

In ossequio ai predetti principi direttivi, l'art. 13 delle norme di attuazione del Codice (contenute nell'allegato 2 del c.p.a.) demandava – già nella sua originaria formulazione – ad un successivo decreto del Presidente del Consiglio dei Ministri il compito di definire «le regole tecnico-operative per la sperimentazione, la graduale applicazione, l'aggiornamento del processo amministrativo telematico, tenendo conto delle esigenze di flessibilità e di continuo adeguamento delle regole informatiche alle peculiarità del processo amministrativo, della sua organizzazione e alla tipologia di provvedimenti giurisdizionali».

La fase di sperimentazione del processo amministrativo telematico, prefigurata dalla disposizione da ultimo menzionata, è stata avviata in virtù del successivo D.L. 30 dicembre 2015, n. 210; questa fase si è svolta nel mese di aprile 2016 ed è stata poi ripresa tra il 10 ottobre ed il 30 novembre dello stesso anno.

Altra significativa norma del Codice in tema di digitalizzazione del processo amministrativo è rinvenibile nell'art. 136 (recante "Disposizioni sulle comunicazioni e sui depositi informatici"): tale norma, al primo comma, stabilisce, innanzitutto, un preciso ordine di prevalenza per le comunicazioni giudiziali a favore della posta elettronica certificata. Il successivo comma 2 (come modificato dal D.L. 27 giugno 2015, n. 83, convertito dalla Legge 6 agosto 2015, n. 132) impone, inoltre, ai difensori, alle parti (nei casi in cui stiano in giudizio personalmente) e agli ausiliari del giudice l'obbligo di depositare tutti gli atti e i documenti con modalità telematiche; il comma 2-*bis* (aggiunto dal D.Lgs. 14 settembre 2012, n. 160, e successivamente modificato più volte) sancisce, poi, che, dall'entrata in vigore del processo amministrativo *paperless*, «tutti gli atti e i provvedimenti del giudice, dei suoi ausiliari, del personale de-

gli uffici giudiziari e delle parti sono sottoscritti con firma digitale». Si osserva, per inciso, che tale obbligo di formazione elettronica di tutti gli atti giudiziali non trova un suo corrispettivo nel processo civile telematico.

2. Il D.P.C.M. 16 febbraio 2016, n. 40, e le modifiche successive

La informatizzazione del processo amministrativo, delineata dal D.P.R. n. 123/2001 e dalle norme codicistiche pocanzi richiamate, è rimasta in una fase di "limbo giuridico" in attesa dell'emanazione delle disposizioni tecnico-operative prescritte dall'art. 13, comma 1, Allegato 2, c.p.a.

Solo nel 2016, le suddette disposizioni attuative sono state varate: con decreto del Presidente del Consiglio dei ministri 16 febbraio 2016, n. 40, è stato adottato, infatti, il regolamento contenente le «regole tecnico-operative per l'attuazione del processo amministrativo telematico». Il predetto regolamento si compone di 21 articoli ed è corredato da un Allegato, in cui sono indicate le "Specifiche tecniche" per l'applicazione concreta delle nuove disposizioni introdotte. Con l'intervento normativo ora ricordato sono state puntualmente determinate le modalità di redazione, sottoscrizione ed (eventuale) asseverazione degli atti digitali; sono stati, altresì, definiti i formati e le dimensioni che devono avere i *files* contenenti detti atti, nonché le regole per la notifica, il deposito e la comunicazione, in via informatica, dei medesimi atti.

L'entrata in vigore di tale provvedimento ha consentito l'avvio della fase operativa: questo avvio, originariamente fissato per il 1º gennaio 2016 (dal già citato D.L. 27 febbraio 2015, n. 83, avente ad oggetto «Misure urgenti in materia fallimentare, civile e processuale civile e di organizzazione e funzionamento dell'amministrazione giudiziaria» convertito, con modificazioni, nella Legge 6 agosto 2015, n. 132), è stato, tuttavia, posticipato al 1º luglio 2016 (per effetto del D.L. 30 dicembre 2015, n. 210, convertito, con modifiche, dalla Legge 25 febbraio 2016, n. 21, proprio in attesa dell'entrata in vigore del D.P.C.M. n. 40/2016), e ulteriormente rimandato alla vigilia della scadenza al 1º gennaio 2017, in forza del D.L. 30 giugno 2016, n. 117, convertito dalla Legge 12 agosto 2016, n. 161.

Con il successivo D.L. 31 agosto 2016, n. 168 (recante, tra l'altro, misure urgenti per l'efficientamento della giustizia amministrativa, convertito con Legge 25 ottobre 2016, n. 197), sono state apportate al c.p.a. le modifiche e le integrazioni funzionali a rendere operativo il nuovo sistema di gestione digitale del processo (art. 7). È stato stabilito, inoltre, il c.d. doppio binario del processo telematico ossia il regime transitorio di convivenza tra il rito informatizzato e quello tradizionale, valevole sino al 1° gennaio 2018. Da tale data, tutti i

giudizi amministrativi si svolgono con modalità esclusivamente telematiche (così statuisce la norma da ultimo menzionata).

Più di recente, sono stati emanati diversi provvedimenti normativi volti a fronteggiare l'emergenza epidemiologica da Covid-19 (coronavirus). Alcuni di essi hanno riguardato anche la giustizia amministrativa: ad esempio, i D.L. nn. 13 e 23/2020 hanno sospeso tutti i termini processuali contemplati dal c.p.a., dall'8 marzo al 3 maggio 2020.

Tra questi ultimi interventi legislativi assume rilievo primario, con specifico riferimento al PAT, il D.L. 30 aprile 2020, n. 28: l'art. 4 di tale decreto-legge, infatti – oltre a configurare un nuovo modello di rito emergenziale «a decorrere dal 30 maggio e fino al 31 luglio 2020» comportante la discussione orale della causa con collegamento delle parti e dei giudici da remoto – ha disposto l'abrogazione (al comma 3) del citato D.P.C.M n. 40/2016. Nello specifico, la norma in questione ha previsto (al comma 2) la sostituzione del suddetto regolamento governativo con un decreto del Presidente del Consiglio di Stato (d.P.C.S.) – emanato su parere del Dipartimento della Presidenza del Consiglio dei ministri competente in materia di trasformazione digitale e degli altri soggetti indicati dalla legge – in cui «sono dettate […] le regole tecnico-operative per la sperimentazione e la graduale applicazione degli aggiornamenti del processo amministrativo telematico, anche relativamente ai procedimenti connessi attualmente non informatizzati, ivi incluso il procedimento per ricorso straordinario». Il medesimo precetto (nell'ultimo periodo) precisa che il nuovo d.P.C.S. entrerà in vigore «a partire dalla data nello stesso indicata, comunque non anteriore al quinto giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana».

Il Presidente del Consiglio di Stato ha adottato il 22 maggio 2020 il decreto richiesto dall'art. 4, D.L. n. 28/2020; quest'ultimo provvedimento (d.P.C.S. n. 134/2020) – pubblicato sulla Gazzetta Ufficiale il 27 maggio 2020 – si compone di tre allegati: i primi due riportano le «Regole tecnico-operative per l'attuazione del processo amministrativo telematico, nonché per la sperimentazione e la graduale applicazione dei relativi aggiornamenti»; tali regole tecniche sono meramente riproduttive di quelle precedentemente fissate dal D.P.C.M n. 40/2016; l'allegato n. 3 definisce, inoltre, «le specifiche tecniche per le udienze da remoto». Non si rinvengono, invece, prescrizioni che estendono il sistema informatizzato, introdotto dal PAT, al ricorso straordinario al Presidente della Repubblica.

Il 26 maggio 2020 il Presidente del Consiglio di Stato ha, altresì, emanato le «linee guida sull'applicazione dell'art. 4 del d.l. n. 28/2020 e sulla discussione da remoto». Lo stesso giorno è stato sottoscritto un protocollo d'intesa tra la Giustizia amministrativa, rappresentata dal Presidente del Consiglio di Stato, l'Avvocatura dello Stato, il Consiglio Nazionale Forense, il Consiglio dell'Ordine degli Avvocati di Roma e le Associazioni specialistiche degli avvocati amministrativisti.

L'emergenza sanitaria ha insomma avuto, come effetto collaterale, un'ulteriore stratificazione (con provvedimenti di rango differente) della normativa applicabile al PAT, che poteva essere evitata, in quanto non utile o necessaria (eccezion fatta per l'adozione delle specifiche tecniche riguardanti le nuove udienze da remoto).

Anche il successivo D.L. n. 76/2020 (D.L. 16 luglio 2020, n. 76, avente ad oggetto Misure urgenti per la semplificazione e l'innovazione, convertito dalla Legge 11 settembre 2020, n. 120) include disposizioni che hanno una immediata incidenza sul PAT: in particolare hanno sicura rilevanza le disposizioni, ivi ricomprese, che disciplinano la notificazione telematica degli atti giudiziari alle pubbliche amministrazioni; le novità introdotte in materia dal decreto-legge ora richiamato saranno, peraltro, illustrate puntualmente nel paragrafo dedicato al tema relativo al domicilio digitale delle P.A. (par. 8): a questo pertanto si rinvia per approfondimenti.

Alla fine della rassegna più sopra compiuta delle norme che attualmente regolano il processo amministrativo telematico non si può fare a meno di sottolineare che dette norme divergono, sotto molti profili (su cui ci si soffermerà nella seguente trattazione), da quelle dettate per il processo civile telematico.

Tale differenza di regime appare irragionevole ed in contrasto con gli obiettivi – perseguiti con la informatizzazione dei processi e comuni a tutti gli ordinamenti giurisdizionali interessati dall'innovazione tecnologica – di semplificazione degli adempimenti formali, di standardizzazione delle procedure, di accelerazione dei tempi della giustizia e di risparmio delle risorse economiche, pubbliche e private.

Risulta, invero, difficilmente armonizzabile con i suindicati obiettivi fondamentali la scelta del legislatore di "costruire", dal punto di vista tecnico-operativo, ogni processo digitale (civile, amministrativo, tributario e contabile), con proprie regole peculiari; altrettanto discutibile appare la previsione dell'uso di piattaforme informatiche distinte (con modalità di funzionamento non coincidenti) per ogni rito telematico attivato. Queste diversità procedurali ed organizzative impongono all'utente di acquisire dimestichezza con una pluralità di disposizioni e specifiche tecniche, esponendolo inevitabilmente al rischio di commettere errori, talora esiziali (con conseguente danno per la parte che agisce in giudizio a tutela dei propri diritti ed interessi legittimi e, più in generale, per il corretto funzionamento della giustizia).

La disomogeneità delle regole tecniche stabilite dal legislatore – come si è detto – vanifica ogni tentativo di semplificare il sistema giudiziario e anche il sistema socio-economico, condizionato dal primo. È invero impellente la necessità di definire principi e criteri operativi uniformi, valevoli per tutte le procedure giudiziali informatizzate.

