Corso di Laurea magistrale

in Governance delle organizzazioni pubbliche

Tesi di laurea

Trasparenza amministrativa e trattamento dei dati personali con focus sul ruolo del GDPR all'interno di una società in house

Relatore

Ch. Prof. Luigi Benvenuti

Laureando

Andrea Pellegrinon
Matricola 849344

Anno Accademico

2021/2022

Sommario

Introduzione

Nell'ultimo periodo storico abbiamo assistito sempre più ad una transizione digitale che ha rappresentato da un lato una maggior confluenza e condivisione di dati (cosiddetto fenomeno dei big data) aiutando le diverse amministrazioni nella gestione delle pratiche e delle mansioni a loro spettanti e dall'altro un irrigidimento in materia di tutela dei dati (siano essi sensibili o meno) con conseguente burocratizzazione dei processi. Ebbene, nonostante si continui ad affermare che sia necessario un intervento di sburocratizzazione con conseguente semplificazione dei procedimenti che fanno capo alle Pubbliche Amministrazioni, più informazioni ci sono da gestire e maggiore si presenta il grado di complessità riguardante la tutela di queste ultime. Basti pensare, da un punto di vista prettamente privatistico, al sistema dei social piuttosto che delle piattaforme digitali di streaming fioriti nel ventunesimo secolo dove la quantità di dati immessi in rete è cresciuta e sta crescendo smisuratamente. È chiaro, quindi, come sia necessario un intervento di salvaguardia della mole di informazioni, riguardanti sia persone fisiche che giuridiche, che ogni giorno viene trattata. Per esempio, la sentenza n° 20 del 2019 rilasciata dalla Corte costituzionale, che verrà analizzata successivamente, si focalizza sul bilanciamento tra i principi della pubblicità e della trasparenza da un lato e il diritto alla riservatezza dall'altro. In un sistema, a livello europeo, molto eterogeneo giuridicamente parlando, il diritto alla protezione dei dati personali ha incontrato diversi limiti, vedendosi quasi sminuire nei confronti di un operato amministrativo sempre più trasparente e sempre più vicino a verificare la famosa metafora a cui ha fatto riferimento il politico nonché leader del partito del socialismo in Italia, Filippo Turati, nel 1908, in un discorso alla Camera dei Deputati nel quale affermava che "dove un superiore pubblico interesse non imponga un momentaneo segreto, la casa dell'amministrazione dovrebbe essere di vetro". Il complesso tema della trasparenza amministrativa è stato

relativamente dibattuto e ha subito delle modifiche (anche rivelatesi, in un secondo momento, ininfluenti), durante gli ultimi decenni, dovute al cambiamento generazionale delle tecnologie sopra citate. Nonostante ancora alcuni punti risultino al limite del pressapochismo (soprattutto in termini di contrasto interno tra leggi derivanti da fonti diverse), dapprima in Europa e successivamente anche in Italia, gli strumenti introdotti per assicurare una maggior condivisione del nuovo "oro nero" (come definito da alcuni) forniscono alle Pubbliche Amministrazioni la possibilità da un lato di operare con maggior efficacia tra di loro ma dall'altro si potrebbero definire limitate da un legislatore sempre più attento ai temi riguardanti, per l'appunto, la tutela dei dati personali in capo a soggetti terzi e facenti parte delle informazioni condivise: il tutto in un sistema di circolazione dei dati che, soprattutto a livello sovranazionale, sta lasciando spazio, in maniera imprescindibile, a degli scenari che andranno sempre più analizzati in un'ottica prettamente normativa. Tematica di attualità visto il caso dell'azienda sanitaria della regione Lazio, che verrà menzionata nel secondo capitolo.

Verrà fornita un'attenta analisi in materia di trasparenza con riferimento ad una società per azioni controllata dal Comune di Venezia (Venis S.p.A.) e in particolare ci si soffermerà sulla particolare tematica riguardante il regolamento generale sulla protezione dei dati, cosiddetto GDPR (acronimo inglese di General Data Protection Regulation) ufficialmente adottato il 27 aprile 2016[1]; di enorme rilevanza e ormai all'ordine del giorno sarà stabilire come quest'ultimo possa interferire con il principio di pubblicità relativo alla tematica della trasparenza, in particolare tenendo presenti due principi importanti quali sono quelli di privacy by design e by default che verranno approfonditi in seguito introducendo ed esemplificando con uno dei progetti di cui la società suddetta è

[1] Wikipedia, *Regolamento generale sulla protezione dei dati,* https://it.wikipedia.org/.

responsabile (piattaforma DiMe con titolare individuato nel Comune di Venezia). Tutto ciò quindi in un panorama in cui le Pubbliche Amministrazioni sono chiamate a valutare molto attentamente quali possano essere le conseguenze di un'eventuale diffusione, anche "impropria", di dati pubblici, i quali risultano essere sempre più al centro di ogni operazione e azione riguardanti sia organi pubblici che organi privati controllati.

Capitolo 1 Trasparenza nella PA

La trasparenza nelle Pubbliche Amministrazioni (da qui in poi verrà utilizzato l'acronimo PA) è una materia molto importante dal punto di vista lavorativo e gestionale. Si riferisce alla pubblicità dei processi svolti con tutte le loro sfaccettature, dall'operato all'utilizzo delle risorse pubbliche e all'accessibilità totale agli atti comprensivi di dati e documenti in possesso dei suddetti organi in ottemperanza di una normativa quale è il decreto legislativo 14 marzo 2013, n°33[2] (c.d. Codice della trasparenza). Rispetto a quanto pubblicato dal Ministero dell'Interno, con quanto sopra descritto si intende:

- Assicurare la conoscenza dei servizi resi;
- Prevenire fenomeni di corruzione (altra tematica che verrà approfondita successivamente);
- Sottoporre al controllo diffuso ogni fase del ciclo di gestione della performance.

In particolare, ogni amministrazione è obbligata a fornire pubblicamente dati inerenti all'organizzazione, l'attività e l'uso delle risorse pubbliche, le prestazioni offerte e i servizi erogati. Quanto appena detto deve comparire in un'apposita sezione denominata "Amministrazione trasparente" nella home page dei rispettivi siti istituzionali[3]. È inoltre previsto un ulteriore strumento di tutela per i cittadini nel caso in cui l'amministrazione non provvedesse a rendere pubblici i suddetti documenti. Si tratta dell'accesso civico che si estrinseca nella richiesta (da parte del cittadino) di informazioni omesse dalla Pubblica Amministrazione. In particolare, si farà riferimento ad una tipologia di accesso, introdotta con il decreto legislativo n. 97 del 2016, relativa al cosiddetto FOIA (Freedom of Information Act) che stabilisce normativamente una quasi totale garanzia

[2] Ministero dell'Interno, https://www.interno.gov.it/.

[3] Camera dei deputati, *Diritto di accesso e trasparenza della pubblica amministrazione*, in Temi dell'attività parlamentare, https://temi.camera.it/.

inerente alla possibilità, riconosciuta a chiunque, di richiedere specifiche informazioni detenute dalle Pubbliche Amministrazioni. L'accesso civico generalizzato, infatti, affiancando ulteriori tipologie di accesso che verranno menzionate successivamente, rappresenta il mezzo con il quale un singolo individuo (cittadino) possa richiedere di accedere a dati e informazioni senza dover dimostrare di essere in possesso di un interesse specifico e qualificato.

Il conflitto tra trasparenza e privacy è un tema di rilevanza fondamentale, tuttavia è possibile definirli come due interessi non contrastanti e ciononostante però la raccolta infinita di informazione possa sfociare nella c.d. opacità per confusione ovvero una raccolta che genera una gestione dei dati confusa a causa del superfluo[4] (la raccolta dei dati deve essere pianificata in modo tale da richiedere solo ed esclusivamente le informazioni necessarie al raggiungimento dei fini prefissati). Tutto ciò è rinvenibile e analizzabile sul fatto che l'amministrazione, nell'ottemperare alle sue funzioni, potrebbe dover giocare due ruoli diversi, ovvero, da un lato assicurando il diritto di accesso al cittadino e quindi fornendo, con estrema cura, una cautela del diritto alla privacy e alla riservatezza di ognuno, dall'altro tutelando questi ultimi diritti sfavorendo e, di conseguenza, ponendo dei limiti all'accesso civico. È chiaro, dunque, come la PA si ritrovi in un limbo nel quale debba garantire, anche se per certi versi, di natura opposta, entrambi i diritti all'accesso civico e alla privacy. Alla luce di tutto ciò, il Regolamento europeo del 2016, inerente la protezione dei dati personali, che verrà ripreso e trattato nel merito nei successivi capitoli, offre una prospettiva comunitaria interessante che coinvolge quanto appena detto. Con una transizione digitale sempre più presente in ambito pubblico, i diritti dei cittadini nella dimensione online devono essere garantiti come in quella c.d. offline, "è necessario considerare che il mondo digitale non debba essere inteso come una

[4] Soro, *PA digitale talks – La protezione dei dati personali nella PA digitale*, Podcast di Ernesto Belisario, 2021, https://www.spreaker.com/.

zona franca in cui i diritti sopra citati possano essere violati"[5], soprattutto in caso di interoperabilità dei diversi sistemi informatici. Tuttavia, una deroga al diritto di accesso è prevista dalla normativa italiana in quanto enuclea un numero tassativo di casi di esclusione (Legge n°15/2005, art. 16 in sostituzione dell'art. 24, legge n° 241/1990) quali:

- Documenti coperti da segreto di Stato, ovvero documenti, notizie ecc., la cui diffusione possa comportare un rischio concreto per l'integrità della Repubblica (legge 124/2007, art. 39, comma 1)[6];
- Procedimenti tributari;
- Attività amministrativa volta all'emanazione di atti normativi, di pianificazione e di programmazione;
- Procedimenti selettivi (in cui si trattino informazioni di carattere psico-attitudinale relativi a terzi).

Successivamente a questa breve disamina del ruolo della trasparenza nella PA, si vuole analizzare un caso specifico, attinente in modo trasversale al Regolamento europeo sulla protezione dei dati personali, riferito al fenomeno del c.d. whistleblowing. Tuttavia, prima di focalizzarsi meglio sul diritto di accesso in chiave di tutela dei dati personali, è utile approfondire le due tematiche di pubblicità e trasparenza anche da un punto di vista storico. Infatti, i due termini summenzionati sono spesso abusati nel loro utilizzo in quanto da un lato esprimono lo stesso concetto (in chiave di diritto del cittadino ad essere informato), ma dall'altro, in concreto, i loro significati, possono non essere del tutto sovrapponibili. Il termine trasparenza è adibito al concetto secondo il quale la Pubblica Amministrazione debba essere intesa come una "casa di vetro"; ovvero, in senso metaforico si vuole pensare a due dimensioni di una scatola

[5] Soro, *PA digitale talks – La protezione dei dati personali nella PA digitale*, Podcast di Ernesto Belisario, 2021, https://www.spreaker.com/.
[6] Wikipedia, *Segreto di Stato (Italia)*, https://www.wikipedia.it/.

nella quale interna agisca la stessa PA connotata di persone fisiche distinguibili in un'ampia gamma, dai semplici funzionari di enti a livello micro ai politici e quindi considerando un livello macro.

La sovrapponibilità tra i due concetti di pubblicità e trasparenza rimane un punto fondamentale non ancora identificato, difatti l'una è considerata parte dell'altra, ovvero, la pubblicità è inglobata alla trasparenza nel senso che affinché venga soddisfatto il principio della trasparenza, una PA è obbligata per legge a pubblicare determinati documenti. Tale legame può quindi essere interpretato come un'endiadi, ovvero suscettibile di complementarità tra trasparenza e pubblicità nel senso che, mai come nei periodi recenti, quest'ultima abbia favorito la prima anche e soprattutto grazie all'avvento di internet. In altri termini in questo periodo storico viene sempre meno il concetto di segreto d'ufficio al quale si faceva riferimento con la legge n. 241 del 1990 (punto di maggior distinzione tra pubblicità e trasparenza) e per il quale le informazioni provenienti e relative alla PA fossero da ritenersi segrete e quindi da non essere condivisibili, tramite la loro pubblicazione, con il "mondo esterno". Quanto appena detto è stato poi rivisitato e "rigorosamente circoscritto ai soli casi in cui sia necessario, obiettivamente, tutelare particolari e delicati settori della pubblica amministrazione"[7].

Dopo aver distinto due termini tanto simili quanto concretamente distinguibili l'uno dall'altro, viene sempre più in evidenza che il vero punctum dolens, è un'analisi della trasparenza da un punto di vista più esterno. Quando si affronta questo delicato tema si fa riferimento inconsapevolmente ad una serie di diritti e di realtà da tenere in considerazione, che in qualche modo entrano in collisione con la trasparenza; uno su tutti è il diritto alla protezione dei dati personali. È

[7] Sanna, *Dalla trasparenza amministrativa ai dati aperti, opportunità e rischi delle autostrade informatiche*, Torino, 2018, p. 68.

dunque doveroso citare l'autore dello scritto "Privacy and freedom"[8] che sosteneva la seguente concezione "la dittatura è il sistema in cui l'individuo è completamente trasparente e l'azione dello Stato è coperta dalla massima riservatezza, mentre la democrazia è il sistema in cui l'azione dello Stato è ispirata al massimo livello di trasparenza e l'individuo è protetto dal massimo livello di privacy rispetto alle informazioni che lo riguardano"[9]. Viene automatico pensare che quindi il diritto menzionato poc'anzi ricopra un ruolo fondamentale nella gestione della trasparenza in quanto, se non trattato correttamente, potrebbe ledere la sfera privata degli individui interessati. Ora l'attenzione deve essere incentrata sul binomio trasparenza-privacy in modo tale da consentire l'uno mantenendo tutelato l'altro e viceversa. Quest'ultima affermazione deve essere evidenziata soprattutto in ottica del tanto citato quanto di recente attuazione diritto di accesso che verrà approfondito successivamente e sul quale verrà posta attenzione in questo capitolo: FOIA che offre uno strumento di nitidezza rispetto a quanto operato dalla pubblica amministrazione.

1.1 Evoluzione della trasparenza sul territorio italiano

Prima di procedere con l'analisi del c.d. FOIA, è utile ricordare brevemente come il tema della trasparenza sia stato affrontato in Italia negli ultimi anni.

Una prima prospettiva in favore di un'amministrazione più trasparente viene evidenziata dalla legge n. 241 del 1990 con l'introduzione dell'istituto dell'accesso documentale agli atti fornendo un primo declassamento del segreto amministrativo. Un particolare strumento che offre la possibilità a semplici individui di richiedere la visione di determinati documenti purché l'istante dimostri un interesse diretto, concreto e attuale (attributi che poi verranno modificati come si vedrà in seguito) e corrispondente ad una situazione

[8] A. F. Westin, professore alla Columbia university.