Giova sottolineare che le difformità esistenti tra i singoli processi telematici attualmente in vigore (relativi al processo amministrativo, civile, tributario e contabile) riguardano aspetti applicativi tutt'altro che marginali, quali, ad esempio, la formazione e il deposito dei documenti informatici; la sottoscrizione digitale degli atti del processo; l'attestazione della conformità dei medesimi atti; la prova della notificazione e le modalità per il pagamento del contributo unificato, ai fini dell'iscrizione a ruolo della causa.

Si tratta all'evidenza di profili applicativi importanti, ma non certo inconciliabili, dato che essi, in epoca antecedente alla digitalizzazione dei processi, erano disciplinati in egual modo per tutti i riti.

3. Il Sistema Informativo della Giustizia Amministrativa

Il Sistema Informativo della Giustizia Amministrativa (S.I.G.A.) è l'insieme delle risorse *hardware* e *software*, mediante le quali la giustizia amministrativa tratta, in via automatizzata, attività, dati, servizi, comunicazioni e procedure relative allo svolgimento dell'attività processuale (così è definito il S.I.G.A. dall'art. 1, comma 1, lett. d), d.P.C.S. n. 134/2020).

Il predetto sistema gestisce con modalità informatiche, in ogni stato del giudizio, la formazione del fascicolo, le operazioni di individuazione del procedimento, la tenuta dei registri, il deposito, la conservazione, la visualizzazione e l'estrazione di copie degli atti inseriti nel fascicolo, la pubblicazione dei provvedimenti giurisdizionali, le comunicazioni di segreteria, la trasmissione dei fascicoli ed ogni altra attività inerente al processo amministrativo telematico (art. 4, d.P.C.S. n. 134/2020).

Il S.I.G.A., di cui è responsabile il Segretario generale della Giustizia amministrativa, assicura, inoltre, la conservazione dei dati e dei documenti, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, in applicazione di quanto previsto dal CAD e nel rispetto delle misure di sicurezza dettate dal Codice dei dati personali e dalla normativa speciale in materia (art. 2 delle specifiche tecniche riportate nell'Allegato 2 del d.P.C.S. n. 134/2020) (v. capitolo V, S. D'ANCONA e capitolo VI, G. CARULLO).

Il sistema informativo, di cui si discute, non deve essere confuso con il «portale dei servizi telematici della giustizia amministrativa», struttura tecnologia-organizzativa autonoma e distinta – accessibile dal sito internet www.giustizia-amministrativa.it – che consente agli utenti di fruire dei servizi informatici resi disponibili dal S.I.G.A.

Detto portale è suddiviso fondamentalmente in tre sezioni. La prima è consultabile da tutti gli utenti senza necessità di alcuna preventiva abilitazione ed

autenticazione. Le altre due (il c.d. «Portale dell'Avvocato» e il c.d. «Portale del Magistrato») sono invece riservate, rispettivamente, agli avvocati e ai magistrati e permettono a questi ultimi di accedere ad atti, documenti, servizi e informazioni ad essi specificatamente dedicati (vi sono anche altre sezioni rivolte agli uffici amministrativi e agli altri soggetti autorizzati; tali ultime sezioni assumono, tuttavia, una rilevanza residuale nella presente trattazione).

Tramite il Portale degli avvocati, il patrocinatore potrà, tra l'altro, visionare il fascicolo del processo e scaricare, altresì, i moduli in formato pdf, che occorre compilare – inserendo le informazioni richieste e allegando gli atti e i documenti – ed inviare telematicamente, ai fini del deposito in giudizio dei medesimi atti e documenti.

Preliminarmente, l'avvocato dovrà richiedere le credenziali di accesso al portale e procedere all'autenticazione (attraverso l'inserimento di una *userid* e una *password*), ogniqualvolta intenda collegarsi al predetto portale ed utilizzare i servizi ivi contenuti.

4. Il fascicolo informatico e il registro generale dei ricorsi

Come prevede il CAD per il procedimento amministrativo (art. 41), anche il d.P.C.S. n. 134/2020 prescrive per il processo amministrativo che il fascicolo cartaceo è sostituito dal fascicolo informatico.

L'art. 5, comma 1, del d.P.C.S. n. 134/2020, dispone, infatti, che «il fascicolo processuale è tenuto sotto forma di fascicolo informatico». Quest'ultimo "contenitore" tecnologico costituisce il fascicolo d'ufficio ed è organizzato e gestito in modo da «garantire la facile reperibilità ed il collegamento degli atti ivi raccolti in relazione alla data di deposito, al contenuto ed alle finalità dei singoli documenti» (art. 5, comma 5, del decreto succitato).

In esso sono inseriti tutti gli atti, gli allegati, i documenti e i provvedimenti del processo redatti come documenti elettronici, ovvero le copie per immagine su supporto digitale dei medesimi atti (art. 5, comma 2, d.P.C.S. n. 134/2020). In particolare, il fascicolo informatico, al pari del tradizionale fascicolo cartaceo, deve contenere l'indicazione (art. 5, comma 3, del predetto decreto):

a) dell'ufficio titolare del ricorso, che sovrintende alla gestione del fascicolo medesimo e cura la correttezza e l'aggiornamento dei dati ivi inseriti;
b) del numero del ricorso;
c) dell'oggetto sintetico del ricorso;
d) dei dati identificativi delle parti e dei difensori;
e) dell'elenco dei documenti contenuti, anche depositati in forma cartacea.

Nel medesimo fascicolo sono riportate, altresì, informazioni riguardanti (art. 5, comma 4, d.P.C.S. n. 134/2020):

a) i componenti del Collegio e i suoi ausiliari, le parti e i difensori (tipologia di parte; data di costituzione, data di rinuncia, partita IVA/codice fiscale);
b) l'oggetto del ricorso per esteso, consistente nella precisa indicazione dei provvedimenti impugnati e/o dell'oggetto della domanda proposta, nonché l'indicazione della materia del ricorso;
c) le comunicazioni di Segreteria e le relative ricevute di PEC;
d) le camere di consiglio e le udienze;
e) i ricorsi collegati;
f) il link al contenuto integrale del fascicolo informatico di provenienza, in caso di appello, regolamento di competenza, revocazione e negli altri casi previsti;
g) i provvedimenti impugnati;
h) le spese di giustizia;
i) il patrocinio a spese dello Stato.

Il fascicolo informatico non è liberamente consultabile: sono, infatti, legittimati ad accedervi i membri del collegio, gli ausiliari del giudice (nei limiti dell'incarico ricevuto e dell'autorizzazione rilasciata dal giudice), i difensori muniti di procura, gli avvocati domiciliatari, le parti personalmente e, previa autorizzazione del giudice, coloro che intendono intervenire volontariamente nel processo (art. 17, d.P.C.S. n. 134/2020).

Per quanto riguarda le modalità di consultazione, i magistrati e gli ausiliari autorizzati utilizzano la sezione loro riservata contenuta nel sito istituzionale della giustizia amministrativa (www.giustizia-amministrativa.it).

Gli avvocati accedono al fascicolo tramite il già menzionato «Portale dell'avvocato». Non solo i difensori delle parti costituite, ma anche i difensori, muniti di procura, di parti non costituite in giudizio possono essere abilitati alla consultazione (questi ultimi dovranno presentare una apposita istanza, la c.d. istanza di "visibilità", secondo le modalità stabilite nel predetto portale).

Per visionare il fascicolo informatico, i patrocinatori devono richiedere preventivamente il rilascio delle credenziali di accesso al fascicolo, avvalendosi dell'apposita sezione presente nel portale dedicato agli avvocati. Le credenziali sono inviate all'indirizzo PEC del difensore richiedente, previa verifica della correttezza dei dati identificativi comunicati dallo stesso difensore istante, e sono disattivate decorsi 60 giorni dalla data del rilascio (art. 18 delle specifiche tecniche allegate al d.P.C.S. n. 134/2020). Nel caso in cui la richiesta sia fatta da un avvocato di una parte non costituita l'autorizzazione all'accesso avrà una durata di 30 giorni dalla data del rilascio (così si prevede nelle FAQ pubblicate sul sito istituzionale della Giustizia amministrativa).

Nel regime del PAT, anche i registri di presentazione dei ricorsi e i registri particolari contemplati dagli artt. 1 e 2 delle disposizioni di attuazione del c.p.a. sono gestiti con modalità informatiche. Tale nuova modalità di tenuta dei registri deve comunque assicurare la numerazione progressiva dei ricorsi, la certezza della data e dell'oggetto delle registrazioni e l'identificazione del soggetto che procede alle registrazioni informatiche (art. 6, comma 1, d.P.C.S. n. 134/2020).

In particolare sono gestiti con sistema automatizzato i seguenti registri ed atti (art. 6, comma 2, del decreto da ultimo menzionato):

– il registro generale dei ricorsi;
– i ricorsi con patrocinio a spese dello Stato;
– i processi verbali;
– i provvedimenti dell'Adunanza plenaria;
– i provvedimenti collegiali (escluse le ordinanze cautelari);
– i provvedimenti monocratici (esclusi i decreti cautelari e cautelari *ante causam*);
– i provvedimenti cautelari (decreti cautelari, decreti cautelari *ante causam*, ordinanze cautelari);
– le istanze di fissazione di udienza;
– le istanze di prelievo.

4. L'atto processuale informatico

L'art. 9, comma 1, del d.P.C.S. n. 134/2020, statuisce che «salva diversa espressa previsione, il ricorso introduttivo, le memorie, il ricorso incidentale, i motivi aggiunti e qualsiasi altro atto del processo, anche proveniente dagli ausiliari del giudice, sono redatti in formato di documento informatico, sottoscritto con firma digitale conforme ai requisiti di cui all'art. 24 del CAD» (in senso sostanzialmente conforme è anche l'art. 136, comma 2-*bis*, c.p.a).

Si ricorda che, secondo l'art. 1, comma 1, lett. p), CAD, il documento informatico è un «documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».

L'art. 20, comma 1-*bis*, CAD, stabilisce, inoltre, che il predetto documento, quando è sottoscritto con firma digitale, soddisfa il requisito della forma scritta ed ha l'efficacia probatoria della scrittura privata, ai sensi dell'art. 2702 c.c. Il medesimo art. 20, comma 1-*bis*, CAD, prescrive, altresì, che il valore probatorio del documento informatico è liberamente valutabile in giudizio «in relazione alle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità».

In base alle specifiche tecniche allegate al d.P.C.S. n. 134/2020 (art. 6), tutti gli atti di parte devono essere sottoscritti digitalmente utilizzando la modalità PAdES (ovvero l'estensione del file .pdf). Sotto questo profilo il processo am-

ministrativo telematico si distingue dal processo civile telematico, nel quale può essere adoperata per la firma digitale, indifferentemente, sia la modalità CAdES (ovvero l'estensione.p7m) sia la modalità PAdES (Cass. civ., sez. un., sentenza 27 aprile 2018, n 10266; giova peraltro segnalare che, secondo la giurisprudenza, la sottoscrizione del ricorso giurisdizionale amministrativo in formato CAdES, anziché PAdES, non rende inammissibile l'atto introduttivo del giudizio, in quanto anch'essa è "pienamente idonea ad assolvere alla funzione di attestare la provenienza dell'atto…. Dunque la mancata conformità alle norme tecniche del PAT, che prevedono l'utilizzo del formato PAdES per la firma digitale, non impedisce la validità della sottoscrizione": così T.a.r. Lazio, Roma, sez. I *bis*, sentenza 25 maggio 2018, n. 5912).

Gli atti processuali di parte (non, quindi, i documenti allegati) possono essere depositati, in via telematica, esclusivamente nel c.d. formato "nativo digitale": gli scritti difensivi devono, quindi, essere generati da un programma di videoscrittura (Open word, Open office, ecc.) e trasformati direttamente in file PDF, senza scansioni (art. 12 delle specifiche tecniche contenute nell'Allegato 2 del d.P.C.S. n. 134/2020).

Si è posto il problema di determinare quali siano le conseguenze derivanti dal mancato rispetto delle norme del PAT che disciplinano la redazione degli atti in formato elettronico ed il deposito di tali atti con modalità telematica, giacché il regime processuale in esame non detta al riguardo alcuna specifica disposizione (si pensi, ad esempio, al caso in cui il ricorrente abbia provveduto a depositare il ricorso solo in formato cartaceo, sottoscrivendolo esclusivamente con firma autografa e senza alcuna attestazione di conformità ad un eventuale originale digitale). Sul punto la giurisprudenza ha avuto modo di chiarire che l'inosservanza di tali norme non comporta la nullità dell'atto non corrispondente alle prescrizioni tecniche stabilite nel PAT – posto che la legge non prevede espressamente simili effetti invalidanti per le violazioni formali, di cui si discute (come richiede, invece, l'art. 156, comma 1, c.p.c.) – ma solo «la sua irregolarità, sanabile, su ordine del Collegio, nel termine perentorio da questo fissato» (Cons. Stato, sez. IV, sentenza 4 aprile 2017, n 1541). A sostegno di tale orientamento sono stati, altresì, richiamati i principi di riserva di legge, che vige in campo processuale *ex* art. 111. Cost., e di gerarchia delle fonti: in virtù di tali principi si è argomentato, infatti, che la violazione di regole tecniche dettate da provvedimenti normativi di secondo grado può provocare la nullità dell'atto o dell'adempimento viziato solo se si traduce anche in violazione di norme di rango legislativo (sul punto si rinvia alla sentenza da ultimo riportata). Si è, inoltre, sottolineato che, se il giudice non rileva l'irregolarità e non ne dispone la regolarizzazione, l'atto compiuto, ancorché imperfetto, deve essere considerato valido e, quindi, inidoneo a produrre alcun effetto negativo o preclusivo in termini processuali (Cons. Stato, sez. V, 28 marzo 2018, n. 1936; Id., 27 giugno 2018, n. 3953).

La medesima giurisprudenza ha, altresì, affermato che «il ricorso e il deposito, non costituiti come documenti informatici sottoscritti con firma digitale […], non determinano neppure l'inesistenza o l'abnormità degli stessi atti», giacché questi hanno comunque raggiunto il loro scopo tipico, «essendone certa la paternità e piana l'intelligibilità» quali strumenti finalizzati «alla chiamata in giustizia e all'articolazione delle altrui relative difese» (Cons. Stato, sez. IV, sentenza 4 aprile 2017, n. 1541, cit.; Id., Sez. V, ordinanza 4 gennaio 2018, n. 56).

5. La procura alle liti

L'art 8 del d.P.C.S. n. 134/2020 contiene la disciplina relativa alla procura alle liti e al conferimento dell'incarico di assistenza e difesa nel PAT.

La norma dispone, innanzitutto, che la procura alle liti è autenticata dal difensore, qualora sia il medesimo a provvedervi, «mediante apposizione della firma digitale» (comma 1).

La procura può essere conferita su documento analogico (art. 8, comma 2, del summenzionato decreto) oppure su documento informatico nativo digitale (comma 1, del precetto testé ricordato).

Nel primo caso, il difensore procede al deposito telematico della copia per immagine su supporto informatico (ottenuta dalla scansione della procura cartacea sottoscritta dal cliente e, per autentica, dal patrocinatore). Tale duplicato è firmato digitalmente dall'avvocato; con quest'ultimo adempimento, esso acquisisce la stessa efficacia probatoria dell'originale (art. 20, comma 1-*bis*, CAD). La copia informatica deve essere, altresì, accompagnata dall'attestazione di conformità prevista dall'art. 22, comma 2, CAD, la quale può essere inserita nel medesimo documento contenente la procura o resa su distinto documento, sempre sottoscritto con firma digitale dall'avvocato (art. 8, comma 2, d.P.C.S. n. 134/2020).

Il richiamato art. 22, comma 2, CAD, statuiva che «Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'art. 71» CAD. La norma sopra citata è stata modificata dal D.Lgs. 13 dicembre 2017, n. 217: con tale novella è stato eliminato il riferimento, contenuto nel precetto in esame, alla «dichiarazione […] asseverata secondo le regole tecniche stabilite ai sensi dell'art. 71» CAD ed è stato disposto, in sostituzione dell'enunciato ora indicato, che la conformità degli atti analogici sia attestata «secondo le linee guida».

Fino all'emanazione delle predette linee guida da parte dell'AgID (Agenzia per l'Italia digitale), rimangono in vigore le regole tecniche dettate in attuazione dell'art. 71 CAD (in tal senso si è espresso il Segretario Generale della Giustizia amministrativa nel parere reso il 10 aprile 2018). Queste ultime regole tecniche (definite dall'art. 4, comma 3, D.P.C.M. 13 novembre 2014), prescrivono, in particolare, che, qualora la conformità della copia all'originale sia certificata dall'avvocato in un documento separato rispetto al documento recante la procura (come avviene, ad esempio, nel caso in cui la notifica del ricorso sia eseguita tramite PEC, essendo, in questo caso, necessario inserire la dichiarazione, di cui si discute, nella relata di notifica, in ottemperanza all'art. 3-*bis*, comma 5, lett. g), Legge n. 53/1994), l'attestazione dovrà riportare, oltre alla firma digitale, anche un riferimento temporale e l'impronta della copia informatica della procura (c.d. *hash*). Tale impronta è una funzione crittografica che assegna alla copia informatica un codice ricavato dall'elaborazione del suo contenuto, la cui menzione nella dichiarazione di conformità serve a collegare inequivocabilmente l'anzidetta dichiarazione alla procura, cui essa si correla.

Di recente (esattamente il 9 settembre 2020) l'AgID ha adottato e pubblicato le linee guida "sulla formazione, gestione e conservazioni dei documenti informatici": ivi si conferma (al punto 2.2, capoverso 4) che l'attestazione di conformità della copia per immagine di un documento analogico, prodotta come atto informatico autonomo e separato, deve necessariamente contenere, oltre alla firma digitale del dichiarante, anche un riferimento temporale e l'impronta *hash* della copia per immagine, oggetto dell'attestazione.

Secondo la giurisprudenza, il deposito in giudizio della copia informatica della procura alle liti in origine cartolare, priva della asseverazione di conformità, non comporta l'inammissibilità del ricorso per inesistenza e/o nullità della procura prodotta, ma semplicemente una irregolarità sanabile mediante l'assegnazione di un termine perentorio per la regolarizzazione, a pena di irricevibilità del ricorso, in forza dell'art. 44, comma 2, c.p.a. (T.A.R. Lazio, Roma, sez. I-*bis*, ordinanza 17 settembre 2018, n. 9411).

Giova sottolineare che la disciplina del PAT innanzi descritta differisce (irragionevolmente) dalla analoga disciplina contemplata dal processo civile: l'art. 83 c.p.c. dispone, infatti, che la conformità della copia informatica della procura alle liti al suo originale è certificata mediante la semplice sottoscrizione digitale della medesima copia informatica della procura, da parte dell'avvocato. Sarebbe stato certamente più logico (e semplice) applicare al PAT quest'ultima regola processuale, consentendo così ai difensori, anche nei giudizi amministrativi, di autenticare la procura alle liti riprodotta su supporto informatico mediante la sola apposizione della firma digitale.

Qualora, invece, la procura alle liti sia stata conferita su documento nativo

elettronico, sia l'avvocato sia la parte rappresentata sono tenuti a sottoscrivere digitalmente il documento, in formato PDF. La procura così redatta e firmata dovrà essere poi depositata in via telematica.

L'art. 8, comma 4, del d.P.C.S. n. 134/2020, stabilisce, inoltre, che, nell'ipotesi di ricorsi collettivi, ove le procure siano state rilasciate su supporti cartacei distinti, il difensore potrà includere in un unico file copia per immagine di tutte le procure conferite.

Si ricorda, infine, che, in ossequio alla norma da ultimo menzionata (comma 3), la procura si considera apposta in calce all'atto cui si riferisce sia quando è rilasciata su documento informatico separato, depositato con modalità telematiche, sia quando è conferita su foglio separato, del quale è estratta copia informatica, anche per immagine. La giurisprudenza ha, tuttavia, chiarito che, anche dopo l'entrata in vigore del PAT, non può essere ritenuto inammissibile un ricorso giurisdizionale, nel quale la procura alle liti sia riportata a margine dell'atto, piuttosto che in calce, come richiesto dal suindicato art. 8, comma 3, d.P.C.S. n. 134/2020 (T.A.R. Campania, Napoli, sez. VIII, sentenza 5 maggio 2017, n. 2420).

6. Le notificazioni telematiche

Con l'art. 25, comma 3, lett. a), della Legge 12 novembre 2011, n. 183, è stata introdotta la facoltà per gli avvocati di notificare gli atti giudiziari per mezzo della posta elettronica certificata. Tale norma ha, infatti, modificato l'art. 1 della Legge 21 gennaio 1994, n. 53, il quale attribuiva agli avvocati la facoltà di «eseguire notificazioni di atti in materia civile, amministrativa e stragiudiziale, a mezzo del servizio postale», concedendo agli stessi la possibilità di avvalersi, per lo stesso adempimento processuale, anche della posta elettronica certificata.

Riguardo alla notificazione con modalità telematica, l'art. 3-*bis* della Legge n. 53/1994 – aggiunto dall'art. 16-*quater*, comma 1, lett. d), del D.L. 18 ottobre 2012, n. 179 – prescrive che essa «si esegue a mezzo di posta elettronica certificata all'indirizzo risultante da pubblici elenchi, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. La notificazione può essere eseguita esclusivamente utilizzando un indirizzo di posta elettronica certificata del notificante risultante da pubblici elenchi».