[9] Colapietro, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, Federalismi.it, 2020, 1-29.

giuridicamente tutelata[10]. Procedendo in ordine cronologico, vi è dapprima l'emanazione della c.d. riforma Brunetta con il d.lgs. n. 150/2009, la quale non ha apportato enormi cambiamenti, cosa invece successa qualche anno dopo, con il c.d. decreto trasparenza (d.lgs. 14 marzo n. 2013/33); è proprio con quest'ultimo che sono stati introdotti diversi obblighi inerenti la pubblicazione di diversi documenti da parte delle amministrazioni sui propri siti istituzionali. In tale ultimo decreto analizzato è possibile ritrovare i primi accenni dicotomici tra trasparenza e privacy concorrendo alla realizzazione di un'amministrazione aperta nella quale però si intravedono i primi limiti sulla sua operabilità in termini di protezione dei dati personali. L'ulteriore passo compiuto verso l'adozione del modello di matrice statunitense (FOIA) si avrà con il d.lgs. n. 97/2016 (Riforma Madia) con la quale venne introdotto il c.d. diritto di accesso civico generalizzato e con il quale cambiò la concezione di trasparenza, da quella riferita alla condivisione dell'attività delle PA nel loro complesso ad una in cui l'operato amministrativo veniva condiviso anche con la pubblicazione di singoli dati facenti parte della macrostruttura "Amministrazione", permettendo un controllo costante dell'attività da parte dei cittadini[11] ed evidenziando il passaggio dal c.d. e passato "Need to know" all'odierno "Right to know".

1.2 FOIA

Negli ultimi anni si è sviluppata sempre più l'idea che l'operato delle Pubbliche Amministrazioni potesse raggiungere un livello di trasparenza tale da cercare di rendere partecipe qualsiasi cittadino sulle decisioni intraprese dalle prime. Con il cosiddetto FOIA l'accesso ai documenti amministrativi è risultato lo strumento per antonomasia capace di condividere le informazioni in possesso delle PA con

[10] Musci, *L'accesso agli atti della Pa è legittimo se sussista un interesse diretto e non leda la privacy*, in Anci, Associazione Nazionale Comuni Italiani, 27 aprile 2022.

[11] Faini, *Trasparenza della Pa, tutto ciò che c'è da sapere sui nostri diritti, Dalla legge 241/1990 al d.lgs. 97/2016: come è cambiato il diritto a conoscere. Ecco il quadro completo fino al Foia, per orientarci in una normativa complessa,* in Agenda Digitale, 11 luglio 2016.

chiunque ne richiedesse l'utilizzo. Andando a ritroso con gli anni, il Freedom of Information Act venne emanato negli Stati Uniti d'America il 4 luglio del 1966 dall'allora presidente in carica, Lyndon Johnson, a seguito di un lungo iter parlamentare[12]. L'obiettivo di tutto ciò era realizzare un sistema capace di permettere un significativo controllo, da parte dei privati cittadini, sulla gestione del settore pubblico e quindi sulla sua accountability (termine che peraltro verrà riconsiderato successivamente in materia di GDPR). Tuttavia, l'introduzione del c.d. FOIA, che in Italia si concretizza in quello che viene chiamato accesso civico generalizzato, avviene solamente con l'emanazione del d.lgs. n. 97/2016 (c.d. decreto FOIA). La ratio del legislatore è stata quella di coinvolgere in maniera reattiva i cittadini; precedentemente si configurava una situazione proattiva in quanto trasparenza e pubblicità venivano in risalto con la pubblicazione obbligatoria di alcuni documenti all'interno dei diversi siti istituzionali tramite delle linee guide studiate e adottate dall'ANAC. Infatti, si è puntato all'evidenziazione del diritto alla trasparenza che ogni persona fisica possa avere quando decida di interfacciarsi con una Pubblica Amministrazione. Tale approccio favorisce inoltre la rilevazione di possibili atteggiamenti corruttivi da parte delle istituzioni pubbliche ma ciò riguarda un altro tipo di studio che non verrà analizzato in questo testo.

Tra le novità che il d.lgs. appena menzionato apporta al diritto amministrativo va considerata la possibilità di ricorrere al suddetto accesso generalizzato in mancanza di un interesse diretto e concreto che in qualche modo giustifichi la richiesta da parte del singolo cittadino (requisito, come si evidenzierà, basilare richiesto dal precedente diritto di accesso documentale) e peraltro costituisce un ulteriore strumento a cui possono ricorrere i singoli cittadini sulla possibilità di prendere visione di tutta una serie di documenti di natura amministrativa (ed in

[12] Andriani, *"Foia". Strumento di accessibilità totale alle informazioni*, in Il principio della trasparenza amministrativa tra nuove tecnologie e contrasto ai fenomeni corruttivi, Aracne, Roma, giugno 2020, p. 54.

capo alle PA) che non fossero presenti tra gli obblighi di pubblicazione emanati dall'ANAC. Il legislatore ha quindi voluto diminuire maggiormente la distanza presente tra istituzione e privato cittadino, rendendo partecipe l'uno nei confronti dell'altro; tuttavia, lo stesso legislatore, come del resto in altre realtà, predispone due diverse tipologie di eccezioni per il ricorso a tali istanze, le une assolute, le altre relative. Con le prime, si intendono per esempio le fattispecie coperte da segreto di stato, mentre nelle seconde vi rientrano i casi di sicurezza pubblica o comunque riguardanti l'ordine pubblico. In quest'ultimo caso, è necessaria una valutazione preventiva dell'amministrazione interpellata che dovrà verificare la presenza di un pregiudizio concreto nei confronti di un interesse pubblico o privato che sia. Di conseguenza l'istanza relativa all'accesso generalizzato può essere rigettata dalla stessa PA[13]. Proprio in merito all'istituto del rigetto, l'introduzione di tale tipologia di accesso può essere interpretata come una forma generosa di agevolazione (per così dire, dal momento che la legge non impone più alcun limite) inerentemente la richiesta di dati e documenti. Tuttavia, la realtà dei fatti offre una descrizione più complessa in quanto ogni PA dovrà essere in grado di soppesare discrezionalmente ogni richiesta pervenuta con le altre situazioni giuridiche meritevoli di tutela[14]. Conseguentemente a questa breve riflessione, il principio di trasparenza potrebbe perciò risultare tutelato, nei confronti dei cittadini, in una misura sicuramente inferiore dal momento che la quantità di rigetti (operati dalla PA) potrebbe essere relativamente ampia. Ecco quindi come, in realtà, tale tipologia di accesso, da un punto di vista prettamente legato al diritto alla privacy e alla tutela dei dati personali, risulti più limitante in termini di possibilità data al singolo cittadino di poter fare da "supervisore" rispetto all'operato delle PA (il

[13] Andriani, *"Foia". Strumento di accessibilità totale alle informazioni*, in Il principio della trasparenza amministrativa tra nuove tecnologie e contrasto ai fenomeni corruttivi, Aracne, Roma, giugno 2020, p. 60.
[14] Rossa, *Trasparenza e accesso all'epoca dell'amministrazione digitale*, in Il diritto dell'amministrazione pubblica digitale, Giappichelli Editore, Torino, 23 ottobre 2020, p. 265.

confronto appena menzionato si riferisce alle differenze, che man mano sono risultate, con l'accesso civico semplice in quanto quest'ultimo si rifà ai c.d. obblighi di pubblicazione voluti dal legislatore, come dichiarato da ANAC).

È evidente quindi come tale strumento, applicato dapprima negli Stati Uniti, presenti tuttora numerosi limiti nonostante, però, abbia consentito agli USA di favorire numerosi interventi su indagini riguardanti singoli organi della Pubblica Amministrazione. A proposito si può citare il caso della senatrice per lo Stato di New York nonché membro del Partito Democratico statunitense nei confronti della quale si indagò su una serie di mail inviate dal proprio account lavorativo per fatti personali. Un altro esempio riguarda "la costituzione di un indice di affidabilità dei medici per individuare, con estrema facilità, casi di malasanità all'interno del paese"[15]. Alla luce di ciò, il 4 luglio del 1966, è stata approvata una legge che da un lato offrisse, come già descritto, la possibilità di analizzare i documenti condivisi dalle PA. Importante sottolineare che, in Italia, l'interessamento coinvolge tutte le organizzazioni pubbliche, le autorità amministrative indipendenti e, come previsto di recente, sia da una parte gli Enti pubblici economici che dall'altra gli Ordini professionali e le Società in controllo pubblico (per le quali si fornirà un esempio nel secondo capitolo), come indicato nel Testo del Pubblico impiego. Differentemente, negli Stati Uniti, l'area degli organi interessati dal FOIA risulta essere minore in quanto tale diritto è esercitabile nei confronti delle agenzie federali ma non delle agenzie governative statali o locali; la richiesta di accesso ai documenti per i cittadini statunitensi risulta essere contrapposta ad un limite di tipo economico poiché è accompagnata dalla corresponsione di un importo fissato in base a determinati parametri[16] relativi a soggetti terzi. Interessante è poi sottolineare come anche nel

[15] Addante, *I limiti del FOIA, che c'è da imparare dagli Stati Uniti*, in Agenda Digitale, 20 settembre 2016.

[16] Parametri individuati, oltretutto, secondo le categorie lavorative che vi prestano il proprio contributo ai fini del rilascio di quanto richiesto dal privato, passando prima per la ricerca e

caso in cui si prospettasse un rigetto, il soggetto istante sarebbe comunque chiamato a corrispondere l'intera cifra per il tempo investito (dalla ricerca all'eventuale rilascio dei documenti) da impiegati, funzionari e dirigenti[17].

1.2.1 Segreto statistico

Con riferimento al trattamento dei dati (in particolare la loro gestione) e di tutto ciò che possa recare danno al diretto interessato, è necessario digredire su alcune questioni normative che assicurano una totale riservatezza riferita al dato personale. Particolare menzione va rivolta al segreto statistico, ovvero alla riservatezza sulle informazioni riguardanti le singole unità statistiche. Il problema si pone quando sia possibile, attraverso la lettura dei risultati riguardanti l'indagine, ricondurre un determinato dato ad una specifica persona[18]. Tutto ciò serve quindi ad assicurare che quanto suddetto non sia oltremodo fattibile.

1.3 Diritto di accesso vs tutela dei dati: punto di incontro?

Dopo aver introdotto uno dei principi cardine delle amministrazioni pubbliche quale è quello riferito alla trasparenza, in questo paragrafo si vuole esaminare il ruolo del diritto di accesso, da quello semplice (c.d. documentale) previsto nel 1990 a quello generalizzato riconosciuto a chiunque, in ottica di una sempre più spietata digitalizzazione in cui la mole di dati immessi in sistemi informatici ormai interoperabili necessiti di tutela da parte delle amministrazioni pubbliche. È infatti paradossale come l'uno agisca a discapito dell'altro per il semplice fatto che ormai tutti i documenti di spettanza amministrativa contengono al loro

ponendo successivamente l'attenzione sulla possibilità che il tutto possa incidere sulla sfera privata in termini di privacy e tutela personale.

[17] Si vuole porre l'attenzione sulle entrate economiche che gli Stati Uniti registrano grazie proprio all'implementazione di questo tipo di strumento. Il discorso non vale invece per l'Italia in quanto la fruizione di tale servizio è prettamente gratuita, per quanto concerne lo stato americano si denoti una più marcata designazione di quelle eccezioni che, peraltro, non consentano l'esercizio del c.d. Freedom of Information Act.

[18] Edizioni Simone, https://www.dizionari.simone.it/.

interno tutta una serie di dati, la cui divulgazione potrebbe ledere la sfera privata dei soggetti interessati. La normativa italiana in merito non è stata molto precisa in quanto viene data ampia discrezionalità ad ogni amministrazione sul fatto di poter limitare un diritto piuttosto dell'altro. In ogni caso, se un privato cittadino richiedesse l'accesso (per esempio, agli atti riferiti ad un concorso pubblico) sarebbe palese una fuoriuscita, anche se volontaria e in modo del tutto cosciente ad opera dell'amministrazione interrogata, di dati appartenenti ad altri soggetti (nelle vesti di controinteressati) e ai quali sia necessario darne avviso per tutelare il loro diritto alla riservatezza e alla protezione dei dati personali.

Tornando ad analizzare l'ordinamento italiano, è necessario porre qualche distinzione tra le varie tipologie di accesso (analizzando i casi in cui siano consentite deroghe, si parlerà dell'espressione "pari rango" presente nell'ordinamento italiano) e al possibile utilizzo che l'istante possa fare dei documenti richiesti. Infatti, mentre con quello generalizzato la persona fisica richiedente può astenersi dal fornire una motivazione potendo quindi utilizzare le informazioni richieste per qualsiasi scopo, nell'accesso documentale, previsto con la legge n. 241/1990, l'istante può sì riutilizzare le informazioni delle quali è venuto in possesso ma secondo lo scopo (motivazione) che ha comunicato all'amministrazione. Nel primo caso, il legislatore prevede che, essendovi poi, con i dati raccolti, la possibilità di riutilizzarli da parte dell'istante e quindi successivamente "divulgarne" le informazioni, la PA debba in qualche modo contemperare i diversi diritti in gioco che rientrano nelle problematiche e nei limiti alla trasparenza. Detto ciò, l'ordinamento italiano prevede "che il trattamento sia consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango (in seguito si coglierà meglio il significato di questo termine) almeno pari ai diritti

dell'interessato [...]"[19]. Vi è qui una prima distinzione tra le due tipologie di accesso, dal momento che, a differenza di quello documentale previsto originariamente in cui gli interessi tutelati da verificare erano solamente quelli inerenti ai settori e all'utilizzo che se ne sarebbe dovuto fare espressamente indicato nella motivazione per i quali l'istante ne richiedesse l'accesso, nel c.d. FOIA le PA sono obbligate ad una verifica a trecentosessanta gradi ed, in particolare, ad accertare che non vi siano condivisioni di "dati relativi alla salute o alla vita sessuale o all'orientamento sessuale" (quest'ultima dicitura è stata introdotta solamente con il d.lgs. n. 101/2018 quale decreto per il recepimento del GDPR in Italia, con il quale si è andati a modificare l'articolo 60 del Codice privacy che si menzionerà assieme al c.d. GDPR nel prossimo capitolo). Tornando al termine "rango", che è possibile ritrovare nell'ordinamento giuridico, questo gioca un ruolo fondamentale nell'azione dell'autorità amministrativa. Quest'ultima è chiamata a verificare che esista un diritto facente parte della sfera soggettiva del richiedente da tutelare e posto allo stesso livello del diritto alla riservatezza del o dei soggetti interessati (e coinvolti) in quei particolari documenti richiesti. Fornendo un banale quanto utile esempio, una richiesta di accesso di documenti nei siano presenti dei dati riferiti alla salute di un terzo soggetto, può essere accolta positivamente dall'autorità amministrativa nel caso in cui, con tale istanza, si volesse tutelare il diritto alla salute (considerato un diritto fondamentale) in capo all'istante stesso. Infatti, l'espressione "pari rango" soggiace ad una obbligatorietà di contemperare i due diritti opposti in deroga ad un limite (indicato dal legislatore) riferito al diritto di accesso stesso e che comunque, anche se trattasi di un diritto soggettivo importante (in capo all'istante), nel caso in cui venga posto al di sotto del diritto alla riservatezza, non potrà mai ultimare l'accesso in relazione a quel tipo di atti richiesti. Viene qui più

[19] Colapietro, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in federalismi.it, Roma, 13 maggio 2020, p. 76.

che mai in risalto come tale diritto alla protezione dei dati personali sia posto in una condizione di quasi predominanza su qualsiasi altro diritto, pure su un diritto che merita una protezione generalizzata come è quello di azione e di difesa (in caso l'istante debba difendersi in ambito giudiziario e richieda la visione e il possesso di determinati atti e/o documenti). L'azione di controllo a dir poco sensibile operata dall'autorità amministrativa, secondo il legislatore, può moderare il diritto di accesso stesso, cercando di appurare se effettivamente tutti i dati personali che saranno resi noti in ottemperanza alla richiesta per il rilascio dei documenti siano da ritenersi nella loro completezza necessari (fondamentale richiamare il rispetto ai principi di necessità, pertinenza e non eccedenza nel trattamento, come basi del Regolamento dell'Unione Europea 2016/679). In ossequio alla riservatezza dell'interessato al quali fanno riferimento i dati e come del resto ci si aspetterebbe nel caso ci fosse necessità di un rapporto con un soggetto terzo, tale interessato dovrà essere chiamato in causa per consentire un eventuale contraddittorio e di conseguenza la possibilità da parte di quest'ultimo di opporsi legittimamente. Da ultimo, com'è logico supporre, vanno menzionati, anche se molto brevemente perché non del tutto pertinenti con l'oggetto del testo, i limiti posti dal legislatore che restano tassativi e che riguardano dei casi specifici espressamente previsti dalla legge; è possibile citare il caso in cui i documenti siano coperti da segreto di Stato, oppure il summenzionato caso in cui "i documenti amministrativi contengano informazioni di carattere psico-attitudinale nonché riguardanti la vita privata […] con particolare riferimento agli interessi epistolare, sanitario, professionale, […]"[20].

Dopo aver solo accennato ai limiti previsti per l'accesso documentale, si viene ora ad analizzare quelli relativi all'accesso civico generalizzato, di matrice più complessa perché denotano la possibilità di condividere le informazioni richieste

[20] Colapietro, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in federalismi.it, Roma, 13 maggio 2020, p.78.

con un numero indeterminato di utenti per le quali è importante il ruolo dell'autorità amministrativa nell'azione di bilanciamento dei diversi diritti in gioco. Il tema è stato a dir poco dibattuto nel corso degli anni, infatti, non sempre è stata voluta e attuata una direttiva comune su un tema molto sensibile quale è la riservatezza delle persone fisiche. In primo luogo, è bene citare la Circolare n. 2/2017 del Dipartimento della Finanza pubblica che nel suo testo individua un "interesse conoscitivo" che debba avere attributi preferenziali rispetto ad altri diritti al cospetto di una "bilancia" in cui si debbano, soppesare i vari interessi in gioco. Secondo questa circolare, quindi, il diritto alla riservatezza giocherebbe un ruolo meno importante venendo quasi soppiantato dall'interesse dell'istante a voler e dover conoscere determinati documenti. Nella questione ha preso posizione il Garante per la protezione dei dati personali sostenendo che, in conformità al d.lgs. n. 33/2013, si sarebbe vanificata quell'esigenza, da parte dell'autorità amministrativa, di dover valutare e bilanciare i due diritti in gioco venendo meno quindi ad un decreto che, secondo anche quanto evidenziato (in modo del tutto critico) da recente dottrina[21], verrebbe ulteriormente pervaso da confusione a causa dell'introduzione della suddetta Circolare ministeriale. Tuttavia, vi è da aggiungere che le circolari ministeriali interpretative "sono prive di efficacia vincolante nei confronti degli organi periferici, i quali possono, infatti, disattenderne l'interpretazione senza che ciò comporti l'illegittimità dei loro atti per violazione di legge"[22].

Dopo aver trattato le particolarità riferite ai diversi accessi previsti dall'ordinamento italiano, torniamo all'analisi di quell'azione amministrativa, sensibile quanto doverosa in termini di legge e di linee guida, quale è la pubblicazione di atti e documenti che in qualche modo svelano l'operato delle

[21] D. U. Galetta.

[22] Colapietro, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in federalismi.it, Roma, 13 maggio 2020, p. 83.

singole amministrazioni. Quest'ultima, come recita il considerando 154 del Regolamento europeo (GDPR), ammette che le autorità pubbliche facenti parte degli stati membri siano obbligati (qualora richiesto da qualsiasi istante) a diffondere dati personali contenuti nei documenti in loro possesso (purché ritenuti di stampo pubblico e quindi da intendersi relativamente alla finalità per la quale viene effettuato il successivo trattamento; si tenga presente che, perciò, con tale dicitura, la fase valutativa, atta ad ottemperare al bilanciamento dei vari interessi di ogni autorità amministrativa, debba effettuarsi in chiave prospettica, analizzando ciò per cui i dati andranno ad essere utilizzati) solamente se richiesto dai propri regolamenti nazionali. Ragione per la quale, tornando al caso "Italia", il c.d. decreto trasparenza obblighi a contemperare il diritto all'accesso civico (in capo all'istante) con quello alla riservatezza (soggetto all'interessato dei dati che andranno poi ad essere trattati) e quindi, prevedendo, in altri termini, una conciliazione tra gli stessi. Lo stesso decreto n. 33/2013 include alcuni obblighi riferiti alla pubblicazione delle amministrazioni, tra i quali si possono citare quelli relativi alla pubblicazione di informazioni facenti capo a titolari di incarichi politici, di amministrazione, di governo nonché di titolari di incarichi dirigenziali. Proprio su questo punto, la Corte costituzionale si è espressa in favore di una maggior riservatezza nei confronti dei soggetti appena elencati perché, per l'appunto, giudicato inammissibile che ci fosse una deroga alla pubblicazione di dati personali anche se relativi a figure apicali. In ordine a ciò, il d. lgs. c.d. Mille proroghe del 2019 ha temporaneamente sospeso gli articoli 46 e 47 del decreto trasparenza in cui è espressa l'obbligatorietà, tra le altre, della pubblicazione della situazione patrimoniale dei vertici di un'amministrazione.

Da ultima, ma molto importante perché risulta essere il modus operandi della Pubblica Amministrazione e in relazione a quanto appena detto, è interessante il fatto che l'azione dell'autorità amministrativa, in accoglimento di un'istanza in cui il richiedente voglia ricevere dei documenti che sarebbero dovuti essere già

pubblicati nel relativo sito istituzionale, sia riservata solamente alla verifica che tale obbligo di pubblicazione sia effettivamente presente nelle Linee guida ANAC e quindi non alla ricerca di una siffatta violazione in termini di riservatezza dei dati dei soggetti inclusi in quei determinati documenti per il fatto che tale tipo di controllo sia stato effettuato a priori dal legislatore nella pubblicazione delle linee guida stesse. Tutto ciò per evitare un doppio controllo che rimarrebbe solamente superfluo e dispendioso in termini di risorse sia economiche che temporali. Si dà il caso che la normativa riguardante gli accessi civici (semplice e generalizzato), ad ora, risulti ancora piuttosto scarna in contrapposizione con quella relativa all'accesso documentale che, essendo stata disciplinata con maggior anticipo, risulta essere più completa.

1.3.1 Protezione dei dati personali nel resto d'Europa

Esaminata la situazione italiana, che, come si è potuto constatare, rimane molto deficitaria sul tema "protezione dei dati personali", si vuole fornire una breve disamina su ciò che avviene a livello degli altri paesi europei.

Com'è logico supporre, il Regolamento 679/2016 è stato introdotto per fornire una visione sempre più similare, all'interno della comunità, sulla tematica presa in considerazione. Tuttavia, tale visione rimarrà quasi utopica dal momento in cui ogni Stato membro continuerà a decidere da sé (si veda il caso dell'Italia, il cui l'ordinamento non tratta il diritto alla riservatezza in modo analogo a quello adottato a livello europeo). A livello europeo, dunque, il discorso si fa meno omogeneo perché, pur essendo data piena autonomia agli stati membri sulle modalità di bilanciamento e contemperamento tra diritti e interessati coinvolti, non sempre viene rispettata la libertà di accesso, in quanto si affronta tale problematica limitando l'accesso da parte di chiunque rispetto alla tutela dei dati

personali (eccezion fatta per l'accesso qualificato)[23] – come risulta dal caso della Francia.

Dapprima si è trattato il diritto di accesso con tutte le sue sfaccettature e menzionando il fatto che l'istante, nel richiedere dati e documenti, possa avere come obiettivo il riutilizzo di questi ultimi. Per menzionare il caso dell'Italia sarebbe utile analizzare la tematica riguardante la qualità del dato pubblico in sé e come le informazioni pubblicate nei vari siti istituzionali debbano essere sempre aggiornate e puntuali per agevolare la semplicità di consultazione e di conseguenza una maggior comprensibilità del dato. Tuttavia, ciò si discosta dal problema che persiste quando invece sia uno Stato estero a richiederne la fruibilità. È proprio di questa tematica che si parlerà nel prossimo paragrafo, introducendo fin da subito le motivazioni che spingono la Comunità europea a consentire il riutilizzo dei dati e a consentirne la condivisione tra i singoli paesi. A proposito di quest'ultima considerazione, l'argomento "condivisione" di dati verrà ripreso anche successivamente, quando si enucleerà la c.d. sentenza Schrems II. In particolar modo si evidenzierà come vi siano differenze normative (in termini di protezione dei dati personali) a livello continentale e come molte volte tale sensibile tematica sia posta in valutazione a discrezione degli enti pubblici o comunque dei singoli soggetti privati tentando, soprattutto, di liberarsi da ogni forma di responsabilità riguardante possibili eventi futuri (ovviamente in caso di lesione di soggetti terzi per la fuoriuscita illecita dei propri dati). In quest'ultimo caso si parla soprattutto di condivisione di dati all'esterno dei confini europei in quanto, come si esaminerà, il GDPR ne tutela l'utilizzo e più in particolare, il titolo V "individua un limite al trasferimento che è quello di non compromettere il livello di protezione delle persone fisiche garantito dallo

[23] D'Alterio, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, gennaio, in Giornale di diritto amministrativo, 2019, p. 21.

stesso Regolamento"[24]. È proprio su quanto appena detto che la Commissione europea ha deciso, come primo provvedimento, di adottare, insieme agli organi dello stesso rango ma con sede oltre oceano, un complesso di principi emanati all'interno del c.d. Privacy Shield il 7 luglio del 2016, successivamente all'adozione del GDPR, che in qualche modo trattasse tutte quelle vicende in cui venivano coinvolti dati personali, di provenienza europea, nell'operato di organizzazioni aventi sedi negli Stati Uniti. Nonostante le relazioni extra-europee siano di grande rilevanza oggigiorno, è pur vero che necessitino vivamente di un approfondimento "a parte" e che quindi, ora, si vuole tornare al focus principale, ovvero ponendosi un quesito ormai logico: come è stato studiato il c.d. riutilizzo dei dati pubblici tra i diversi Stati membri dell'UE? Ebbene, tale tematica è stata analizzata dalla Corte di giustizia europea (CGUE) la quale ha superato ulteriormente, nel 2020, il summenzionato Privacy Shield in quanto considerato anch'esso non completamente conforme rispetto alla normativa del GDPR. Infatti, ciò che la CGUE decise in merito fu proprio un doppio coinvolgimento di soggetto esportatore dei dati e soggetto destinatario in quanto entrambi hanno l'obbligo di verificare che il livello di protezione delle persone fisiche garantito da tale regolamento (GDPR) non venga in nessun modo compromesso. In tal modo, anche in questa occasione, si è fatto affidamento ad una valutazione, a priori, e quindi con un sistema basato sulla discrezionalità affidata ai diversi soggetti trattanti i dati personali.

1.3.2 Riutilizzo dei dati pubblici

Nel territorio europeo, fin da subito, si è assistito a finalizzare l'interazione tra gli Stati attraverso un sempre più concreto ricorso alla condivisione dei dati pubblici in modo da creare quello che viene chiamato "mercato europeo digitale". Già nel 2003 il legislatore europeo optò per regolamentarne il riutilizzo attraverso

[24] Bolognini, *Il superamento del Privacy Shield e la (libera?) circolazione commerciale dei dati fuori dalla UE*, in Privacy e libero mercato digitale, Giuffrè Francis Lefebvre, Milano, 2021, p. 90.

l'introduzione di una direttiva comunitaria (2003/98/CE) che in qualche modo riuscisse ad azzerare le differenze a livello di ordinamento degli stati europei. Tuttavia, come evidenziato dal d.lgs. 24 gennaio del 2006 con il quale l'Italia attuava giuridicamente la direttiva suddetta, la problematica sull'effettiva ammissione del riutilizzo dei dati pubblici non fu risolta nel senso che in quest'ultima, al comma 2 dell'articolo 1, si dichiarava che "le pubbliche amministrazioni e gli organismi di diritto pubblico non hanno l'obbligo di consentire il riutilizzo dei documenti e, in particolare, che la decisione di consentire o meno tale riutilizzo spetta all'amministrazione"[25]. In ordine allo sviluppo di un mercato unico di dati e per ottemperare allo sfruttamento del potenziale delle ICT (una delle misure dell'Agenda digitale europea adottata nel maggio 2010 nel quadro della strategia Europa 2020) nel 2013 (Direttiva 2013/37/UE) la questione "riutilizzo dei dati" ha subito una modifica con la quale si è voluto che lo stesso fosse adottato all'interno della Comunità. In tutto ciò, però, la direttiva stessa, ancora una volta, poneva dei vincoli e in un certo senso è parso chiaro come il legislatore europeo volesse salvaguardare gli ordinamenti interni di ogni paese membro: come recita l'articolo 1, lett. c), con il quale vengono sottratti all'attività di riutilizzo tutti quei documenti che, in base alla normativa interna sul diritto di accesso, siano esclusi a priori. Viene quindi meno, come si può supporre e come già avvenuto nel 2013, la possibilità di creare un mercato unico di condivisione di dati e documenti basato sul riutilizzo di questi ultimi. È da chiedersi come, in base a tali vincoli, possa operarsi la ricerca di un indirizzo comune che possa gestire la grande mole di dati che sempre più investirà i paesi europei grazie al progressivo sviluppo delle tecnologie digitali. Infatti, per citare un esempio, (anche se trattasi del settore privato) il colosso Amazon ha dimostrato che proprio grazie all'utilizzo di algoritmi capaci di apprendere i bisogni delle persone attraverso l'immagazzinamento di una serie

[25] Sanna, *La nuova direttiva comunitaria 2013/37/UE sul riutilizzo: il riutilizzo diventa vincolante per gli Stati membri*, in Dalla trasparenza amministrativa ai dati aperti, Torino, 2018, p.256.

di dati riguardanti spesso la vita privata di queste ultime in termini di preferenze, sia riuscito ad avere il successo che ha tutt'ora perché appunto capace di ridurre la distanza virtuale tra venditore e cliente proprio attraverso gli algoritmi sopracitati. Il legislatore europeo ha dimostrato e sta dimostrando che l'obiettivo prefissato sia proprio quello esplicato con l'esempio riguardante la suddetta azienda di commercio elettronico statunitense. Il punto che continuerà a costituire un problema o comunque un ostacolo a tutto ciò, è rappresentato proprio dall'impossibilità (per ora) di conciliare il riutilizzo dei dati con il diritto alla riservatezza e quindi alla tutela di questi ultimi. Dopo l'emanazione della Direttiva europea del 2013, l'Italia si conformerà all'aggiornamento sul tema riutilizzo solamente il 18 maggio 2015 con il d.lgs. n. 102.