Il Ministero della Giustizia – con il decreto 3 aprile 2014, n. 48, modificativo del precedente D.M. n. 44/2011 – ha poi stabilito le regole tecniche ed operative per l'esercizio della facoltà di notificazione in via telematica, da parte degli avvocati. Tale regolamento ministeriale, tuttavia – per espressa previsione ivi contenuta – è finalizzato a garantire «l'adozione nel processo civile e

nel processo penale delle tecnologie dell'informazione e della comunicazione»; stando, quindi, al dato testuale, è escluso dall'ambito di operatività del regolamento in questione il processo amministrativo.

Il tenore letterale del succitato decreto ministeriale e del già evocato art. 16-*quater*, comma 3-*bis*, del D.L. n. 179/2012 – il quale sembra subordinare la validità e l'efficacia del meccanismo di notificazione in esame alla preventiva emanazione di un apposito regolamento – ha suscitato in giurisprudenza dubbi ed incertezze in ordine all'applicabilità della nuova disciplina introdotta dall'art. 25, comma 3, lett. a), della Legge n. 183/2011, al processo amministrativo.

Sul punto si sono formati (almeno sino all'adozione del D.P.C.M. 16 febbraio 2016, n. 40, contenente, per l'appunto, il regolamento per l'attuazione del processo amministrativo telematico) due opposti indirizzi interpretativi: secondo un indirizzo minoritario (Cons. Stato, sez. IV, sentenza 17 gennaio 2017, n. 130; Id., sentenza 13 dicembre 2016, n. 5226) la notifica del ricorso giurisdizionale amministrativo mediante posta elettronica certificata, ai sensi della Legge n. 53/1994, doveva essere considerata inammissibile, in assenza di una espressa autorizzazione del Presidente del T.A.R. o del Consiglio di Stato rilasciata in forza dell'art. 52, comma 2, c.p.a.; l'indirizzo prevalente (Cons. Stato, sez. IV, sentenza 22 novembre 2016, n. 4895; Id., sez. V, sentenza 4 novembre 2016, n. 4631) era, invece, orientato a riconoscere la piena ed immediata applicabilità nel processo amministrativo della facoltà concessa dai menzionati artt. 1 e 3-*bis* della Legge n. 53/1994, anche in mancanza della suindicata autorizzazione presidenziale e di una specifica disciplina regolamentare destinata a dare esecuzione nel processo amministrativo alle norme sulle notifiche via PEC.

Il contrasto giurisprudenziale sopra descritto è stato composto dall'Adunanza plenaria del Consiglio di Stato con la sentenza 19 settembre 2017, n. 6: in tale pronuncia l'Organo della giustizia amministrativa con funzioni nomofilattiche ha stabilito che la notificazione del ricorso introduttivo del giudizio amministrativo poteva essere effettuata per posta elettronica certificata, nel rispetto delle disposizioni generali che la regolano, anche prima dell'emanazione del D.P.C.M. n. 40/2016 e indipendentemente dall'autorizzazione presidenziale contemplata dall'art. 52, comma 2, c.p.a.

Come si è già accennato, la questione interpretativa innanzi segnalata non si pone più per i ricorsi proposti dopo l'entrata in vigore del D.P.C.M. n. 40/2016 e l'avvio (fissato per il 1° gennaio 2017) del processo amministrativo telematico: l'art. 14, comma 1, del predetto decreto ministeriale (oggi sostituito dal d.P.C.S. n. 134/2020, avente, però, il medesimo contenuto del D.P.C.M. n. 40/2016, abrogato dall'art. 4, del D.L. n. 28/2020), prescrive, infatti, che «i difensori possono eseguire la notificazione a mezzo PEC a norma dell'art. 3-*bis* della legge 21 gennaio 1994, n. 53».

L'avvocato, che intende avvalersi dello strumento telematico, ai sensi e per gli effetti determinati dall'art. 1 della Legge n. 53/1994, deve essere munito della procura alle liti ed essere in possesso di un indirizzo di posta elettronica certificata risultante da pubblici elenchi (art. 3-*bis*, Legge n. 53/1994). Per la notifica via PEC non è più necessaria l'autorizzazione del Consiglio dell'ordine, che continua ad essere obbligatoria solo per le notifiche in proprio a mezzo posta.

Al messaggio, inviato telematicamente, deve essere allegato:

– l'atto processuale da notificare, predisposto nel formato nativo digitale e sottoscritto con firma elettronica;

– la procura alle liti, sempre sottoscritta con firma digitale (come sì è già segnalato, la relativa attestazione di conformità, ove necessaria, deve, invece, essere inserita nella relata di notifica, come pure l'impronta *hash*, qualora richiesta);

– la relazione di notifica: quest'ultima è redatta dall'avvocato su foglio separato, sottoscritto con firma digitale. In particolare, nella relazione devono essere indicati (art. 3-*bis*, comma 5, Legge n. 53/1994):

a) il nome, il cognome ed il codice fiscale dell'avvocato notificante;

b) il nome e il cognome o la denominazione e ragione sociale ed il codice fiscale della parte che ha conferito la procura alle liti;

c) il nome e il cognome o la denominazione e ragione sociale del destinatario;

d) l'indirizzo di posta elettronica certificata a cui l'atto è notificato;

e) l'attestazione di conformità richiesta dall'art. 3-*bis*, comma 2, Legge n. 53/1994.

Per le notificazioni effettuate in corso di procedimento occorre, inoltre, specificare nel messaggio inviato l'ufficio giudiziario, la sezione, il numero e l'anno di ruolo della causa (art. 3-*bis*, comma 6, Legge n. 53/1994).

In ogni caso è necessario che la *mail* certificata contenga nell'oggetto la dicitura «notificazione ai sensi della legge n. 53 del 1994» (art. 3-*bis*, comma 4, Legge n. 53/1994).

La notifica si perfeziona, per il soggetto notificante, nel momento in cui viene generata dal sistema informatico la ricevuta di accettazione regolata dall'art. 6, comma 1, del D.P.R. n. 68/2011, e, per il destinatario, nel momento in cui viene generata la ricevuta di avvenuta consegna contemplata dall'art. 6, comma 2, del decreto presidenziale da ultimo citato (art. 3-*bis*, comma 3, Legge n. 53/1994).

L'art. 14, comma 3, d.P.C.S. n. 134/2020, stabilisce che «ai fini della prova in giudizio della notificazione a mezzo PEC, le ricevute di avvenuta consegna contengono anche la copia completa del messaggio di posta elettronica certificata consegnato, secondo quanto previsto nell'articolo 6, comma 4, del decre-

to del Presidente della Repubblica 11 febbraio 2005, n. 68».

La medesima norma, al comma 4, prescrive poi che le ricevute di accettazione e di avvenuta consegna, in formato .eml. e .msg., devono essere depositate, in via telematica, unitamente al ricorso, alla relazione di notifica, alla procura alle liti e agli altri atti e documenti processuali.

La notifica via PEC è effettuabile dal mittente sino alle ore 24.00 dell'ultimo giorno utile (senza che il sistema telematico possa rifiutare l'accettazione e la consegna). L'originario testo dell'art. 16-*septies* del D.L. n. 179/2012 disponeva, invero, che la notifica in via telematica, eseguita dopo le ore 21.00, si perfezionava alle ore 7.00 del giorno successivo (la *ratio* del precetto era quella di tutelare il destinatario e il suo diritto al riposo nella fascia oraria ricompresa tra le ore 21.00 e le ore 7.00 del giorno seguente). È, tuttavia, intervenuta la Corte Costituzionale, la quale ha dichiarato l'illegittimità costituzionale delle norma sopra richiamata, nella parte in cui prevedeva il differimento al giorno successivo dell'efficacia della notifica, via PEC, compiuta dopo le ore 21.00 (Corte Costituzionale, sentenza 9 aprile 2019, n. 75): in particolare la Consulta ha osservato che tale differimento appare ingiustificato nei riguardi del mittente «al quale – senza che ciò sia funzionale alla tutela del diritto al riposo del destinatario e nonostante che il mezzo tecnologico lo consenta – viene invece impedito di utilizzare appieno il termine utile per approntare la propria difesa: termine che l'art. 155 c.p.c. computa "a giorni" e che, nel caso di impugnazione, scade allo spirare della mezzanotte dell'ultimo giorno».

Indubbiamente l'innovativo mezzo di notificazione introdotto dalla Legge n. 53/1994 offre all'avvocato e al proponente il ricorso significativi vantaggi, sotto il profilo pratico: innanzitutto la notifica via PEC è sostanzialmente gratuita; inoltre – come si è rilevato – la scelta della modalità digitale non richiede la preventiva autorizzazione da parte del Consiglio dell'Ordine degli avvocati di appartenenza, ai sensi della Legge n. 53/1994; l'uso della posta elettronica, ai fini qui considerati, non impone neppure l'annotazione delle notifiche effettuate sull'apposito registro cronologico (che rimane obbligatoria, per gli avvocati, solo per le notifiche in proprio eseguite a mezzo posta); non vi è poi la necessità di apporre alcuna marca da bollo al momento dell'esibizione o del deposito dell'atto notificato; la notifica, in via telematica, è consentita sino alle ore 24.00 del giorno di scadenza; infine, vi è la sostanziale coincidenza tra il momento dell'invio dell'atto da notificare e quello della sua consegna al destinatario e, quindi, l'immediata contezza, per il mittente, del buon fine e della tempestività della comunicazione eseguita.

Giova in ultimo ricordare che la tradizionale notificazione cartacea rimane comunque consentita anche nel vigore del processo amministrativo telematico, per espresso disposto dell'art. 14, d.P.C.S. n. 134/2020.

7. Il domicilio digitale

Si è già avuto modo di segnalare che la notifica telematica può essere effettuata solo da e verso indirizzi PEC risultanti da pubblici registri (art. 3-*bis*, Legge n. 53/1994). Ciò significa che spetta ai difensori individuare l'indirizzo di posta elettronica certificata cui inviare il ricorso, estraendolo dai pubblici elenchi contenenti i domicili digitali per la ricezione delle notifiche, in via informatica, degli atti giudiziari.

Tale compito risulta tutt'altro che agevole per l'avvocato, in quanto la disciplina del processo *paperless* è definita da una moltitudine di provvedimenti normativi, spesso non coordinati tra loro e caratterizzati da carenze ed incongruenze, che determinano sovente incertezze e difficoltà applicative non facilmente risolvibili in via interpretativa.

In materia la norma fondamentale è costituita dall'art. 16-*ter* del D.L. n. 179/2012 (convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221). La disposizione statuisce che «ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale si intendono per pubblici elenchi quelli previsti dagli articoli 6-*bis, 6-quater*, e 62 del decreto legislativo 7 marzo 2005, n. 82, dall'art. 16, comma 12, del presente decreto, dall'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185 […], nonché il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia».

Dal precetto sopra riferito si evince che sono molteplici i pubblici registri da cui è possibile trarre i recapiti di posta elettronica certificata validi per la notificazione degli atti giudiziari.