Alla luce di ciò, rimane chiaro come la condivisione dei dati pubblici sia ancora in fase migliorativa in quanto non esiste tutt'ora una direttiva, intesa come indirizzo comune, adottata dai paesi della Comunità europea che ne stimoli l'applicazione. A condizionarne l'utilizzo rimane infatti il tema della riservatezza che, soprattutto in Italia, gioca un ruolo molto importante e non facilmente conciliabile con ciò che concerne il riutilizzo degli stessi dati.

È bene ricordare come la giurisprudenza comunitaria sia conscia del fatto che, come verrà dedotto nelle conclusioni, "offuscare" sempre più il diritto alla riservatezza a discapito di una maggior fruibilità delle informazioni potrebbe essere controproducente e in merito, per esempio, la normativa italiana si è espressa tempestivamente. È questo il caso del decreto legislativo 25 maggio 2016, n.97, che abrogò l'articolo 4 del precedente d.lgs. 33 del 2013 in quanto quest'ultimo "ammetteva che la diffusione e il riutilizzo dei dati personali potessero seguire il canale non istituzionale del sito Internet dell'ente; e - di conseguenza affermando che - il loro trattamento potesse avvenire secondo modalità che ne consentissero la indicizzazione e la rintracciabilità tramite i

motori di ricerca web"[26]. Con ciò, il legislatore italiano ha voluto porre un freno al progressivo avanzamento del carattere democratico che la trasparenza (a livello europeo) stava osservando.

1.3.3 Preoccupazioni comunitarie in merito al riutilizzo delle informazioni pubbliche

È chiaro come, a livello interno, in Italia (previa consultazione del Garante per la privacy) si stia optando per mantenere un certo grado di tradizionalità nel riutilizzo come nel diritto di accesso in quanto, appunto, in ottica progressista permangono alcuni limiti che è necessario non porre in secondo piano.

A livello di macrosistema, la Comunità europea sta cercando di favorire l'utilizzo dei c.d. open data (i quali verranno approfonditi brevemente in un secondo momento) sfavorendo così il tanto acclamato diritto alla riservatezza in virtù di generare uno scambio di informazioni tra più realtà europee che soddisfi il concetto di "trasparenza europea". La mole di dati che sempre più verrà generata dalle operazioni della pubblica amministrazione (e non solo) nel prossimo futuro, sarà talmente ampia che il tentativo di proteggere i dati personali dei singoli individui potrebbe venire, inconsapevolmente, meno. Già oggi, il legislatore europeo afferma come lo scambio di informazioni con il fine di rendere trasparente l'operato pubblico statale sia possibile in diverse occasioni cercando di anonimizzare i dati personali rientranti nelle stesse. Infatti, lo stesso diritto alla riservatezza, per il suo esercizio, necessita del fatto che i dati rientranti e utilizzati in qualsiasi informazione debbano non essere (in qualche modo) riconducibili all'interessato stesso e quindi sostanzialmente resi del tutto anonimi. Il problema, secondo alcuni, non sussisterebbe dal momento che la quantità di dati personali presenti nei vari documenti in ottica di salvaguardare

[26] Sanna, *La nuova direttiva comunitaria 2013/37/UE sul riutilizzo: il riutilizzo diventa vincolante per gli Stati membri*, in Dalla trasparenza amministrativa ai dati aperti, Torino, 2018, p. 272.

il principio della trasparenza, non risulti rilevante e quindi, come anticipato poc'anzi, facilmente trascurabile mascherandone gli stessi.

Tornando all'incremento dei dati dei quali verrà in possesso (sempre più) la Pubblica Amministrazione, potrebbero sorgere non solo problemi di insostenibilità del diritto in relazione alla protezione dei dati personali come già evidenziato, bensì pure una sorta di offuscamento delle vere informazioni. Potrebbe dunque generare delle insolite difformità atte ad "alimentare un generico sospetto nei confronti dell'amministrazione stessa, anziché favorire la buona amministrazione"[27].

1.3.3.1 Big data & Open data

Parentesi doverosa è da aprire sul tema riguardante il fenomeno che tanto sta dilagando nell'era moderna e che interesserà sempre più il settore pubblico, considerando l'ampiezza in termini di volume e varietà che ne obbligano la gestione attraverso l'utilizzo di nuove tecnologie[28]. Si parla in questo caso dei c.d. big data, menzionati nell'introduzione, che comprendono tutti quei dati, sotto forma digitale, i quali, secondo uno studio condotto nel 2011[29], pure a seguito dell'archiviazione, raddoppiavano ogni tre anni. Quanto appena affermato mette in luce la necessità di provvedere all'implementazione di limiti nel loro utilizzo per assicurare la, svariate volte menzionata, tutela della privacy. Per fornire un esempio molto banale, i semplici messaggi di testo che vengono inviati attraverso un'applicazione di messaggistica (sia essa installata su qualsiasi device) piuttosto che i dati personali richiesti e immessi in un qualsiasi form online (da considerarsi i cosiddetti campi vuoti inizializzati nei siti web con il solo scopo di

[27] Bombardelli, *Fra sospetto e partecipazione: la duplice declinazione del principio di trasparenza*, in Istituzioni del Federalismo, rivista di studi giuridici e politici, pp. 670-671.
[28] *Big data e open data: definizione, differenze e figure professionali che se ne occupano*, in Communication Village, 19 marzo 2020.
[29] Studio condotto da M. Hilbert (Università del Sud della California, Los Angeles) e P. Lopez (Università della Catalonia, Barcelona) e pubblicato nel loro testo "The world's technological capacity to store", 10 febbraio 2011.

essere completati dall'utente, per esempio, nella richiesta di un servizio sia pubblico, come su un portale di un ente pubblico che privato, per l'iscrizione su un social media) sono ricompresi nella macrocategoria appena illustrata. Prima di proseguire, però, è necessario enunciare il significato di un'altra categoria di dati che è possibile denominare come conseguenza di quanto appena scritto. Si tratta dei c.d. Open data, che richiamano ai concetti illustrati nei paragrafi precedenti in tema di trasparenza e riuso. Infatti, è possibile delinearli come quella categoria soggetta ad una condivisione, più o meno ampia, di informazioni riferite a qualsiasi soggetto fisico o giuridico che sia. In questa breve disamina, verranno considerati quelli riferiti al settore pubblico.

L'espressione "big data" si rifà quindi all'esigenza di esporre taluni dati piuttosto che altri alla completa visione del pubblico in modo tale da ricavarne una maggior trasparenza e di conseguenza una maggior efficienza, in termini di controllo da parte dei cittadini, sull'operato della PA. Si parla quindi di una locuzione tramite cui si vuole intendere una fetta mirata, o meglio, una sub-categoria rientrante nell'insieme composto da tutti i dati. Detto ciò, è necessario ribadire come gli open data rappresentino quella tipologia di dati presa in causa nei primi paragrafi, ovvero una categoria capace di abbracciare in un continuum non perfettamente sovrapponibile, tanto i profili della trasparenza amministrativa (con tutte le tipologie di accesso, maggiormente riferito a quello civico piuttosto che al documentale), quanto quelli legati al riuso creativo[30] dei dati.

[30] Con il termine "creativo" si vuole enfatizzare il fatto che tali dati possano essere utilizzati in un secondo momento sia per fini economici che non, ma questa distinzione necessiterebbe di un ulteriore approfondimento. In questo capitolo sono stati considerati i secondi.

Capitolo 2 GDPR

Il 25 maggio del 2018 rappresenta una data importante per quanto concerne una delle tematiche più sensibili del ventunesimo secolo. Nell'era della digitalizzazione, con l'avvento di Internet e delle innovazioni tecnologiche, protezione e il relativo trattamento dei dati personali (riferiti a persone fisiche), nonché la loro libera circolazione, sono divenuti oltremisura rilevanti in un sistema fortemente basato sulla condivisione di informazioni alla base di sistemi interscambiabili e interoperabili. Si pensi a tutti quei casi in cui ogni persona fisica sia chiamata a inserire propri dati all'interno di moduli per la sottoscrizione di un qualsiasi tipo di contratto: in questi casi si rende necessaria una specifica tutela che garantisca all'interessato il pieno utilizzo delle suddette informazioni unicamente all'oggetto del contratto e non per ulteriori fini (casistica rientrante nel cosiddetto Data Breach).

Tornando al tema dell'evoluzione tecnologica, la diffusione del c.d. Internet of Thing (IoT) ha contribuito a rendere necessaria la regolamentazione della diffusione di dati che influisce e accompagna la vita quotidiana di qualsiasi individuo. Con IoT si indica il complesso degli "oggetti" in connessione tra loro, relativamente, per esempio, a smart building, smart environment ma soprattutto smart city che si svilupperà in un secondo momento (relativamente al Comune di Venezia).

Nasce così l'esigenza da parte dell'Unione Europea di adottare un regolamento unico e condiviso tra gli stati membri capace di garantire la libera circolazione dei dati personali nel rispetto di una serie di regole. Il GDPR, acronimo inglese di General Data Protection Regulation, si applica a società, imprese, professionisti, studi professionali che svolgono un'attività di raccolta e trattamento di dati personali che abbiano sede in Italia o in qualsiasi altro paese dell'Unione Europea; sia al trattamento automatizzato dei dati personali che a

quello non automatizzato di dati contenuti in archivi o destinati a figurarvi[31]. Per comprenderne meglio l'importanza, si procederà con una breve disquisizione circa l'origine della Privacy a livello internazionale e i suoi sviluppi storici.

2.1 Privacy, evoluzione della normativa europea e cenni in Italia

Il tema della privacy è stato riconosciuto come primo strumento internazionale giuridicamente vincolante in una prima fase con la Convenzione per la protezione delle persone rispetto al trattamento automatizzato dei dati personali nel 1981[32]. Nello specifico, la suddetta Convenzione ha rappresentato un ruolo fondamentale per gli sviluppi in ambito europeo, gran parte delle disposizioni sono infatti state trasfuse nella Direttiva 95/46/CE (punto iniziale in materia): la Comunità europea decise di contemperare la tutela dei dati personali con la loro libera circolazione tra gli Stati membri, quest'ultima propedeutica per il buon funzionamento del mercato[33]. Strumento concepito e voluto in modo tale da regolarizzare quella branca di attività prettamente economiche.

Un secondo "pilastro", meno rilevante in termini di grandezza, fu introdotto con il Regolamento 45/2001/CE il quale introdusse l'obbligo, da parte delle istituzioni europee, di nominare un "incaricato della protezione dei dati" c.d. privacy officer (figura che verrà poi prevista nelle organizzazioni pubbliche e in tutte quelle attività per le quali sia necessario il trattamento di dati pubblici). Con tale novità si decise di fornire garanzia per la protezione dei dati relativamente alle attività delle istituzioni europee. In concreto venne istituita una nuova autorità, la "European Data Protection Supervisor" (EDPS). Facendo qualche passo indietro sulla linea temporale, è possibile risalire al cosiddetto "Right to let be alone" scritto dai due giuristi Samuel Warren e Louis Brandeis nel dicembre del 1890. Si trattava per l'appunto della revisione di un articolo di legge che trattava il diritto

[31] La Pubblica Amministrazione digitale, in https://www.lapadigitale.it/.
[32] Prineos, *Breve storia della Privacy*, 28 gennaio 2022, https://prineos.com/.
[33] Pizzetti, *Approfondimenti informativi*, in Sette anni di protezione dati in Italia, Giappichelli Editore, Torino, 2012, p. 193.

dei singoli alla riservatezza e tradotto nella tutela di tutte quelle informazioni in cui terzi estranei non avessero un particolare interesse motivato. Una particolarità riguardante il suddetto diritto era che fosse a contenuto negativo, ovvero quello di ottemperare alla riservatezza di alcune informazioni considerate specifiche della sfera personale, piuttosto che a contenuto positivo, nel senso di eseguire un controllo sulle medesime[34]. Successivamente, con l'avvento di Internet nell'era digitale, la tutela suddetta diveniva sempre più stringente, diversificando l'accesso a determinati dati ritenuti pubblici da quelli considerati di dominio privato e quindi riguardanti la mera sfera personale. Più nello specifico, l'Autorità per le garanzie nelle comunicazioni in Italia riporta che coloro che operano nel web possono risalire ai dati personali di tutti i fruitori dei loro servizi attraverso l'utilizzo degli strumenti a loro disposizione. Per esempio l'azienda statunitense fornitrice di servizi online Google può ottenere informazioni riguardanti i propri utenti semplicemente dalle ricerche eseguite all'interno dei propri browser (per esempio Google Chrome) piuttosto che dalla propria posta elettronica (Gmail). In questa fase storica, altro importante pilastro è rappresentato dalla Direttiva 2002/58/CE con la quale si è disposto in materia di telecomunicazioni e di trattamento dei dati, con riguardo alla sfera privata, digitalmente parlando. Più precisamente, la suddetta Direttiva operò in materia di memorizzazione di, o accesso a, informazioni contenute nei dispositivi elettronici dei vari utenti e/o fruitori di servizi online (per esempio, ai fini di marketing e attraverso i c.d. cookies, è stata introdotta la necessità di un consenso in via preventiva che informasse l'utente sulla profilazione della loro navigazione). Più recente risulta essere l'ufficializzazione della Direttiva 2006/24/CE che, riguardante "la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al

[34] Carlino, *L'origine della privacy e l'esigenza di tutelare i dati personali*, in Ius in itinere, 13 luglio 2020, https://www.iusinitinere.it/.

pubblico o di reti pubbliche di comunicazione"[35], ha interessato, nel quadro della lotta ai reati di terrorismo informatico, un innalzamento del livello di conservazione e trattamento dei dati riguardante il settore delle comunicazioni elettroniche (modificando quindi la precedente e appena menzionata Direttiva del 2002). Quest'ultimo pilastro esaminato è possibile ritrovarlo nei piani anticorruzione che ogni amministrazione è obbligata a predisporre, ma ciò rappresenta oggetto di un altro importante quanto complesso studio sull'attività amministrativa delle PA. In ultima, un ruolo chiave nella realizzazione di un unico quadro giuridico è stato ricoperto dal Trattato di Lisbona con il quale, da una parte si istituisce la Comunità europea regolarizzandone numerose tematiche (tra cui il trattamento dei dati personali) e, dall'altra, si cerca di normalizzare tutte le normative sopracitate puntando sempre più all'interoperabilità tra i diversi Stati membri. In ambito nazionale, invece, il percorso per uniformare Direttive e Regolamenti europei è iniziato con leggero ritardo. Dapprima con un provvedimento rilevante in materia di privacy che fu emanato in Italia con la pubblicazione del Codice privacy nel decreto legislativo n°196 del 30 giugno 2003. Detto testo, attinente alla tutela dei dati personali, verrà poi surclassato dal regolamento europeo cosiddetto GDPR (Regolamento generale sulla protezione dei dati) nel 2016 al quale tutti gli stati membri si conformeranno nel giro di due anni, pena sanzioni che potrebbero prevedere multe fino a 20 milioni di euro. L'Italia vi si adeguerà con la pubblicazione in Gazzetta ufficiale il 4 settembre del 2018 e successivamente in vigore dal 19 settembre[36].

[35] Privacy.it, *Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006*, in Privacy.it, https://www.privacy.it/.

[36] Coppola, *Il nuovo codice della privacy*, in La legge per tutti, 24 ottobre 2018, https://www.laleggepertutti.it/.