In particolare, l'elenco indicato dall'art. 6-*bis* del D.Lgs. n. 82/2005 (contenente il Codice dell'amministrazione digitale, CAD) è l'«Indice nazionale dei domicili digitali delle imprese e dei professionisti», meglio noto come INI-PEC: quest'ultimo elenco «è realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e degli ordini professionali» (art. 6-*bis*, comma 2, primo periodo, CAD). I domicili digitali inseriti in tale Indice rappresentano, inoltre, il «mezzo esclusivo di comunicazione e notifica con i soggetti di cui all'articolo 2, comma 2, CAD [*id est*, con le pubbliche amministrazioni]» (così prescrive la norma da ultimo richiamata).

Per quanto riguarda le imprese, l'art. 16-*ter* del D.L. n. 179/2012 menziona pure il Registro delle imprese – istituito con D.L. n. 185/2008 – al quale le medesime imprese sono tenute a comunicare il proprio indirizzo di posta elettronica certificata.

L'art. 16-*ter* del D.L. n. 179/2012 fa, altresì, riferimento all'elenco contemplato dall'art. 6-*quater*, CAD, ovvero all'«Indice nazionale dei domicili digitali

delle persone fisiche e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro delle imprese»: detto elenco non risulta, tuttavia, ancora operativo.

Occorre aggiungere che l'art. 6-*ter*, CAD, fa riferimento ad un ulteriore pubblico elenco non espressamente richiamato dall'art. 16-*ter* del D.L. n. 179/2012, ossia l'«Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori dei pubblici servizi», comunemente definito anche come IndicePa o solo IPA. Quest'ultimo Indice è stato istituito con l'obiettivo di «assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi» ed è alimentato dai dati comunicati dalle stesse amministrazioni, in ottemperanza all'art. 47, comma 3, CAD. Tale precetto prevede che i soggetti pubblici sono tenuti a rendere disponibile, attraverso l'IPA, «almeno una casella di posta elettronica certificata per ciascun registro di protocollo». Per espresso disposto dell'art. 6-*ter*, CAD, i recapiti digitali figuranti nell'elenco ora considerato sono, peraltro, destinati a consentire solo «le comunicazioni e lo scambio di informazioni e […] l'invio dei documenti» (non sono menzionate le notificazioni).

Infine, l'ultimo elenco menzionato dall'art. 16-*ter* del D.L. n. 179/2012 è il «registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia» (c.d. ReGIndE). In detto pubblico elenco sono contenuti i dati identificativi e i riferimenti telematici di diversi soggetti, tra cui i professionisti e le imprese, i cittadini censiti nell'Anagrafe Nazionale della Popolazione Residente, i professionisti non iscritti in albi e le pubbliche amministrazioni.

Il ReGIndE è la fonte più sicura da cui estrarre gli indirizzi digitali fruibili per le notificazioni degli atti giudiziari, giacché la sua utilizzabilità, per tali scopi, è normativamente stabilita ed è pacificamente riconosciuta dalla giurisprudenza sia civile sia amministrativa.

Occorre, tuttavia, sottolineare che la formazione di tale Registro e le modalità di raccolta dei dati informatici ivi riportati sono diverse a seconda della tipologia del soggetto da indicizzare.

Per quanto riguarda i privati, il sistema prevede che sia il Ministero a recuperare ed immettere automaticamente nell'elenco i recapiti già indicati in albi o registri pubblici (ad esempio i dati comunicati dai professionisti ai propri Ordini). Ne consegue che, per tali soggetti, l'indirizzo PEC desunto dal ReGIndE coincide con quello risultante dall'elenco INI-PEC o dall'albo professionale di appartenenza.

Al contrario, per le pubbliche amministrazioni, l'individuazione del recapito telematico (dedicato alla ricezione delle notifiche) e la relativa comunicazione al ReGIndE è lasciata all'iniziativa delle stesse amministrazioni (e, quindi, alla loro diligenza). Queste ultime, infatti, sono tenute ad eleggere uno specifico do-

micilio digitale per il ricevimento delle notifiche e a trasmetterlo al Ministero; in particolare l'art. 16, comma 12, D.L. n. 179/2011, ha statuito che le pubbliche amministrazioni dovevano rendere noto, entro il 30 novembre 2014, al Ministero della Giustizia l'indirizzo PEC adibito alla predetta funzione.

È inutile dire che molti enti pubblici non hanno adempiuto all'obbligo comunicativo ora ricordato, in tal modo precludendo di fatto (o, quantomeno, rendendo oltremodo incerto ed aleatorio) ai terzi l'esercizio della facoltà di notificazione, in via telematica, nei loro confronti. Si rammenta al riguardo che gli indirizzi PEC estraibili dall'IndicePa sono, a stretto rigore, destinati esclusivamente alle comunicazioni, allo scambio di informazioni e all'invio dei documenti.

È stato giustamente rilevato dalla dottrina (G. CARULLO, 2019) che il differente trattamento riservato dalla disciplina in esame ai privati e alle pubbliche amministrazioni non trova adeguate giustificazioni di ordine logico-giuridico. In effetti, le stesse esigenze organizzative e gestionali, che possono giustificare, per le pubbliche amministrazioni, la previsione di distinte PEC per le notifiche degli atti giudiziari e per le altre tipologie di comunicazione e, quindi, l'elezione di più domicili digitali, sono parimenti predicabili anche per molti privati (si pensi alle grandi e medie imprese o ai liberi professionisti).

Il ReGIndE, inoltre, non è liberamente consultabile, a differenza di tutti gli altri elenchi pubblici contemplati dal CAD, ovvero l'INI-PEC, l'IPA e l'istituendo elenco di cui all'art. 6-*quater*. L'accesso al registro gestito dal Ministero della Giustizia richiede, infatti, una specifica abilitazione, la quale deve avvenire «mediante carta d'identità elettronica o carta nazionale dei servizi e sul punto di accesso mediante autenticazione a due fattori oppure tramite token crittografico (smart card, chiavetta USB o altro dispositivo)» (così stabiliscono le specifiche tecniche al D.M. 21 febbraio 2011, n. 44). Si tratta, dunque, di una abilitazione particolarmente rigorosa – di cui francamente si stenta a comprendere la necessità – che si fonda su una procedura complessa finalizzata all'identificazione dell'utente che desidera visionare il ReGIndE. Tale limitazione all'accesso del Registro in questione rende ancor più disagevole la posizione del soggetto che intende notificare, in via telematica, un atto giudiziale alla Pubblica Amministrazione dato che questi può conoscere, con certezza, il domicilio digitale da utilizzare per l'adempimento solo compulsando il predetto registro.

Le suesposte considerazioni inducono a dubitare della conformità del regime innanzi descritto al principio di uguaglianza sancito dall'art. 3 della Costituzione. Inoltre, le restrizioni poste dal legislatore alla consultabilità del ReGIndE non appaiono suffragate da valide ragioni di interesse pubblico e, quindi, risultano in conflitto con i principi di ragionevolezza e trasparenza della Pubblica Amministrazione (v. capitolo VIII, S. ROSSA).

Sarebbe quanto mai auspicabile un intervento del legislatore volto a razionalizzare e semplificare la materia: in particolare sarebbe opportuno che si prevedesse un unico sistema di raccolta dei dati telematici relativi a soggetti pubblici e privati ed un unico pubblico elenco degli indirizzi PEC, validi per le notifiche e le comunicazioni, liberamente accessibile per chiunque.

8. Il domicilio digitale della P.A.

Si è già avuto occasione di porre in rilievo le oggettive difficoltà di identificare, con certezza, l'indirizzo PEC da utilizzare per le notifiche telematiche alle pubbliche amministrazioni.

I problemi che si possono presentare sono molteplici: innanzitutto non è infrequente il caso che la notificazione all'amministrazione sia stata effettuata ad indirizzo di posta elettronica estratto da un elenco pubblico (essenzialmente l'elenco IPA) diverso dal ReGIndE per l'impossibilità di reperire nel registro ministeriale il domicilio digitale dell'amministrazione interessata destinato alla ricezione delle notifiche. In altre ipotesi, l'utilizzo di un recapito telematico non risultante dal ReGIndE è determinato dal mero errore del soggetto notificante. Un simile errore è possibile, in quanto – come si è pocanzi sottolineato – gli enti pubblici hanno la facoltà di dotarsi di più indirizzi PEC, con funzioni distinte, e perché esistono diversi registri contenenti i recapiti digitali delle amministrazioni.

Di tali questioni si è occupata la giurisprudenza amministrativa, la quale, peraltro, non è riuscita sinora a elaborare soluzioni univoche e pacifiche.

Vi è un orientamento più intransigente, che appare ormai recessivo (T.A.R. Sicilia, Palermo, sez. III, sentenza 13 luglio 2017, n. 1842; T.A.R. Toscana, sez. I, sentenza 27 ottobre 2017, n. 1287), secondo cui la notifica via PEC di un atto giudiziario a una amministrazione, presso un recapito informatico non figurante nel ReGIndE, sarebbe inammissibile. L'orientamento ora riferito – che si richiama alla prevalente giurisprudenza della Corte di Cassazione – attribuisce rilievo prioritario all'asserito proponimento del legislatore di individuare un unico domicilio digitale della Pubblica Amministrazione destinato alla ricezione degli atti giudiziali, coincidente con l'indirizzo PEC inserito nel Registro generale gestito dal Ministero della Giustizia. Per l'opinione giurisprudenziale in esame, detto registro è l'unico «qualificato ai fini processuali ed idoneo a garantire l'organizzazione preordinata all'effettiva difesa» (Cass. civ., sez. III, sentenza 8 febbraio 2019, n. 3709).

La notifica telematica eseguita nei modi innanzi descritti sarebbe, dunque, nulla (Cons. giust. amm. Reg. Sicilia, sez. giurisd., sentenza 16 luglio 2018, n. 43; T.A.R. Lombardia, Brescia, sez. I, sentenza 26 febbraio 2018, n. 234); è inoltre,

generalmente esclusa la rinnovabilità della notificazione (anche attraverso i mezzi tradizionali) e la ricorrenza dell'errore scusabile – e, quindi, la possibilità di concedere la rimessione in termini – salvo che sussistano specifiche condizioni.

L'indirizzo giurisprudenziale prevalente è, al contrario, propenso a considerare, nelle ipotesi in esame, la notifica affetta da mera irregolarità e ad ammettere, quindi, la sanabilità della stessa (Cons. Stato, sez. VI, sentenza 13 dicembre 2017, n. 5891; T.A.R. Sicilia, Palermo, sez. I, sentenza 22 gennaio 2018, n. 179). Si fa giustamente notare che la nullità costituisce l'*extrema ratio* ed è configurabile nei soli casi in cui sia espressamente prevista *ex lege* e salva l'ipotesi di conservazione dell'atto che comunque abbia raggiunto lo scopo al quale è preordinato (in ottemperanza all'art. 156, comma 3, c.p.c.). Si osserva, inoltre, che l'IndicePA è qualificato dalla legge come «pubblico elenco di fiducia» (art. 6-*ter*, comma 1, CAD); per questa ragione si ritiene che tale elenco assuma valore equipollente al ReGIndE (Cons. Stato, sez. V, sentenza 12 dicembre 2018, n. 7026). Si rileva, infine, che, qualora l'invio del ricorso ad un indirizzo PEC diverso da quello risultante dal registro ministeriale sia stato determinato dall'inottemperanza dell'obbligo di comunicare il recapito informatico da inserire nel predetto elenco da parte dell'amministrazione, l'errore nell'identificazione del domicilio digitale è imputabile alla medesima amministrazione e, come tale, è emendabile (Cons. giust. amm. Reg. Sicilia, sentenze nn. 216 e 217 del 12 aprile 2018). In taluni pronunciamenti si prospetta la linea interpretativa ora indicata anche nell'ipotesi in cui l'errore, di cui si discute, non sia stato causato dal comportamento dell'amministrazione destinataria della notifica (si vedano le sentenze da ultimo richiamate).

L'orientamento giurisprudenziale ora riferito, pur avendo l'indubbio pregio di richiamare ed applicare in *subiecta materia* i principi di leale collaborazione, autoresponsabilità, tutela dell'affidamento e strumentalità delle forme, non risulta comunque pienamente condivisibile. Infatti, il riconoscimento, nella fattispecie, della sussistenza di una mera irregolarità sanabile fa comunque ricadere gli effetti sfavorevoli della notifica telematica non perfettamente eseguita (solo) sul soggetto ricorrente – il quale sarà comunque tenuto a rinnovare la notificazione, con tutti i rischi e gli oneri che questo ulteriore adempimento comporta – anche nel caso in cui la irregolarità riscontrata sia, in realtà, dovuta alla mancata elezione del domicilio digitale per la ricezione degli atti giudiziali da parte dell'amministrazione.

Un simile comportamento omissivo è senza dubbio censurabile, non solo perché rende incerta la notificazione del ricorso (ingenerando difficoltà operative e dubbi sulle modalità della notifica ed esponendo il ricorrente al rischio manifesto di cadere in errori, potenzialmente esiziali), ma anche (e soprattutto) perché è incontrovertibilmente contraria ai doveri di imparzialità, correttezza e

buon andamento. La trascuratezza in parola – a stretto rigore – inibisce, in termini concreti, alla parte privata la notificazione informatica a favore di quella cartacea, di per sé disagevole e onerosa, nonché possibile fonte di imperfezioni formali all'atto della successiva inclusione nel modulo di deposito telematico; la suddetta mancanza, poi, è comunque e di per sé rappresentativa di una condotta antigiuridica, lesiva dei principi di trasparenza e buona fede.

L'inosservanza, da parte dell'amministrazione, della previsione che impone di comunicare l'indirizzo agli uffici ministeriali non è, tuttavia, espressamente sanzionata dal Legislatore, il quale non appresta alcun rimedio né coercitivo né punitivo all'indolenza della P.A. Le condotte pubbliche confliggenti con una norma di legge e implicanti una deviazione dai doveri costituzionali di imparzialità e buon andamento – come quella qui considerata – non possono, però, essere prive di qualsiasi conseguenza per il soggetto responsabile di tali condotte e comunque non devono risolversi in un vantaggio indebito per quest'ultimo. In tale prospettiva, sembrerebbe più giusto e ragionevole trasferire eventuali disagi processuali sulla parte (e solo su quella parte) che, con la sua negligenza, ha impedito al ricorrente di notificare l'atto secondo le disposizioni che disciplinano l'assolvimento, in via telematica, degli oneri processuali funzionali all'instaurazione del giudizio.

Per le suesposte ragioni sarebbe opportuno che la giurisprudenza giungesse finalmente ad affermare, almeno in linea di principio, l'incondizionata validità ed efficacia della notificazione *paperless* a domicilio digitale tratto (anche) dall'IndicePA (nella sentenza del T.A.R. Piemonte, Torino, sez. II, 10 gennaio 2018, n. 41, è stata considerata valida anche la notificazione fatta ad un indirizzo PEC desunto dal sito istituzionale dell'amministrazione destinataria).

La notificazione dovrebbe essere ritenuta esente da vizi, difetti o irregolarità anche nel caso in cui l'errore nell'individuazione del corretto domicilio digitale non sia stato indotto dal comportamento dell'amministrazione, che abbia colpevolmente trascurato di fornire al Ministero l'indirizzo PEC valido per la notificazione, in via telematica, degli atti giudiziari.

In quest'ultimo caso, tuttavia, la soluzione interpretativa ora prospettata è configurabile solo qualora sussistano talune condizioni "minime", in grado di garantire l'esito positivo della notificazione effettuata, ossia la sicura ricezione dell'atto inviato e la piena conoscibilità dello stesso da parte del destinatario: a tal fine appare necessario, innanzitutto, che il differente recapito utilizzato dal ricorrente sia comunque riconducibile, con certezza, all'amministrazione resistente (detta ipotesi è predicabile, in particolare, quando l'indirizzo in concreto impiegato per la notificazione sia stato estratto dal sito istituzionale dell'autorità interessata o da elenchi pubblici, quali, ad esempio, gli elenchi INI-PEC o IPA); occorre, inoltre, che siano rispettati i requisiti indispensabili per la

consistenza strutturale dell'adempimento in parola (in primo luogo la dizione nell'oggetto del messaggio «notificazione ai sensi della legge n. 53 del 1994», che, di per sé, consente al destinatario di apprendere agevolmente il contenuto e la finalità della comunicazione e dell'atto allegato) e che, naturalmente, il sistema informatico del mittente dia evidenza della ricezione dell'atto stesso.

Qualora siano rinvenibili i suindicati presupposti, la notificazione, seppur non perfettamente corrispondente al modello legale di riferimento, appare pienamente idonea ad assolvere alla funzione sua propria, ovvero a quella di rendere edotto il destinatario dell'iniziativa giudiziale *ex adverso* intrapresa e di metterlo nelle condizioni di costituirsi in giudizio e di esercitare i diritti di difesa. Infatti, anche il ricorso inviato ad un indirizzo PEC dell'amministrazione resistente diverso da quello contenuto nel ReGINde è, comunque, indiscutibilmente pervenuto nella sfera di conoscibilità della stessa amministrazione, una volta che quest'ultima abbia ricevuto il relativo messaggio di posta elettronica certificata; pertanto la notificazione in tal modo eseguita ha raggiunto il suo scopo.

In ossequio ai principi del giusto processo, enucleati nell'art. 111 Cost., e del principio della strumentalità delle forme, le regole processuali sono, o perlomeno dovrebbero essere, preordinate ad assicurare il rispetto di effettive garanzie difensive. Nelle ipotesi di cui si discute, non sembra, peraltro, che le fondamentali esigenze del contraddittorio siano suscettibili di essere pregiudicate o compromesse, almeno sino a prova contraria (nel qual caso sembrerebbe sufficiente, in forza dei principi di ragionevolezza, proporzionalità e conservazione degli atti, una mera regolarizzazione postuma). In effetti, con l'uso della normale diligenza l'amministrazione è certamente in grado di compiere l'attività giudiziale che ritiene utile o necessaria anche qualora abbia ricevuto la notificazione del ricorso ad un indirizzo PEC differente da quello da essa stessa prescelto per tale tipologia di comunicazione legale rivolta nei suoi confronti.

Rimane, tuttavia, ferma anche nel vigore del PAT la regola, già invalsa nel sistema processuale precedente (art. 11, r.d. 30 ottobre 1933, n. 1611, e succ. modif.), secondo cui la notificazione del ricorso ad una amministrazione statale deve essere eseguita presso l'Avvocatura distrettuale delle Stato, territorialmente competente, a pena di nullità della stessa notifica (sanabile dall'eventuale costituzione in giudizio dell'autorità pubblica intimata): in ossequio a tale regola generale, il T.a.r. Lombardia, Milano, sez. I, nella recente sentenza 29 settembre 2020, n. 1725, ha dichiarato l'inammissibilità di un ricorso per nullità della relativa notificazione effettuata all'indirizzo PEC dell'amministrazione statale resistente, piuttosto che all'indirizzo PEC dell'Avvocatura distrettuale dello Stato domiciliataria *ex lege*.

Occorre sottolineare che, di recente, il legislatore è intervenuto a regolare la materia qui esaminata con una nuova disposizione che, sebbene non assuma

valore risolutivo rispetto ai problemi sopra illustrati, relativi alla determinazione del domicilio digitale delle pubbliche amministrazioni, è comunque destinata ad agevolare in modo significativo il compito di coloro che hanno l'esigenza di individuare il predetto domicilio, al fine di eseguire una notificazione telematica. Si tratta, in particolare, dell'art. 28, comma 1, lett. c), del già citato DL-semplificazioni n. 76/2020 (D.L. 16 luglio 2020, n. 76, convertito dalla Legge 11 settembre 2020, n. 120), il quale stabilisce che «in caso di mancata indicazione nell'elenco di cui all'articolo 16, comma 12 [*id est* nel ReGIndE], la notificazione alle pubbliche amministrazioni degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale è validamente effettuata, a tutti gli effetti, al domicilio digitale indicato nell'elenco previsto dall'articolo 6-*ter* del decreto legislativo 7 marzo 2005, n. 82, [*id est* nell'IndicePA] e, ove nel predetto elenco risultino indicati, per la stessa amministrazione pubblica, più domicili digitali, la notificazione è effettuata presso l'indirizzo di posta elettronica certificata primario indicato, secondo le previsioni delle Linee guida di AgID, nella sezione ente dell'amministrazione pubblica destinataria». La stessa novella ha, inoltre, introdotto la facoltà, per i pubblici apparati, di comunicare al Ministero della Giustizia gli indirizzi di posta elettronica di propri organi o distaccamenti, anche territoriali, ai fini del loro inserimento nel ReGIndE, in tal modo consentendo anche a queste ultime articolazioni interne di ricevere comunicazioni e notificazioni in forma ufficiale e diretta.

La norma ora riferita attribuisce, dunque, ancora valore preferenziale e prioritario al ReGIndE; tuttavia essa ha l'innegabile pregio di riconoscere chiaramente l'utilizzabilità, per le notifiche alle pubbliche amministrazioni, anche dell'IndicePa, qualora nel registro ministeriale non sia riportato alcun recapito utile a tale scopo.

9. Il deposito telematico

Un volta notificati a mezzo PEC o con gli strumenti tradizionali contemplati dagli artt. 137 ss. c.p.c., il ricorso e i documenti correlati – in formato PDF o negli altri formati elettronici consentiti dall'art. 12 delle specifiche tecniche contenute nell'Allegato 2 al d.P.C.S. n. 134/2020 – sono depositati nella segreteria del giudice con le modalità telematiche prescritte dalla disciplina del PAT (così dispongono l'art. 136, comma 2, c.p.a., e l'art. 9, comma 2, d.P.C.S. n. 134/2020).