2.1.1 Codice privacy 30 giugno 2003

Entrato in vigore il 1° gennaio del 2004, il codice privacy rappresenta il Testo unico in grado di riordinare e normalizzare tutti i comportamenti in materia di trattamento dei dati personali. Nonostante sia stato spesso aggiornato anche grazie al mutamento tecnologico e informatico (come del resto qualsiasi legge esistente), tale codice rimane ad oggi l'intervento, in chiave nazionale, più rilevante e corposo di adeguamento alle norme europee in ambito privacy. In esso sono state assorbite le norme disposte nella Direttiva 95/46.

Più nello specifico, esso ha previsto la costituzione di un'autorità che possa fare da garante per la protezione dei dati personali, in ordine ad uno degli ultimi interventi di modifica quale è stato quello finalizzato al rendere conforme la normativa italiana rispetto al GDPR (europeo). Il nuovo comma 1 dell'articolo 153, identifica il Garante nell'affiancamento tra Collegio, che ne costituisce il vertice, e Ufficio, rendendolo meno indipendente di quanto lo fosse precedentemente all'emanazione del suddetto Regolamento europeo. Il nuovo testo ne disciplina anche le modalità di selezione in modo tale da garantirne trasversalmente maggiore trasparenza in quanto i componenti "devono essere eletti tra coloro che presentano la propria candidatura nell'ambito di una procedura di selezione il cui avviso deve essere pubblicato nei siti internet della Camera, del Senato e del Garante almeno sessanta giorni prima della nomina"[37].

Tuttavia, due novità rilevanti, inserite dalla riforma oggetto di questo scritto, si riconoscono da una parte nell'introduzione di vincoli supplementari adibiti ai componenti il Collegio, ovvero di "mantenere il segreto, sia durante sia successivamente alla cessazione dell'incarico, in merito alle informazioni riservate cui hanno avuto accesso nell'esercizio dei propri compiti o nell'esercizio

[37] Zuddas, *L'Autorità di controllo: il "nuovo" Garante per la protezione dei dati personali*, in Il "nuovo" codice in materia di protezione dei dati personali, a cura di Scagliarini S., Giappichelli editore, Torino, luglio 2019, p. 264.

dei propri poteri" (art. 153, comma 4, Codice della privacy) e dall'altra, regola valida anche per tutti i dipendenti, di esimersi dal trattare "per i due anni successivi alla cessazione dell'incarico [...], procedimenti dinanzi al Garante [...]" (comma 8).

Per quanto concerne accertamenti e controlli operati dall'organo garante, si fa riferimento a determinate figure che si analizzeranno successivamente (titolare e responsabile del trattamento dei dati) e viene introdotta, oltre a queste, quella del c.d. rappresentante del titolare o del responsabile a cui il Garante può richiedere di fornirgli informazioni. La nomina di tale ultima figura viene prevista obbligatoriamente nel caso in cui si trattassero dati personali di interessati che si trovano nell'Unione europea in modo continuativo[38].

2.2 Principi fondamentali

Volendo esaminare nel dettaglio la normativa GDPR, è necessario enucleare quelli che possono essere considerati, come da titolo del paragrafo, principi fondamentali in materia di trattamento dei dati personali. Tali presupposti sono enunciati dal legislatore comunitario nel capo II del Regolamento (artt. 5-11)[39].

La nuova normativa tratta ulteriori linee guida, rispetto al passato, dalle quali è possibile evincerne i principi più rilevanti elencati di seguito e che si possono riscontrare maggiormente nel terzo capo (artt. 12-23) del GDPR:

- La *liceità* del trattamento;
- La *trasparenza* del trattamento;
- Il c.d. diritto all'*oblio*;
- L'*accountability* del titolare del trattamento;
- La c.d. *privacy by design* e *by default*.

[38] *Chi è il Rappresentante del titolare e quando va nominato*, in Lexdo.it, https://www.lexdo.it/.
[39] Guastalla, *Privacy e data protection: principi generali,* in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 66.

Prima di passare ad un'analisi più approfondita è importante sottolineare che le suddette nozioni sono tutte riferite e applicabili al trattamento dei dati personali. È rimarchevole, quindi, disaminare di seguito il concetto posto alla base del GDPR, ovvero quello del dato personale.

2.2.1 Dato personale

L'articolo 4, paragrafo 1 del GDPR definisce dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad 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". Detto ciò, è normale che, con l'enorme quantità di dati presenti digitalmente che fa parte di ogni individuo fin dalla nascita, la suddetta macrocategoria può essere suddivisa in tre sottocategorie:

- Dati **genetici** (art. 4, n°13 GDPR) → relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica;
- Dati **biometrici** (art. 4, n°14 GDPR) → ottenuti da un trattamento specifico come l'immagine facciale o i dati dattiloscopici;
- Dati **relativi alla salute**: (art. 4, n°15 GDPR) → attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, per esempio riguardanti disabilità, anamnesi medica, trattamenti clinici, ecc.

Le tre tipologie sono considerate dati particolari per i quali debba essere richiesto il consenso da parte dell'interessato in caso di trattamento. Tale categoria di dati è ricompresa, insieme ai dati comuni (per esempio dati anagrafici, coordinate

bancarie, recapiti, istruzione e competenze, ecc.) e a quelli giudiziari (riferiti a condanne) nella checklist a cui si farà riferimento in un secondo momento.

2.2.1.1 Data Breach

Dopo aver analizzato la definizione di dato personale in tutte le sue sfaccettature, è necessario procedere con lo studio del cosiddetto data breach; un argomento di estrema importanza nel mondo digitale ovvero della violazione di tutti quei dati immessi da un soggetto, fisico o giuridico che sia, sul web. In particolare, si intendono tutte quelle azioni non autorizzate, dal titolare o da soggetto indicato al trattamento dei dati, di copiatura, trasmissione o semplicemente rubando questi ultimi. La divulgazione di informazioni riservate o confidenziali relative, nel caso specifico, sia ad una qualsiasi azienda privata che ad enti pubblici, può arrecare danno a livello concorrenziale alle imprese oltreché direttamente all'utente. Di norma si evidenziano quattro casi di diffusione, sia essa illecita o semplicemente involontaria[40]:

- Perdita accidentale, riferito di norma a smarrimento di chiavette contenti dati sensibili oppure relativamente a distruzione in seguito ad incidenti o eventi avversi;
- Furto, per esempio di laptop o altri dispositivi informatici;
- Infedeltà aziendale, nel caso di divulgazione da parte di un dipendente non autorizzato;
- Accesso abusivo ogni qualvolta si verifichi un attacco esterno (elusivo dei software di protezione) ai sistemi informatici aziendali per esempio tramite malware.

Qualsiasi sia la natura di una trasmissione non autorizzata, può ledere (a volte anche in maniera compromettente) l'operato di un'azienda. Per citare un

[40] Redazione avvocato360, *Data breach: cosa significa e quali sono i rimedi?*, in Avvocato360, Torino, 2019, https://avvocato360.it/.

esempio, si ricorda l'accadimento del 30 luglio 2021 nel quale la Regione Lazio subì un attacco ransomware (ovvero un software malevolo, realizzato per la richiesta di un riscatto, in grado di cifrare tutti i dati presenti nella disponibilità della vittima attraverso anche l'involontaria complicità di quest'ultima) con la conseguente inutilizzabilità dei propri sistemi informatici, in particolare quello sanitario (settore più vulnerabile perché strutturalmente impreparata e obsoleta a livello tecnologico e culturalmente più arretrato: un gioielliere, per esempio, si aspetta di essere derubato a differenza di chi opera in ambito sanitario[41]) e quello dedicato alla vaccinazione contro il COVID-19. In questo caso, secondo le indagini si trattò probabilmente di un furto di credenziali relative ad un dipendente di Frosinone. I danni subiti sono stati ingenti; dalla sopravvenuta impossibilità di accesso ai registri dei dati delle farmacie al crash del database riguardante vaccinazioni e rilascio dei green pass[42]. Proprio per questo motivo si rende sempre più necessaria l'implementazione di un sistema di cybersicurezza pubblica più robusto. In particolare, ogni azienda deve ottemperare a redigere un piano di gestione inclusivo di tutte quelle misure atte a prevenire quanto detto finora adottando quindi un'ottica proattiva nei confronti di questa materia.

In ordine a ciò la legge prevede che, per ogni impresa privata, venga predisposto un modello di organizzazione, gestione e controllo che preveda, tra le varie tematiche, una sezione riguardante i delitti informatici e il trattamento illecito dei dati in conformità alla normativa vigente (D. Lgs. 231/2001 che è composto da una serie di procedure che servono a proteggere le società da accuse penali) che enuclei le tipologie di reati ipotizzabili e indichi le misure preventive atte a scongiurare diffusioni non autorizzate di dati di cui è in possesso l'azienda stessa. In ordine all'aggiornamento, tale modello dovrà essere modificato soltanto

[41] Giustozzi, *Cosa devono fare le PA per contrastare gli attacchi ransomware?,* Podcast di Ernesto Belisario, 2021, https://www.spreaker.com/.
[42] Panda Security, *Attacco hacker alla Regione Lazio: cosa sappiamo e cosa ci insegna*, in Panda mediacenter, 23 settembre 2021, https://pandasecurity.com.

successivamente a mutamenti normativi oppure qualora siano intervenute violazioni dello stesso o scostamenti dalle sue previsioni che ne abbiano reso inefficiente la prevenzione dei reati menzionati dal suddetto Decreto[43].

Ma come poter prevenire concretamente tutto ciò? È sicuramente necessario essere preparati attraverso la predisposizione di piani utilizzando strumenti tradizionali quali carta e penna (prendendo in considerazione la possibilità di un eventuale crash o terminazione improvvisa dei sistemi informatici), oltre che dover comunicare questi tipi di attacchi e minacce a soggetti esterni quali garante della privacy e polizia postale. Un passaggio fondamentale risulta essere l'attivazione di backup interni di dati, permettendo alle pubbliche amministrazioni di non essere suscettibili ad eventuale totale cancellazione dei dati (azione tuttavia consigliata e prevista nel contratto di servizio tra Comune di Venezia e Venis S.p.A.). In ordine a tutto ciò l'Agid (Agenzia per l'Italia Digitale) ha emanato nell'aprile del 2017 le misure minime di sicurezza per le PA (trattasi di checklist).

2.2.2 Liceità del trattamento

Il primo principio analizzato è rappresentato dalla liceità del trattamento, che si può, di conseguenza, suddividere in due requisiti alternativi e propedeutici (individuati singolarmente) quali sono la necessità dello stesso e il consenso dell'interessato. Per quanto attiene al primo, i casi sono individuati dall'articolo 6 GDPR, per esempio, "necessario all'esecuzione di un contratto di cui l'interessato è parte" – oppure - "necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento". Il secondo requisito è riferito al momento in cui, per esempio, prima di stipulare un contratto, venga chiesta l'esplicita autorizzazione tramite apposizione di firma autografa piuttosto che attraverso mezzi elettronici, oppure oralmente ed è individuato nell'art. 4 GDPR

[43] Venis S.p.A., *Modello di Organizzazione, Gestione e Controllo*, in Società trasparente, https://www.venis.it/files/redazione/Trasparenza/.

in "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso a che i dati personali che lo riguardano siano oggetto di trattamento"[44]. In questi casi, ogni forma di inattività e di silenzio non dovrebbe rappresentare consenso.

2.2.3 Trasparenza del trattamento

Il secondo principio viene individuato nella previsione che le informazioni con destinatario il/i soggetto/i interessato/i debbano essere di semplice accesso e comprensione; esso è indicato dagli articoli 12 e ss. del GDPR che riguardano la relazione tra titolare del trattamento e interessato. È infatti necessario che chiunque sottoscriva un contratto sia informato sul fine per cui i propri dati vengano richiesti e sull'utilizzo che il soggetto gestore debba farne.

Superfluo risulta analizzare gli studi empirici riguardanti il rapporto tra consenso esplicito e scelta consapevole. La maggior parte degli individui tralascia spesso l'informativa senza quasi mai prenderne visione e comprendere che ruolo avranno e soprattutto come verranno trattati i dati richiesti per la sottoscrizione di un qualsiasi contratto. Ciononostante, per ovviare a tutto ciò, il legislatore ha previsto i cosiddetti formati multistrato, riguardanti le privacy policies, con i quali si mira a migliorare la qualità dell'informazione, condensando in strati informativi semplificati tutto ciò che consenta all'interessato di intendere la propria posizione in merito.

2.2.4 Diritto all'oblio

Altro principio fondamentale è rappresentato da un diritto assoluto quale è il diritto all'oblio, contemplato dall'articolo 17 del GDPR. Esso consiste nella possibilità di rettifica e cancellazione dei dati personali, compresi qualsiasi link, copia o riproduzione (trattati e resi pubblici da altri titolari), da parte

[44] Guastalla, *Privacy e data protection: principi generali,* in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 71.

dell'interessato ove ne faccia richiesta e senza ingiustificato ritardo. È più propriamente definito con una logica secondo la quale persista il contrasto tra il diritto dell'interessato di avere pieno controllo del proprio passato, potendo ordinare la cancellazione dei suoi dati direttamente al titolare del trattamento, e l'interesse pubblico (nel caso si parli di interesse privato, la cancellazione si rende obbligatoria non appena venga richiesta dall'interessato) al quale quei precisi dati sono finalizzati (diritto all'informazione).

Secondo un filone di pensiero, lo si può inquadrare nel più generale diritto alla riservatezza ovvero riferito alla volontà di ciascun individuo ad escludere, nei confronti di terzi, tutto ciò che sia correlato alla propria persona[45]. Si ricade, quindi, sotto una chiave prettamente obiettiva, nelle fattispecie in cui i dati personali raccolti non sono più necessari per le finalità preposte. Tuttavia, deroga tassativa alla facoltà di utilizzo del diritto all'oblio è rappresentata dal fatto che non possa essere esercitato qualora:

- Il trattamento fosse essenziale per motivi di interesse pubblico riferiti al settore della sanità pubblica;
- Per fini di archiviazione nel pubblico interesse, in ambito di ricerca o per motivi statistici[46];
- Per ottemperare ad un obbligo legale previsto dalle normative europee;
- Per l'esercizio del diritto alla libertà di espressione e di informazione[47].

Tuttavia, l'esercizio del diritto all'oblio, in un'ottica di digitalizzazione della Pubblica Amministrazione, è di complessa attuazione. Prima dell'avvento di internet, le attività della PA si sostanziavano nella compilazione e nel passaggio

[45] Edizioni Simone, *Il diritto alla riservatezza*, in La legge per tutti, 27 febbraio 2016, https://www.laleggepertutti.it/.
[46] Guastalla, *Privacy e data protection: principi generali,* in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 81.
[47] Sammarco, *Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 170.

di moduli cartacei che assicuravano piena esecutività del diritto suddetto. Con l'avvento della digitalizzazione e quindi con un aumento di quantità di dati immessi e circolanti nel web con successivo ampliamento della numerosità di soggetti (sia pubblici che privati) sempre più interoperabili, garantire la piena cancellazione dei dati sull'eventuale richiesta dell'interessato non risulta più semplice. In ultima, la disciplina comunitaria non indica se debba rilevare il diritto (all'oblio) del singolo piuttosto che l'interesse collettivo; tuttavia, è bene evidenziare come sia necessario demandare la suddetta scelta all'interpretazione della giurisprudenza di cui hai facoltà anche l'Autorità garante per la protezione dei dati.