In particolare, per il deposito del ricorso introduttivo e degli allegati è necessario compilare il modulo denominato «ModuloDepositoRicorso», scaricabile dal Sito istituzionale della giustizia amministrativa (www.giustizia-amministrativa.it).

Le parti intimate possono, a loro volta, costituirsi in giudizio e difendersi

esclusivamente depositando e producendo, in via telematica, atti e documenti in formato digitale (art. 136, comma 2, c.p.a.).

Per il deposito degli atti successivi al ricorso occorre utilizzare uno specifico modulo, denominato «ModuloDepositoAtto», parimenti reperibile nel sito istituzionale della giustizia amministrativa (art. 6, comma 2, delle specifiche tecniche riportate nell'Allegato 2 al d.P.C.S. n. 134/2020).

I predetti moduli sono in formato PDF e devono essere sottoscritti dall'avvocato con firma digitale PAdES (art. 6, comma 4, delle specifiche tecniche da ultimo richiamate).

Si ricorda, inoltre, che, in forza dell'art. 136, comma 2-*ter*, c.p.a., il difensore, quando deposita la copia informatica, anche per immagine, di un atto processuale di parte, di un provvedimento del giudice o di un documento redatto su supporto analogico e detenuto in originale o in copia conforme, è tenuto ad attestare la conformità della copia depositata all'atto in suo possesso con la dichiarazione prescritta dall'art. 22, CAD.

Il deposito del ricorso introduttivo e degli altri atti di parte si effettua tramite PEC individuale dell'avvocato difensore (art. 6, comma 4, delle specifiche tecniche definite nel d.P.C.S. n. 134/2020); i predetti atti devono essere inviati alla casella di posta elettronica certificata della sede giudiziaria adita, pubblicata sul sito istituzionale della giustizia amministrativa (art. 7, comma 1, delle specifiche tecniche testé menzionate).

In via subordinata, è possibile procedere al deposito del ricorso e degli altri atti di parte mediante *upload* (ovvero mediante caricamento del modulo di deposito direttamente sul sito istituzionale della giustizia amministrativa), utilizzando la relativa funzione presente nel predetto sito (art. 8, comma 1, delle specifiche tecniche riportate nel d.P.C.S. n. 134/2020). Per usufruire di tale servizio, l'avvocato deve, però, rendere noti i motivi che non gli hanno consentito il deposito via PEC e comunicare, altresì, il codice identificativo del messaggio ricevuto di mancato deposito dell'atto con il mezzo informatico "ordinario" (così stabilisce la disposizione da ultimo citata, al comma 2).

Ai fini del rispetto dei termini processuali, il deposito si considera effettuato nel momento in cui è stata generata dal S.I.G.A. (sistema informativo della giustizia amministrativa) la ricevuta di accettazione della PEC di deposito (art. 7, comma 5, delle specifiche tecniche allegate al d.P.C.S. n. 134/2020). L'avvenuta registrazione del deposito può essere verificata anche attraverso l'apposita funzione accessibile tramite il Portale dell'avvocato.

Nel processo *paperless* è assicurata la possibilità di depositare, in via informatica, gli atti fino alle ore 24.00 dell'ultimo giorno consentito; in particolare il deposito è tempestivo se entro le ore 24.00 del giorno della scadenza è generata dal S.I.G.A. la ricevuta di accettazione (art. 4, comma 4, All. 2, delle nor-

me di attuazione del c.p.a., come modificato dall'art. 7, comma 2, lett. b), del D.L. n. 168/2016).

Peraltro, nei casi in cui la disciplina processuale prevede il deposito di atti e documenti sino al giorno precedente la trattazione di una domanda in camera di consiglio, rimane ferma la regola, valevole nel regime anteriore all'entrata in vigore del PAT, secondo cui il deposito deve avvenire entro le ore 12.00 dell'ultimo giorno utile (art. 4, comma 2, All. 2, delle norme di attuazione del c.p.a.; art. 9, comma 4, d.P.C.S. n. 134/2020).

Il Legislatore ha altresì imposto agli avvocati una ulteriore incombenza – che appare invero in contraddizione con la *ratio* e i principi che informano il processo *paperless* – consistente nell'obbligo di depositare presso la segreteria del giudice adito almeno una copia "di cortesia", in formato cartaceo, del ricorso e degli altri scritti difensivi, accompagnata dall'attestazione della sua conformità all'originale depositato in via telematica (art. 7, comma 4, D.L. n. 168/2016). La giurisprudenza ha affermato che quest'ultimo adempimento costituisce una condizione per la fissazione e/o la trattazione dell'istanza cautelare e dell'udienza di merito (Cons. Stato, sez. VI, ordinanza cautelare 3 marzo 2017, n. 880).

Detto onere processuale è, tuttavia, venuto meno di recente: infatti, la già citata Legge 25 giugno 2020, n. 70, di conversione del D.L. 30 aprile 2020, n. 28 (contenente, tra l'altro, «disposizioni integrative e di coordinamento in materia di giustizia amministrativa») ha abrogato la suindicata norma, che prevedeva l'obbligo di deposito della copia analogica. In tal modo è caduto l'ultimo baluardo cartaceo che caratterizzava il PAT e, di conseguenza, il processo amministrativo è divenuto (finalmente) un rito integralmente digitale.

In assenza di espresse indicazioni normative, sono sorti dubbi ed incertezze in ordine alle conseguenze derivanti dal mancato rispetto delle forme prescritte dal PAT per il deposito degli atti. In via interpretativa, la giurisprudenza ha rilevato che tale inosservanza non rende il ricorso (o l'atto di causa compiuto) inammissibile o nullo, non essendo esplicitamente previsti simili effetti preclusivi e invalidanti dalla nuova disciplina processuale. Secondo l'orientamento giurisprudenziale pacifico e consolidato, la violazione delle regole in questione determina piuttosto una «situazione di mera irregolarità, sanabile, su ordine del Collegio, nel termine perentorio da questo fissato» (Cons. Stato. sez. IV, sentenza 4 aprile 2017, n 1541, cit.; Id., sentenza 4 aprile 2017, n. 1541, cit.; Id., sez. V, ordinanza 4 gennaio 2018, n. 56, cit.).

10. Le comunicazioni telematiche

A mente dell'art. 13 del d.P.C.S. n. 134/2020, tutte le comunicazioni di segreteria sono effettuate esclusivamente con modalità telematiche.

In particolare, le comunicazioni di segreteria rivolte ai difensori delle parti sono inviate all'indirizzo PEC, risultante da pubblico elenco, di ciascun avvocato componente il collegio difensivo o, in alternativa, all'avvocato domiciliatario eventualmente nominato (art. 13, comma 1, del decreto da ultimo citato). Ai fini dell'efficacia dell'adempimento informativo, è sufficiente che vada a buon fine una sola delle comunicazioni telematiche effettuate dalla segreteria a ciascun avvocato componente il collegio difensivo (art. 136, comma 1, c.p.a.).

Le comunicazioni destinate ai soggetti pubblici e all'Avvocatura dello Stato avvengono, sempre tramite posta elettronica certificata, seguendo la speciale forma di «trasmissione sicura» prevista dall'art. 47 CAD.

Nel messaggio sono riportati gli estremi del provvedimento ed è contenuto l'avviso che il medesimo provvedimento è visibile sul fascicolo informatico relativo alla causa; alla PEC deve essere, altresì, allegato il biglietto di segreteria in formato PDF, del quale occorre riportare nel testo del messaggio anche il codice identificativo (art. 13 delle specifiche tecniche allegate al d.P.C.S. n. 134/2020).

Qualora la trasmissione in via telematica non vada a buon fine per errore del S.I.G.A., l'invio del messaggio è ripetuto e, in caso di ulteriore avviso di mancata consegna, la comunicazione è effettuata a mezzo fax.

L'utilizzazione nel processo amministrativo della PEC, quale mezzo per eseguire le comunicazioni di segreteria (e le notificazioni), ha consentito di superare la regola dettata dall'art. 25, comma 1, lett. a) e b), c.p.a., in virtù della quale la parte che non abbia eletto domicilio nel comune sede del tribunale amministrativo regionale, davanti a cui pende il ricorso, o a Roma, nei giudizi dinnanzi al Consiglio di Stato, si intende domiciliata, ad ogni effetto, presso la segreteria del tribunale amministrativo regionale o del Consiglio di Stato. È stato, infatti, stabilito (art. 25, comma 1-*bis*, c.p.a.) che anche «nel processo amministrativo si applica, in quanto compatibile, l'articolo 16-*sexies* del decreto-legge 18 ottobre 2012, n. 179», in ossequio al quale la notifica in cancelleria è ammessa «esclusivamente quando non sia possibile, per causa imputabile al destinatario, la notificazione presso l'indirizzo di posta elettronica certificata, risultante dagli elenchi di cui all'articolo 6-*bis* del decreto legislativo 7 marzo 2005, n. 82, nonché dal registro generale degli indirizzi elettronici, gestito dal ministero della giustizia».

In tal modo è stata fissata anche per il processo amministrativo la regola già invalsa nel rito civile, secondo cui il domicilio digitale deve essere ritenuto il domicilio principale, ad ogni effetto di legge (Cons. Stato, sez. III, sentenza 22 maggio 2019, n. 3329; Id., sez. IV, sentenza 4 settembre 2019, n. 6089).

Nessun dubbio sussiste in ordine alla *ratio* che ispira la disciplina del PAT ora descritta: è chiara la volontà del legislatore di designare il domicilio digitale come domicilio eletto *ex lege*, perché funzionale alla piena efficienza del processo te-

lematico e alle esigenze a questo connesse (accelerazione dei tempi della giustizia, standardizzazione delle procedure, risparmio di spesa e semplificazione degli adempimenti processuali). Tuttavia, questa designazione, anche in ambito processualcivilistico, assume carattere non esclusivo, ma preferenziale (Cass. civ., sez. III, sentenza 8 giugno 2018, n. 14914; Id., ordinanza 29 gennaio 2020, n. 1982, ivi); è riconosciuta, infatti, una residua area di operatività al domicilio fisico, nel caso di inefficienza della PEC riferibile al destinatario (per causa a questo imputabile), in base alla *regula juris* dettata dall'art. 82, R.D. n. 37/1934, la quale ammette la perdurante rilevanza giuridica dell'elezione del domicilio fisico, in aggiunta al domicilio digitale (Cass. civ., sez. III, sentenza 11 luglio 2017, n. 17048; Id., sez. VI, sentenza 14 dicembre 2017, n. 30139, ivi).

Come si è detto, nel regime del PAT il domicilio digitale, corrispondente all'indirizzo PEC del difensore contenuto in pubblici registri, costituisce il domicilio eletto *ex lege*; ciò significa che il predetto indirizzo è utilizzabile per le comunicazioni di segreteria anche in assenza di una espressa indicazione dello stesso negli atti di causa. In mancanza di tale indicazione, spetta, quindi, alla segreteria il compito di reperire d'ufficio la PEC del difensore attraverso la consultazione dei pubblici registri (ReGIndE o albo avvocati).

In ogni caso, nel processo amministrativo è richiesto agli avvocati di comunicare alla segreteria e alle parti costituite le eventuali variazioni, intervenute nel corso del giudizio, dell'indirizzo di posta elettronica certificata (art. 136, comma 1, c.p.a.). Secondo l'interpretazione data dall'Ufficio Studi del Consiglio di Stato (parere 9 marzo 2018), detto onere imposto ai patrocinatori è giustificato e dovrebbe essere mantenuto almeno sino a quando «il PAT, inteso come sistema operativo, non sia in grado di assicurare la piena e costante accessibilità delle parti e delle segreterie ai pubblici registri e ai loro aggiornamenti».

L'attuale disciplina del processo amministrativo prevede, inoltre, che i difensori devono specificare, nel ricorso o nel primo atto difensivo, il recapito fax, che può anche essere diverso da quello del domiciliatario; quest'ultimo recapito – per espresso disposto normativo – è utilizzabile, per le comunicazioni di segreteria, «esclusivamente qualora sia impossibile inviare tali comunicazioni all'indirizzo di posta elettronica certificata risultante da pubblici elenchi, per mancato funzionamento del sistema informatico della giustizia amministrativa» (art. 136, comma 1, c.p.a.).

Si rammenta, infine, che è ancora consentita e giuridicamente rilevante, anche nel nuovo assetto normativo, l'elezione del domicilio fisico (in aggiunta a quello digitale): anche in questo caso, però, la comunicazione presso il domicilio fisico eletto è legittima solo nell'ipotesi in cui non sia reperibile la PEC dell'avvocato per causa imputabile a quest'ultimo.

11. Copie degli atti, verbale informatico e provvedimenti del giudice

Come si è avuto modo di segnalare in precedenza, tutti gli atti e i documenti processuali sono contenuti in formato digitale nel fascicolo informatico (art. 5, d.P.C.S. n. 134/2020).

In forza dell'art. 136, comma 2-*ter*, c.p.a., all'avvocato è attribuito il potere di attestare la conformità degli atti e dei provvedimenti presenti nel predetto fascicolo, «con conseguente esonero del versamento dei diritti di copia». La medesima disposizione chiarisce che la copia munita dell'attestazione di conformità equivale all'originale o alla copia conforme dell'atto o del provvedimento. Nell'esercizio di tale potere certificativo, i difensori assumono, ad ogni effetto, la veste di pubblici ufficiali.

È in ogni caso fatta salva la facoltà, per la parte, di richiedere alla segreteria dell'ufficio giudiziario adito il rilascio di un duplicato informatico o di una copia informatica, anche per immagini, degli atti, provvedimenti o documenti presenti nel fascicolo informatico. A tal fine, è necessario che l'interessato compili e trasmetta, in via telematica, l'apposito modulo digitale di richiesta, scaricabile dal sito istituzionale della giustizia amministrativa, e che versi, altresì, i relativi diritti di copia (art. 16, comma 1, d.P.C.S. n. 134/2020). La conformità della copia rilasciata all'originale documento elettronico inserito nel fascicolo processuale è attestata dalla sottoscrizione della PEC da parte del segretario, con apposizione della sua firma digitale (art. 16, comma 6, del decreto da ultimo menzionato).

Dopo l'entrata in vigore del processo amministrativo telematico anche il verbale d'udienza deve essere redatto in formato digitale; in particolare, il verbale è sottoscritto, dopo la sua conversione in documento PDF, con firma elettronica dal presidente del collegio e dal segretario d'udienza ed è conservato nel fascicolo informatico (art. 10, d.P.C.S. n. 134/2020).

Allo stesso modo tutti i provvedimenti del giudice sono predisposti e depositati sotto forma di documento informatico e sottoscritti con firma digitale. I provvedimenti collegiali sono redatti dall'estensore, da questo firmati e trasmessi telematicamente al presidente del collegio, il quale, a sua volta, li sottoscrive e li trasmette, in via telematica, alla segreteria per il deposito.

Il segretario di sezione sottoscrive, con propria firma digitale, gli atti inviatigli e provvede al loro deposito nel fascicolo informatico e alla loro contestuale pubblicazione, mediante inserimento dei medesimi atti nel SIGA e nel sito internet della giustizia amministrativa, nel rispetto delle cautele previste dalla normativa in materia di tutela dei dati personali (art. 7, comma 2, d.P.C.S. n. 134/2020).

Il deposito dei provvedimenti con modalità informatiche sostituisce, ad ogni effetto, il deposito con modalità cartacee (art. 7, comma 4, del decreto da ultimo citato).

12. L'Adunanza plenaria e il PAT

In ultimo occorre perlomeno accennare all'innovazione apportata dall'art. 7, comma 3, D.L. n. 168/2016, il quale ha aggiunto alle norme di attuazione del c.p.a. l'art. 13-*bis*, rubricato «Misure transitorie per l'uniforme applicazione del processo amministrativo telematico». Tale novella ha introdotto uno speciale ricorso "accelerato" all'Adunanza plenaria del Consiglio di Stato per la risoluzione dei contrasti giurisprudenziali insorti in merito all'interpretazione e all'applicazione delle norme relative al PAT.

Il citato art. 13-*bis*, c.p.a., prevede, in particolare, che, per tre anni dall'avvio del processo amministrativo telematico (quindi fino al 31 dicembre 2019), il collegio di primo grado cui è assegnato il ricorso, se rileva che il punto di diritto sottoposto al suo esame e vertente sull'interpretazione o sull'applicazione delle norme in tema di processo amministrativo telematico ha già dato luogo a significativi contrasti giurisprudenziali rispetto a decisioni di altri tribunali amministrativi regionali o del Consiglio di Stato, tali da incidere in modo rilevante sul diritto di difesa di una parte, può – con ordinanza emanata su richiesta di parte o d'ufficio e pubblicata in udienza – sottoporre al presidente del Consiglio di Stato istanza di rimessione del ricorso all'esame dell'Adunanza plenaria. Qualora assuma tale iniziativa, il collegio provvede contestualmente all'emanazione dell'ordinanza di rimessione a rinviare la trattazione del giudizio alla prima udienza successiva al sessantesimo giorno dall'udienza in cui è pubblicata l'ordinanza.

Il presidente del Consiglio di Stato comunica l'accoglimento della richiesta entro trenta giorni dal ricevimento e, in tale ipotesi, nell'udienza davanti al tribunale il processo è sospeso fino all'esito della decisione dell'Adunanza plenaria. La mancata risposta del presidente del Consiglio di Stato entro trenta giorni dal ricevimento della richiesta equivale a rigetto. L'Adunanza plenaria è convocata per una data non successiva a tre mesi dalla richiesta e decide la sola questione di diritto relativa al processo amministrativo telematico.

Bibliografia

CARDARELLI F., *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. dell'informazione e dell'informatica*, 2015, p. 227.

CARULLO G., *Elezione del domicilio digitale per la ricezione di notifiche di atti giudiziari: dubbi in relazione alla diversa disciplina dettata per i privati e per le pubbliche amministrazioni*, in *Dir. proc. amm.*, 2019, p. 228.

CARULLO G., *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, Torino, 2017.

CARULLO G., *Nuove insidie nel processo amministrativo telematico: standard di firma*

digitale e validità della notifica, in *Giustamm.it*, 4, 2017.
CARULLO G., *Posta Elettronica Certificata e domicilio digitale: futuro ed incertezze in una prospettiva europea*, in *Riv. it. dir. pubbl. com.*, 2016, p. 51.
CASSANO G., GIURDANELLA C. (a cura di), *Il codice dell'amministrazione digitale, commentario al D.Lgs. n. 82 del 7 marzo 2005*, Giuffrè, Milano, 2005.
D'ALESSANDRI F., *Il processo amministrativo telematico tra questioni risolte e problematiche ancora aperte e la notifica via PEC alle pubbliche amministrazioni*, in *www.giustizia-amministrativa.it*, 2018.
D'ALESSANDRI F., *Processo amministrativo telematico*, in *Treccani.it*, 2019.
D'ALESSIO D., *Il processo amministrativo telematico. Profili generali e disciplina*, Relazione al convegno "*Il Processo Amministrativo Telematico*", Roma, 12 maggio 2017, in *www.giustizia-amministrativa.it*.
D'ORLANDO E., *Profili costituzionali dell'amministrazione digitale*, in *Dir. dell'informazione e dell'informatica*, 2011, p. 213.
DE LEONARDIS F., *La notificazione diretta del ricorso giurisdizionale via posta elettronica certificata (PEC) tra autonomia ed eteroreferenzialità del processo amministrativo*, in *Dir. proc. amm.*, 2016, p. 432.
DUNI G., *L'amministrazione digitale. Il diritto amministrativo nella evoluzione telematica*, Giuffrè Milano, 2008.
FANTIGROSSI U., *Per un processo amministrativo telematico giusto*, in *Lexitalia.it*, 1, 2016.
FRENI F., CLARIZIA P., *Il nuovo processo amministrativo telematico*, Giuffrè, Milano, 2016.
GAFFURI F., *Brevi note sulle notifiche via PEC alla pubblica amministrazione*, in *CERIDAP*, 3, 2020.
GALETTA D.-U., ZILLER J. (a cura di), *Information and Communication Technologies Challenging Public Law, beyond Data Protection*, *Atti del 12° congresso annuale della Societas Iuris Public Europaei (SIPE)*, Nomos Verlagsgesellschaft, 2018.
GALLO C.E., *L'attuazione del processo amministrativo telematico*, in *Urb. app.*, 2016, 6, p. 631.
MADDALENA M.L., *La digitalizzazione della vita dell'amministrazione e del processo*, in *Foro amm.*, 2016, p. 2585.
PISANO I.S.I., *Manuale di teoria e pratica del processo amministrativo telematico*, Giuffrè, Milano, 2013.
PROVENZANO P., *Decreti Madia e nuova disciplina del c.d. "domicilio digitale": quali prospettive?*, in *Federalismi.it*, 6, 2010.
SDANGANELLI A., *Notificazione degli atti a mezzo PEC nel processo amministrativo*, in *Lexitalia.it*, 1, 2016.
VIOLA L., *Il P.A.T. dopo l'emergenza Covid-19*, in *Urb. app.*, 2020, 4, p. 476.
VIOLA L., *I diversi modi di guardare il P.A.T. e le strategie di adattamento dell'ambiente forense*, in *Lexitalia.it*, 4, 2018.
VIOLA L., *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Foro amm.*, 2018, p. 1598.
VIOLA L., *Diritto e tecnica nel processo amministrativo telematico*, in *Federalismi.it*., 11, 2016.

Indice analitico

T

V

Finito di stampare nel mese di ottobre2020
nella Stampatre s.r.l. di Torino
Via Bologna, 220