Risulta dunque necessario contemperare gli obblighi di pubblicazione, per esempio di atti e documenti amministrativi (richiesti dal d.lgs. 33/2013 sulla trasparenza), con il diritto appena considerato e riguardante la sfera privata di ogni interessato. Tale necessità si affronterà quando si tratteranno gli elementi trasversali che interessano GDPR e Trasparenza nella PA.

2.2.5 L'accountability

Nonostante risulti abbastanza complicato tradurre il termine accountability in una parola del vocabolario italiano, è possibile risalirne ritrovando il significato nel connubio tra responsabilità e compliance che a sua volta può essere visto come l'essere conforme a precise normative. Detto ciò, il ruolo di accountability è menzionato nel capo IV del GDPR in cui si evidenziano due figure molto importanti, quella del titolare del trattamento e quella del responsabile del trattamento. Quest'ultima definita nell'articolo 4 come il soggetto "che tratta dati personali per conto del titolare del trattamento"[48]. Tale principio potrebbe risultare un surrogato o comunque intendibile similmente al concetto di trasparenza; tuttavia, non si tratta di comprendere come il c.d. titolare svolga la

[48] Guastalla, *Privacy e data protection: principi generali,* in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 83.

propria mansione in termini di trattamento di dati personali cosicché l'interessato ne possa tracciare tutti i "movimenti", bensì di una garanzia per quest'ultimo al che l'attività di trattamento venga predisposta in conformità alla disciplina del settore. Una previsione additiva, in ottemperanza all'accountability, hanno le cosiddette regole deontologiche previste nel nuovo Codice Privacy previsto dopo l'entrata in vigore in Italia del D.lgs. 101/2018, che ha adeguato la normativa privacy italiana al Regolamento (UE) 2016/679[49]. In particolare, le regole sopra citate, sono espressione del c.d. principio di sussidiarietà[50], da intendere nel suo carattere orizzontale e quindi nel rapporto tra pubblici poteri e privati (tema che verrà ripreso e riproposto successivamente) che, analizzando l'articolo 2-quater del nuovo Codice, si articola nell'esercizio dei primi di cui è investito il titolare.

2.2.6 Privacy by design e by default

In questo paragrafo ci si limiterà a definire in termini generali i concetti di privacy by design e by default, tematiche che verranno riprese in seguito, analizzando un caso concreto riferito ad un progetto di collaborazione tra ente pubblico e soggetto privato. I due concetti possono essere visti, seppur per alcuni aspetti opposti, come complementari e distinguibili dicotomicamente. Quanto al primo principio, si intende che "tutte le attività progettate e realizzate dall'impresa devono tenere conto della protezione dei dati personali dei soggetti coinvolti"[51], mentre il concetto di "default" indica che qualsiasi prodotto o servizio rilasciato debba adottare un'impostazione predefinita in un'ottica di minimizzazione e

[49] Gazzetta Ufficiale della Repubblica Italiana, https://www.gazzettaufficiale.it/.
[50] Zuddas, *L'Autorità di controllo: il "nuovo" Garante per la protezione dei dati personali*, in Il "nuovo" codice in materia di protezione dei dati personali, a cura di Scagliarini S., Giappichelli Editore, Torino, luglio 2019.
[51] Redazione Alma Laboris, *Privacy by design e by default: significato, definizione, differenze*, in Alma Informa, 2021, https://www.almalaboris.com/.

limitazione delle finalità che si propone di raggiungere il titolare del trattamento dei dati stesso. Questi concetti verranno poi ripresi più nello specifico.

2.3 Soggetti interessati nel trattamento dei dati personali

Dopo aver analizzato i principi fondamentali inerenti al GDPR è importante comprendere come la complessa tematica relativa al trattamento dei dati sia gestita da un punto di vista soggettivo, ovvero con una disamina dei soggetti coinvolti, soprattutto nei casi in cui vengano sottoscritti dei contratti tra enti o comunque realtà giuridiche diverse. A tal proposito, è bene definire le principali figure evidenziate dal Regolamento europeo preso in esame e che verranno elencate di seguito:

- Titolare del trattamento: si tratta della persona fisica (per esempio un professionista) o giuridica (es. società, associazione, etc.) che determina le finalità e i mezzi del trattamento dei dati personali (articolo 4, n° 7, del GDPR). Si tratta del c.d. data controller (ovvero colui che raccoglie i dati e li destina[52]);
- Responsabile del trattamento: l'appena citato art. 4 lo riconosce nella figura di colui, persona fisica o giuridica che sia, il quale tratta dati per conto del titolare. In questo caso lo si riconosce nel ruolo del c.d. data processing che si configura nell'attività esecutiva di gestione e manipolazione dei dati. È possibile, per il titolare, nominare più responsabili al fine di agevolarne la gestione. Occorre precisare che i dati dell'interessato potranno circolare tra i due soggetti senza ulteriore approvazione (se non genericamente in via preventiva siglando l'informativa) da parte di quest'ultimo proprio per semplificare il processo;

[52] Brutti, *Le figure soggettive delineate dal GDPR: la novità del data protection officer,* in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 125.

- Data protection officer (DPO): quest'ultima carica non è da confondere con il responsabile del trattamento già analizzato. Si tratta di una figura strettamente innovativa a cui è affidato il ruolo di consulente in materia di protezione di dati personali. Introdotto con l'emanazione del GDPR, è necessario che tra i requisiti siano presenti soprattutto capacità professionali da un punto di vista giuridico e di sicurezza informatica. È dunque possibile ritenerlo un soggetto in grado di assicurare l'ottemperanza alle prescrizioni normative di tutti i soggetti che in qualche modo svolgono una funzione in materia di trattamento di dati personali[53].

Come evidenziato, le figure di titolare e di responsabile del trattamento dei dati sono tra di loro interoperabili, soprattutto per quanto riguarda la comunicazione di eventuali violazioni sulla gestione dei dati personali. L'articolo 33 del GDPR ne costituisce un esempio, in quanto definisce le modalità con le quali, nel caso in cui si riscontrassero delle inottemperanze alla normativa e quindi dei c.d. data breach, si debba provvedere alla trasmissione della suddetta violazione all'Autorità di controllo entro 72 ore (nel caso in cui non sia rispettato tale termine, si dovrà motivare il ritardo). La suddetta comunicazione avverrà sempre per mezzo del titolare, anche nel caso in cui si presenti un'irregolarità rispetto a quei trattamenti svolti sotto la gestione del responsabile che in tal caso avviserà tempestivamente il titolare; quest'ultimo, successivamente, potrà anche esimersi dal ruolo di interposto e, sotto la sua responsabilità, decidere che la violazione suddetta non sia caratterizzata da una discreta probabilità di rischio. Il Regolamento europeo sottolinea inoltre che, nel caso si presenti un rischio elevato per i diritti e le libertà delle persone fisiche, debba essere reso partecipe anche l'interessato[54].

[53] Brutti, *Le figure soggettive delineate dal GDPR: la novità del data protection officer*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 139.
[54] Brutti, *Le figure soggettive delineate dal GDPR: la novità del data protection officer*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 144.

2.3.1 Data Protection Officer (DPO)

Successivamente a questa breve disamina riguardante le due figure rilevanti e presenti prima dell'emanazione del GDPR per le quali potrebbe essere utile analizzare più nel dettaglio le loro mansioni, ci si vuole focalizzare sul ruolo del terzo soggetto operante in realtà dove persista un'attività pubblica, o comunque in organismi pubblici, nonché di attività suscettibili di gestire un ingente flusso di dati (soprattutto se riguardanti la categoria dei dati sensibili) che si struttura nella figura del DPO (indicante il Responsabile della protezione dei dati e richiesta obbligatoriamente dall'articolo 37, par. 1 del GDPR). Secondo la normativa vigente, è ritenuto un soggetto (fisico o giuridico che sia) avente rilevanza centrale all'interno di un ente societario.

Passando alle funzioni adibite alla suddetta figura innovativa, l'articolo 39 del GDPR ne contempla i seguenti compiti:

- "informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati (monitorare la compliance inteso come conformità alla normativa europea GDPR);
- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

- cooperare con l'autorità di controllo quale il Garante;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione".

La figura analizzata in questo paragrafo è dotata di autosufficienza e discreta indipendenza (attributi che devono essere riconosciuti da parte di titolare e responsabile al trattamento dei dati personali) rispetto all'attività aziendale dell'impresa a cui è adibito. Tuttavia, come del resto nella maggior parte delle funzioni aziendali, è opportuno menzionare il possibile rischio di una sua capture, ovvero di fenomeni corruttivi. Il DPO, infatti, oltre al ruolo di responsabile della protezione dei dati nell'azienda in cui è stato nominato, può svolgere altre mansioni che in qualche modo potrebbero evidenziare dei conflitti di interessi (prevenibili attraverso la dettatura di una serie di regole atte ad evitare l'intromissione di figure terze nel proprio operato scongiurando inopportuni condizionamenti da parte di questi ultimi). Oltre alle problematiche suddette, è necessario che il DPO abbia una conoscenza informatica (relativamente all'ampio spettro della c.d. cyber security) che assicuri il coinvolgimento in un'ottica proattiva con lo scopo di sventare attacchi informatici alla luce di una Pubblica Amministrazione, e comunque complessivamente di un sistema lavorativo, sempre più digitale.

Capitolo 3 Applicazioni GDPR

Dopo aver introdotto il tema del trattamento dei dati personali, si procede con l'analisi dei progetti (soffermandosi sullo studio riguardante il portale "Dime, la città di Venezia per te") che vedono coinvolti un ente pubblico (Comune di Venezia) e un soggetto privato (Venis S.p.A., società in house) operante all'interno dello stesso comune, sotto il profilo "GDPR", il quale accomuna entrambe le realtà. Agendo per conto del Comune e quindi dovendo operare in un settore dove il reperimento e il successivo trattamento dei dati relativi ai propri cittadini (sia come fruitori di servizi che come utenti) da parte dell'ente è all'ordine del giorno, è necessario che la suddetta società attui pianificazione e progettazione in ottemperanza della normativa europea n. 2016/679. Tale questione risulta rilevante soprattutto in ordine alla nascita delle c.d. smart city nelle quali il cittadino può fruire di numerosi servizi, soprattutto in chiave digitale, e per le quali vi è, come anticipato nel precedente capitolo, persistenza di una serie di dati sempre più smisurata. Con il termine "smart city" si intendono, per l'appunto, le sempre più presenti città intelligenti, nelle quali si consegue l'efficienza con la trasformazione dei servizi resi in modo tradizionale in servizi che si avvalgono di tecnologie digitali e delle telecomunicazioni[55]: Venezia ne è un esempio e, secondo il rapporto ICity Rank 2021 sulla digitalizzazione delle città italiane, redatto ogni anno da FPA (Forum Pubblica Amministrazione), occupa la tredicesima posizione[56].

Prima di procedere però, è utile delineare gli aspetti appartenenti ai soggetti coinvolti nella condivisione dei progetti, partendo da una breve disamina e rappresentazione delle funzioni.

[55] Compagnucci, *Smart City 2020-2021 in Italia quali sono attualmente e in via di sviluppo*, in Business Online, 2022, https://businessonline.it/.
[56] Redazione FPA, *ICityRank, Rapporto annuale 2021, Indice di trasformazione digitale*, in Forum PA, 23 novembre 2021, https://www.forumpa.it/.

3.1 Società in house

Per società in house si intende una società di diritto privato, che solitamente si rispecchia in una società per azioni (S.p.A.), controllata per gran parte da un ente pubblico e per il quale svolge funzioni e attività da quest'ultimo assegnate. Nel caso di Venis S.p.A., la partecipazione del Comune di Venezia al capitale sociale per l'anno 2021 consta di 19.530 azioni ordinarie su 30.000 (65,10%)[57]. Tralasciando la quota riservata alla Città metropolitana di Venezia (10,00%) la quale verrà presa in considerazione nei paragrafi in cui si tratterà l'importante aspetto della contitolarità dei dati (in relazione al GDPR), il rimanente è assegnato ad altre società che a loro volta sono controllate dal comune stesso (24,90%)[58]. Tornando all'enucleazione dei compiti, una società della tipologia descritta svolge lavori prettamente per l'ente pubblico (più dell'80% delle attività è effettuata nei confronti dell'ente pubblico controllante[59]); non lavora quasi mai per terzi esterni alla propria compagine. È possibile definirlo come un soggetto ibrido, da una parte regolato secondo le regole del diritto privato (compresa la sua natura giuridica, con annesse procedure di selezione del personale e di colloqui interni) e dall'altra in grado di svolgere attività che perseguono dei fini pubblici.

La società presa in considerazione ha stipulato il 19 dicembre del 2017 il contratto di servizio con il Comune di Venezia denominato "Servizio di gestione del sistema informativo comunale" con il quale, tra tutti i servizi erogati e dei quali il Comune è beneficiario, è presente la fornitura dei c.d. servizi SaaS (Software as a Service). Questi ultimi sono riferiti alla piattaforma Dime della quale i cittadini possono fruire. Verrà ora analizzato nel dettaglio quanto sopra detto.

---

[57] Venis S.p.A., *Bilancio Venis 2021*, in Società trasparente, 2021, https://www.venis.it/.
[58] Dati visualizzabili e consultabili all'interno del sito internet di Venis S.p.A. alla sezione "Società trasparente".
[59] Uncategorized, *Società in house 2022: cos'è e come funziona, requisiti, differenze*, in Soldi oggi, 1 ottobre 2022, https://www.soldioggi.it/.

3.2 Cosa si intende per SaaS?

Prima di fornire una propria definizione di questa tipologia di servizi è necessario compiere un passo indietro. Innanzitutto, è utile rilevare che si tratti di un modello di distribuzione che insieme ad altri rappresenta l'implementazione dei c.d. servizi di cloud computing i quali, l'agenzia del governo degli Stati Uniti d'America, NIST (National Institute of Standards and Technology), denomina come infrastruttura. Appoggiandosi ai servizi internet, consente l'accesso incondizionato ad una serie condivisa di risorse da parte degli utenti senza che queste ultime siano presenti (anche se virtualmente) sui propri dispositivi informatici. Scopo di tale modello è quello di permettere l'accesso da remoto a dei software (o applicativi) attraverso delle interfacce web e più in generale, consentendone la fruizione a degli utenti thin; ovvero coloro che, per accedervi e fruire del singolo servizio, utilizzano dei computer con potenza di calcolo limitata tramite l'impiego di applicativi (ad esempio, con l'utilizzo di browsers)[60].

Nonostante il suo utilizzo sia di facile comprensione, quello dei servizi di cloud computing rappresenta, per le Pubbliche Amministrazioni, un tema assai delicato se analizzato da un punto di vista di tutela dei dati personali. Infatti, esso si rifà e prende in causa l'articolo 28 del GDPR in quanto si richiede che il titolare dei dati possa ricorrere solamente a determinati soggetti: responsabili che previamente presentino idonee garanzie al che vengano predisposte tutte quelle misure di tipo tecnico e organizzativo in grado di assolvere alle normative del regolamento in chiave di trattamento dei dati personali[61]. Nel prossimo paragrafo verranno enunciate alcune caratteristiche che evidenzieranno trasversalmente il legame tra tutela dei dati (e della privacy) e i servizi di cloud computing.

---

[60] Valle, Russo, Locatello, Bonzagni, *Privacy e contratti di cloud computing*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 508.

[61] Cosmi, *Servizi cloud e compliance GDPR: obblighi e soluzioni*, in CyberSecurity360, 3 maggio 2019, https://www.cybersecurity360.it/.

3.2.1 Tutela della privacy e cloud computing

All'interno dei contratti di cloud computing il trattamento sia dei dati personali che di quelli non personali risulta una materia molto importante da evidenziare. Per quanto riguarda il progetto preso in considerazione in questo scritto, si tratta di una piattaforma che andrà a gestire con operazioni di trattamento (ovvero archiviazione, elaborazione ed eventuale trasmissione) una sostanziale mole di dati privati appartenenti ai singoli cittadini. La tutela della privacy e l'agire conformemente al regolamento europeo GDPR sono di rilievo in una città che punta alla digitalizzazione quale è Venezia e in ottica di realizzazione di un mercato unico digitale a livello europeo. Con quest'ultima espressione si vuole intendere di creare un mercato di dati (non personali) in cui sia consentita la libera circolazione tra gli Stati membri (c.d. free flow). In merito si menziona il Regolamento europeo 1807/2018, pubblicato nella Gazzetta Ufficiale dell'Unione Europea, che disciplina in tema di circolazione di dati non personali. Questi vengono definiti (articolo 3 Reg. 2018/1807) come diversi dai dati personali indicati dall'articolo 4, punto 1 e quindi comprendono tutti quelli per i quali non sia possibile risalire ad una persona fisica o che comunque non vi appartengano. Tale regolamento andrebbe ad integrare le norme già previste, in tema di dati personali, dal GDPR. Il Regolamento del 2018 sarebbe suscettibile ad ulteriore applicazione in ambito di dati personali anonimizzati o pseudonimizzati perché appunto non riconducibili ad alcuna persona fisica. Tuttavia, una problematica riguarda i due processi suddetti e quindi alla dubbia fattibilità delle operazioni di anonimizzazione e pseudonimizzazione dei dati che, secondo la dottrina, "it would appear (…) that no data can be entirely anonymized"[62] potrebbero ricadere nella "giurisdizione" dell'applicazione del GDPR. Importante è stabilire chi tra provider (nel caso esaminato, nel soggetto di Venis S.p.A.) e fruitore

[62] Valle, Russo, Locatello, Bonzagni, *Privacy e contratti di cloud computing*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 516.

(Comune di Venezia) del servizio ricopra la carica di responsabile del trattamento e chi di titolare del trattamento.

In relazione a quanto detto riguardo alla progettazione ed erogazione di soluzioni informatiche (cloud computing), considerevole importanza è adibita al rilascio della c.d. certificazione ISO 27001, ovvero dello standard normativo internazionale atto ad asserire la sicurezza delle informazioni curate da un soggetto (quale persona giuridica). Tale attestazione, con validità di tre anni e prettamente facoltativa, offre credibilità al soggetto (tra i quali Venis S.p.A.) che ne richiede il rilascio in conseguenza ad una consapevolezza di tipo legale agli occhi dei soggetti che collaboreranno con loro.

3.2.2 Titolarità vs Responsabilità

Il tema che si propone ora sarà analizzato in chiave di responsabilità per quanto riguarda il trattamento dei dati. La differenza, per certi versi dicotomica, presente e inerente a quanto individuato dal suddetto titolo, rappresenta un carattere rilevante nella gestione dei dati conformemente al GDPR; anche nell'eventuale (più o meno possibile, a seconda del livello di rischio connesso) violazione o fuoriuscita illecita come visto nel precedente capitolo al paragrafo relativo al c.d. data breach. Su quest'ultimo fenomeno, in particolare, la giurisprudenza si è espressa in maniera drastica, prevedendo l'obbligo in capo al responsabile del trattamento dei dati di comunicare la violazione al titolare (con estrema puntualità) non appena ne sia venuto a conoscenza. Successivamente, il titolare avrà settantadue ore di tempo per informare l'autorità di vigilanza preposta tramite atto di notifica[63]. Nel caso in questione, il soggetto titolare dei dati (relativi ai cittadini) si concretizza nell'ente pubblico (Comune di Venezia, abilitato al trattamento dei dati richiesti in ogni pratica offerta all'interno della piattaforma "Dime") che si avvale di un responsabile (Venis S.p.A.) che, secondo la

[63] Valle, Russo, Locatello, Bonzagni, *Privacy e contratti di cloud computing*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 528.

convenzione stipulata nel dicembre 2016, si riconosce come soggetto adibito alla gestione dei server e alla manutenzione dell'infrastruttura informatica. Più complesso risulterebbe comprendere su quale soggetto (o su quali, nel caso risulti una contitolarità) ricada la responsabilità nell'ipotesi in cui il provider del servizio nomini (e quindi faccia affidamento per ottemperare, tanto in fase di progettazione quanto in quella di gestione, alla realizzazione del servizio di cloud computing) dei sub-fornitori. In tal caso, sarebbe necessaria un'analisi sul ruolo e sull'attività svolta dai sub-fornitori per poterli eventualmente definire sub-responsabili, ma di ciò si potrebbe parlare in un altro scritto. Ciò che invece risulterebbe di non facile comprensione sarebbe il caso in cui ci fossero due o più titolari a determinare le finalità e i mezzi del trattamento e che porrebbe la questione sulla c.d. contitolarità del trattamento. L'articolo 26 recita in favore di quanto appena detto disciplinando che anche un'eventuale azione atta ad esercitare i propri diritti in tema di trattamento dei dati debba essere posta dagli interessati (dei dati) nei confronti di ciascun titolare (i quali potrebbero dover rispondere in solido)[64]. Tuttavia, il ruolo di Venis S.p.A. come responsabile del trattamento dei dati non sorge automaticamente, bensì tramite apposito atto di nomina da parte dello stesso titolare. In questi casi è quindi necessario che l'atto sia predisposto formalmente indicando quali dati personali verranno trattati dal responsabile (distinguendo tra dati comuni, particolari, relativi a procedimenti giudiziari) e quali saranno i compiti ad esso affidati. Con quest'ultima dicitura si vuole fare riferimento al trattamento in termini di comunicazione, affidabilità e non divulgazione fornendo le necessarie garanzie, nonché di sicurezza in ordine a misure tecniche e procedure per testarne, verificarne e valutarne regolarmente l'efficacia in modo tale da non permettere eventuali accessi privi di autorizzazione.

[64] Tale problematica è stata trattata nell'introduzione di un progetto per il quale è stato necessario stabilire i ruoli dei differenti attori (soggetti, enti) in questione ovvero, Comune e Città Metropolitana di Venezia. Si tratta del progetto emergenza Ucraina.

Tornando al ruolo del GDPR, viene previsto che, se prescritto dalla legislazione dello Stato membro, venga prolungata la conservazione dei dati anche oltre la scadenza definita dal contratto: il Comune di Venezia, con riguardo allo sportello digitale "Dime" presente nel proprio sito istituzionale, prevede che "i dati personali sono trattati […] per il tempo strettamente necessario a conseguire gli scopi per cui sono raccolti […]"[65].

Ancora una volta, il legislatore ha voluto definire un approccio di tipo proattivo nella progettazione di quei servizi (digitali) che andranno a richiedere e successivamente trattare dati personali per conto del titolare. Si procede ora evidenziando come debba essere sviluppato un servizio di cloud computing alla base menzionando le due modalità indicate nei primi paragrafi dell'articolo 25 del GDPR[66]:

- Protezione dei dati fin dalla progettazione [par. 1];
- Protezione dei dati per impostazione predefinita [par. 2].

In conclusione, e in riferimento alla responsabilità dei soggetti riconosciuti in titolare e responsabile dei dati personali, si riporta un provvedimento del Garante per la protezione dei dati personali, che ha sanzionato pecuniariamente una società fornitrice di software per la Polizia Locale di un comune italiano; all'interno del portale si gestivano i dati relativi ai destinatari di contravvenzioni, per la violazione delle disposizioni di servizio. In tale nota, viene in rilievo come solamente il responsabile del trattamento sia stato sanzionato e non il titolare, soggetto adibito alla gestione dei dati personali. Tutto ciò perché, alla luce del fatto che la società fosse stata riconosciuta come soggetto dotato di esperienza in campo tecnologico, avrebbe dovuto provvedere più rigorosamente all'adozione di misure di sicurezza adeguate verificandone l'effettiva efficacia. Alla luce di

[65] Dime, La città di Venezia per te, *Privacy Policy*, in Comune di Venezia, https://dime.comune.venezia.it/.
[66] Farace, *Privacy by design e privacy by default*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 496.

ciò, risulta estremamente necessario (per un fornitore di software finalizzato alla fruizione di servizi che coinvolgano una pluralità di interessati quali, in questo caso, cittadini) analizzare attentamente ciò che consegnerà in gestione al fine di ottemperare alle norme di sicurezza informatica.

3.2.3 Data protection by design & by default: approccio preventivo

Il presente paragrafo mette in chiaro il ruolo della globalizzazione nel mercato dei dati (definito come "scambio" di dati personali e non tra paesi comunitari e non). L'avanzamento tecnologico che ha coinvolto e coinvolge tuttora la società odierna permette un coinvolgimento di mole di dati sempre più cospicuo. Il ruolo della tecnologia ha consentito la mutazione tanto di rapporti economici quanto di relazioni sociali (social networks) permettendo da un lato una circolazione e condivisione di dati sempre più accentuata e dall'altro sottolineando il bisogno di ricorrere a degli strumenti via via più sofisticati. Il tutto per regolarne in qualche modo il flusso quasi incontrollato non solo all'interno dell'Unione, bensì verso paesi terzi.

Definiti gli attori principali e individuati i relativi servizi offerti in ambito di cloud computing, si passa ora alla delicata questione della cosiddetta progettazione del servizio. Si tratta di un passaggio fondamentale, che sancisce quella che sarà l'interfaccia finale che in un certo modo collegherà l'utente al titolare del trattamento dei dati (individuato nel precedente capitolo). Infatti, il titolare del trattamento, identificato in un momento antecedente, ha il diritto di richiedere una serie di dati ai propri utenti ma tale diritto dovrà essere esercitato solamente per il conseguimento degli scopi predeterminati e quindi, in un certo senso, la richiesta dei suddetti dati dovrà essere congrua alla finalità preposta (sempre secondo il GDPR). In sostanza, non devono essere richiesti dati che possano considerarsi superflui alla causa e che quindi non siano ritenuti necessari. L'articolo 25 del Regolamento generale sulla protezione dei dati disciplina in merito specificando per l'appunto che "il titolare […] debba

garantire che siano trattati […] solo i dati personali necessari per ogni specifica finalità del trattamento"[67]. A supporto di quanto accennato poc'anzi vi è il Considerando n°78 che recita a favore dell'individuazione di quelle misure tecniche e organizzative[68] adeguate ad ottemperare a quanto richiesto dal regolamento europeo in materia di tutela dei dati personali. L'attività del titolare risulta perciò di particolare rilevanza e la sua figura può ritenersi caratterizzata in prima analisi da autonomia, in quanto spetta a quest'ultimo definire obiettivi e mezzi del trattamento e in secondo piano necessità perché in questa disciplina la sua nomina è imprescindibile.

Detto ciò, per comprendere tutti gli obblighi (eterogenei tra loro) ascritti in capo al titolare del trattamento è utile considerare l'articolo 5 del GDPR, il quale disciplina in materia di principi applicabili al trattamento dei dati personali, che vengono citati in sei punti come di seguito (verranno evidenziati i caratteri "chiave" di ogni punto):

- Liceità, correttezza e trasparenza;
- Limitazione delle finalità;
- Minimizzazione;
- Esattezza;
- Limitazione della conservazione;
- Integrità e riservatezza.

Quanto appena sottolineato è accompagnato dalla garanzia di poter eventualmente (ove richiesto) dimostrare, in capo al titolare, che il trattamento sia stato eseguito in ossequio al regolamento (art. 24, GDPR).

[67] GDPR, *Art. 25 GDPR – Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*, in Altalex, Ip-It e Data protection, 14 gennaio 2019, https://www.alltalex.com/.
[68] Farace, *Privacy by design e privacy by default*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 493.

Tornando ai due criteri presentati nella rubrica dell'articolo 25 (GDPR) è utile partire dall'esamina del profilo riguardante la protezione dei dati per impostazione predefinita (c.d. privacy by default). Quest'ultima è enunciata nel paragrafo 2 del suddetto articolo che impone, a colui che tratterà i dati, degli obblighi specifici di valutazione concernenti aspetti tecnici e organizzativi in modo tale che siano trattati esclusivamente dati per le finalità che si sono poste fin da principio.

In merito alle azioni da intraprendere, nel testo di legge vengono citate quelle riguardanti la quantità dei dati, l'estensione del trattamento, il periodo di conservazione e l'accessibilità[69]. In ogni caso, il titolare deve garantire all'interessato che i suoi dati personali non siano accessibili da un numero indefinito di soggetti senza che ne sia stato rilasciato il proprio consenso (a meno che non si parli di contitolarità). Per quanto riguarda il secondo criterio (art. 25, par 1, GDPR) concernente la protezione dei dati fin dalla progettazione, il legislatore prevede tre obblighi:

- Considerare gli aspetti riguardanti le proprie attività in ottica di trattamento dei dati (compresa una valutazione dei rischi);
- Esaminare le misure tecniche e organizzative affinché i principi di protezione dei dati vengano attuati in maniera efficace e secondo una logica di minimizzazione (valutando gli aspetti relativi alla sicurezza dei dati personali);
- Integrare nel trattamento le necessarie garanzie e tutelare i diritti degli interessati.

Quanto al secondo punto, la disciplina del GDPR indica solamente la pseudonimizzazione (ovvero rendendo il dato completamente non associabile ad un interessato in particolare senza l'utilizzo di ulteriori informazioni) dei dati che

[69] Farace, *Privacy by design e privacy by default*, in Privacy Digitale, a cura di Tosi E., Giuffrè Francis Lefebvre, Milano, 2019, p. 497.

però, si vedrà (in seguito) in un caso specifico menzionato, non basterà a garantire la totale anonimità del soggetto a cui fanno capo i dati per via di strumenti supplementari come ad esempio i cookies.

Venendo ora ad analizzare più nello specifico il caso concreto del portale del Comune di Venezia (Dime), quest'ultimo si basa sull'erogazione e la gestione di una serie di servizi remoti (tra i quali si possono citare quelli di richiesta di particolari certificati, per esempio anagrafici piuttosto che residenziali, e quelli relativi a servizi di segnalazione, per esempio, di affissioni abusive piuttosto che riferiti a rifiuti, cassonetti e pulizia). Ogni servizio, nella sua progettazione, viene individuato dalla redazione di una scheda chiamata Check list che propone una sintetica descrizione del progetto o servizio indicando poi le tipologie di dati e le modalità di attuazione del trattamento di questi ultimi nonché le misure di sicurezza previste e atte a prevenire fenomeni cosiddetti di data breach. Tema di fondamentale rilevanza, previsto con il criterio privacy by design dal Regolamento europeo 2016/679, è rappresentato dalla compilazione delle summenzionate misure di sicurezza. Con riferimento a queste ultime, che si delineano in misure tecniche e organizzative, il GDPR all'articolo 25 prevede che, in ottica di predisposizione, venga considerato lo stato dell'arte. Con quest'ultima dicitura, il legislatore ha voluto intendere che titolare e responsabile (o comunque qualsiasi soggetto che in qualche modo possa dover gestire una serie di dati personali) debbano attenersi al progredire tecnologico prevedendo eventuali aggiornamenti riguardanti le misure di sicurezza implementate (con estremo riguardo a quelle tecnologiche); infatti, è possibile che il titolare riscontri che una determinata misura non sia più adeguata a conferire un livello di protezione in ottemperanza del sopra citato articolo 25 GDPR[70]. È necessario quindi che sia implementata, per esempio, una congrua formazione del personale

[70] Butti, *Le misure di sicurezza nel GDPR: quali sono, come applicarle, costi di attuazione*, in NetworkDigital360, 11 maggio 2021, https://www.cybersecurity360.it/.

orientata al continuo aggiornamento in tema di sicurezza (in chiave di trattamento dei dati personali). Sempre in relazione alla check list, è prevista un'area dove vengono ricomprese tutte le tipologie dei dati trattati tenendo conto, in particolare, che la scelta dei dati richiesti non può eccedere quelle che sono le finalità predisposte da quel determinato progetto o servizio. Per fornire un esempio molto semplice ma in grado di far cogliere al lettore la particolare obbligatorietà prevista in tema di trattamento dei dati personali, nella richiesta di rilascio di un certificato anagrafico, non potrà essere richiesto all'utente, oltre, tra i vari, a nome e cognome, la giacenza media perché appunto la sua conoscenza non rappresenta propedeuticità alla finalità preposta (ovvero semplice rilascio di certificato anagrafico). Successivamente, un ruolo abbastanza sensibile lo ricopre la possibilità di prevedere interoperabilità tra i sistemi gestionali di più soggetti (di norma, uffici di enti pubblici o privati che siano). Tornando all'esempio appena riportato, quando il Comune di Venezia rilascia un certificato anagrafico, può essere previsto che l'utente (cittadino) non debba inserire la totalità dei dati (che in un secondo momento compariranno nel certificato in questione) via input (digitando su apposito form). In tal caso sarà necessario ricorrere, attraverso i dati immessi dall'utente nel proprio portale, ad uno "scambio" di informazioni con l'ufficio anagrafe (al quale verranno richieste altre informazioni) per il quale il soggetto interessato e richiedente dovrà essere messo a conoscenza attraverso il consenso al trattamento dei dati personali.

Ultimata e predisposta nelle sezioni di cui si compone, ogni scheda deve seguire un determinato iter procedurale prima di essere confermata e attuata nella pratica. In primis, sarà sottoposta, dal responsabile (nel caso citato, Venis S.p.A.), a validazione del c.d. data protection officer (nominato dal soggetto responsabile), figura competente in materia di trattamento dei dati personali e introdotta nel precedente capitolo. Il DPO dovrà dunque segnalare al mittente dell'istanza qualsiasi non conformità riguardante la richiesta dei dati e la tutela

della privacy in generale (con riguardo ai dati sensibili, qualora fossero previsti dalla singola scheda). Ottenuto il consenso di quest'ultimo, è necessario ottemperare al passaggio successivo, ovvero presentare il tutto al titolare del trattamento dei dati personali (Comune di Venezia) che, procederà analogamente ponendo ogni scheda pervenuta dal responsabile del trattamento al proprio DPO.

Altro punto fondamentale è enunciato nell'articolo 35 (GDPR) che disciplina il caso in cui il trattamento dei dati personali comporti un rischio elevato per i diritti e le libertà delle persone interessate (per esempio quando siano trattati dati sensibili di un'ampia numerosità di soggetti)[71]. In tal caso, il titolare è obbligato a sviluppare una valutazione di impatto prima di realizzare il trattamento stesso. Tale valutazione prende il nome di Data Protection Impact Assessment (DPIA) ed è predisposta dal titolare coadiuvato, in caso fosse previsto, dal responsabile del trattamento. È utile segnalare che, il Regolamento europeo già richiede al titolare di effettuare tutte le operazioni relative al trattamento stesso in ottemperanza di quanto previsto nell'articolo 24 il quale afferma che "[…] il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, […], che il trattamento è effettuato conformemente al presente regolamento". L'articolo appena menzionato, figurante nel principio dell'accountability, riguardante l'attività del titolare del trattamento dei dati personali, potrebbe sembrare e presentare connotati analoghi a ciò che è previsto nell'articolo 35 (GDPR); la distinzione tra i due si può esplicare nell'analisi a valle, riferita al trattamento, in ottica preventiva. Il WP29, che ora è stato sostituito dall'European Data Protection Board (in italiano, Comitato europeo per la protezione dei dati), organismo consultivo indipendente composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della

[71] Garante privacy, *Valutazione d'impatto della protezione dei dati (DPIA)*, in Garante per la protezione dei dati personali, https://www.garanteprivacy.it/.

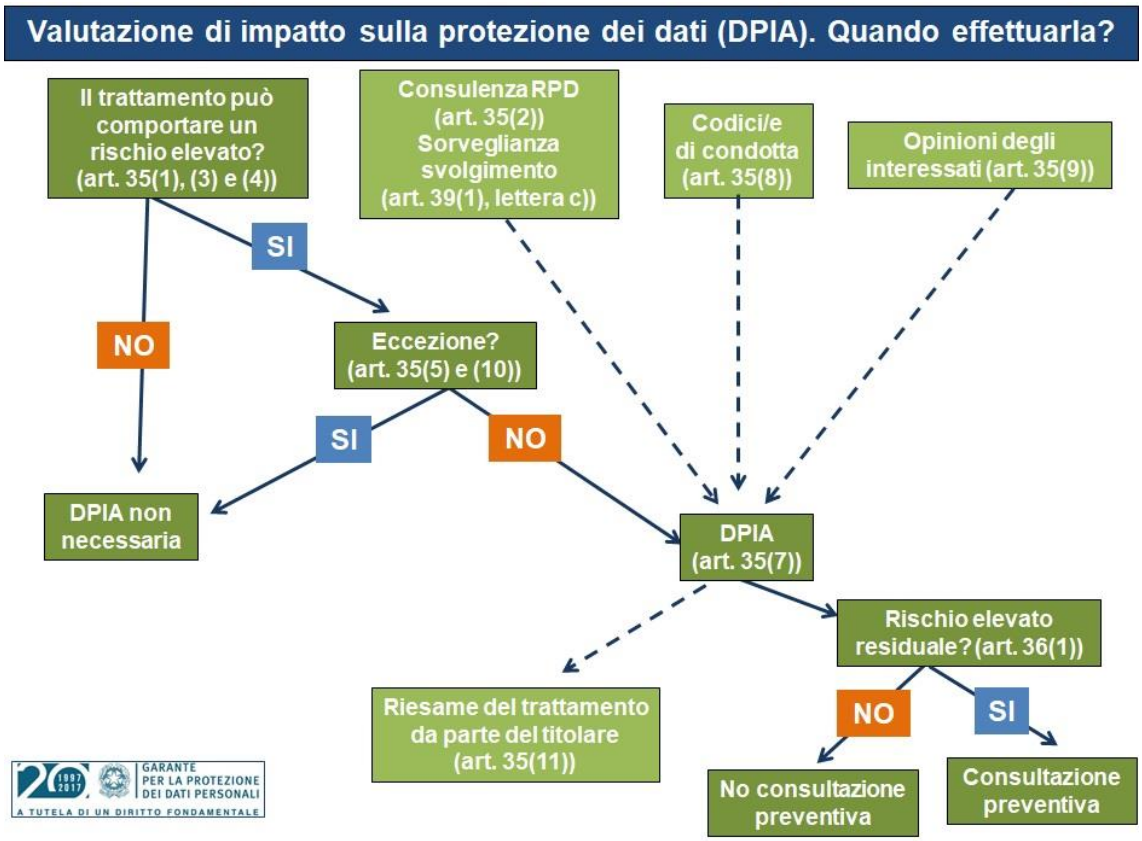
protezione dei dati e da un rappresentante della Commissione europea[72], ha precisato in quali casi la suddetta procedura sia obbligatoria, in cosa consista e da chi debba essere predisposta. Generalmente, la c.d. DPIA è utile a prevenire eventuali incidenti futuri in tema di trattamento dei dati personali e rappresenta il principale fondamento in ottica di protezione dei dati fin dalla fase di progettazione (by design).

Quanto appena detto rientra nei tre provvedimenti adottati dal gruppo dei Garanti Privacy indicando e sottolineando alcuni punti fondamentali del GDPR in chiave di nuove tecnologie[73] (anche in ambito PA, in base al coinvolgimento di una serie di dati acquisiti; questa tematica meriterebbe un approfondimento anche in base all'utilizzo dell'Intelligenza Artificiale in ambito economico e giuridico ma del quale non si tratterà)[74]:

- "Guidelines on Data Protection Impact Assessment and determining weheter processing is "llikely result in high risk" for the purposes of Regulation 2016/679;
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679;
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679".

[72] Saetta, *European Data Protection Board (ex WP29)*, in European Data Protecion Board, 14 giugno 2018, https://protezionedatipersonali.it/.
[73] Inglobando il cosiddetto Machine Learning, inteso letteralmente come apprendimento automatico e basato su algoritmi che riescono a migliorare le performance.
[74] European Commission, *Data protection impact assessment (DPIA)*, 22 agosto 2022, https://ec.europa.eu/.

Di seguito uno schema procedurale riguardante il funzionamento della valutazione di impatto sulla protezione dei dati (DPIA)[75] [Figura 1].



Di seguito si aprirà una breve parentesi su un fenomeno, riconosciuto a livello internazionale, che sta avendo delle rivisitazioni proprio a tutela del diritto alla privacy e ad un trattamento "incognito" dei propri dati. Il whistleblowing, nonostante presenti lacune normative, ha preso forma soprattutto nelle PA.

3.2.4 Whistleblowing: garanzia dell'anonimato secondo GDPR

Con il termine whistleblowing (in italiano letteralmente "soffiare nel fischietto") si vuole intendere il fenomeno delle segnalazioni in materia di illeciti corruttivi

[75] Garante per la protezione dei dati personali, DPIA grafico, https://www.garanteprivacy.it/.

per quanto concerne l'ambito lavorativo (ci si occuperà del settore pubblico, nonché delle realtà private ma svolgenti attività pubblica), ai sensi della Legge Anticorruzione, n° 190/2012. Nonostante sia regolamentato in tema di anticorruzione, in questo scritto verranno evidenziati solamente i caratteri principali riferiti alla tutela dei dati personali secondo la normativa europea. Infatti, con questo strumento, si permette a chiunque (lavoratori di una determinata azienda) di poter segnalare internamente condotte illecite commesse da un collega, suscettibili di totale anonimato, non correndo il pericolo di eventuali ritorsioni. È inoltre garantito il fatto che non debba essere possibile risalire, sia direttamente che indirettamente, all'identità del c.d. whistleblower (segnalante). Ogni pubblica amministrazione ha l'obbligo (a differenza del settore privato in cui non si riscontra alcun obbligo legale), secondo la normativa vigente, di prevedere, all'interno del proprio sito istituzionale o aziendale, una sezione relativa a quanto summenzionato. Viene quindi ribadito il ruolo del GDPR il quale obbliga il titolare del sistema citato ad assicurare la totale anonimizzazione del soggetto segnalante con conseguente tutela dei suoi dati personali.

Prima di procedere, però, è necessario introdurre un nuovo soggetto che si identifica nel Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT, introdotto con la legge 6 novembre 2012 n°190 insieme alla figura del sopracitato whistleblower inteso come "dipendente pubblico che segnala illeciti"), la quale persona fisica viene individuata dagli organi di governo dell'amministrazione stessa e il suo operato si sostanzia nell'assicurare la trasparenza in materia di obblighi di pubblicità nonché di segnalare all'ANAC eventuali inadempimenti[76]. Tale figura assume un ruolo rilevante all'interno del processo relativo al whistleblowing perché, rappresenterà il "punto cardine"

[76] Carta, La Selva, *Il responsabile trasparenza e anticorruzione (RPCT)*, in Ius in itinere, 03/03/2019, https://www.iusinitinere.it/.

della specifica segnalazione. Quest'ultima, infatti, giungerà a costui previo totale anonimato del segnalante che potrà verificare e supervisionare l'operato dello stesso RPCT attraverso delle credenziali. Queste, generate secondo una procedura automatica, gli verranno assegnate al momento della segnalazione.

Come si può banalmente rilevare, i dati trattati non fanno capo solamente alla persona del segnalante, a cui, non debba essere in alcun modo consentito di risalirvi, bensì anche alla persona del soggetto segnalato. Nonostante il whistleblowing non sia normato a livello nazionale con delle direttive precise (a differenza della Germania, la quale autorità, al pari di ANAC, ha emesso proprie linee guida) sarebbe tuttavia necessario tutelare anche quest'ultimo secondo la normativa GDPR, nonostante non sia possibile, come è scontato ritenere, sottoporgli una richiesta di consenso al trattamento dei dati. In questo caso, il legislatore si desume essere permissivo consentendo il trattamento dei dati per due motivi principali; il primo è perché ritenuto necessario che il titolare ottemperi ad un obbligo legale[77], il secondo per il fatto di perseguire un interesse legittimo utilizzando i dati (quale quello di poter gestire la segnalazione). Nel caso in cui entrambe le motivazioni non siano applicabili, il Regolamento europeo sulla protezione dei dati personali stabilisce che debba ricorrere l'interesse pubblico come finalità per il trattamento dei dati del segnalato; infatti, quest'ultimo si ritroverebbe in una situazione soggettiva nella quale i suoi dati verrebbero gestiti senza il suo previo consenso e quindi contrariamente a quanto indicato nel GDPR. Da un altro punto di vista, inoltre, la tematica si fa più restrittiva in quanto al soggetto segnalato sono preclusi, in alcuni casi e quindi non in termini assoluti, i diritti di accesso (previsto dalla legge 241/1990) e di eventuale cancellazione dei dati che lo riguardano riferiti ad una sua presunta condotta illecita (artt. da 15 a 22, GDPR) per il semplice fatto che, il whistleblower

[77] Tosoni, *Whistleblowing e GDPR: punti critici e scenari futuri*, in Agenda Digitale, 13 gennaio 2020, https://www.agendadigitale.eu/.

(segnalante) debba essere suscettibile di tutela e la sua identità non possa essere conosciuta in alcun modo (per l'appunto atti ad evitare azioni moralmente riprovevoli nei suoi confronti successivamente alla perdita di riservatezza). Quanto appena descritto rappresenta un aspetto molto sensibile riguardante la tutela della privacy in quanto il trattamento di cui sopra prevarrebbe, ad insaputa del soggetto segnalato, non solamente in una fase iniziale di registrazione della segnalazione, bensì anche di una successiva e adeguata indagine interna operata coinvolgendo gli uffici interessati (secondo quanto dichiarato dal segnalante stesso). La sensibilità dei dati richiesti da una qualsiasi piattaforma di whistleblowing, nella quale, secondo il regolamento di Venis S.p.A. (2021), sono ricompresi il nominativo del soggetto segnalante con annesso ufficio di appartenenza, la descrizione dei fatti (luogo e periodo), le generalità del soggetto segnalato[78], è da considerarsi alta. Il garante per la protezione dei dati personali, con una nota emessa il 10 giugno 2021, sostiene che sia necessaria, data la mole di dati sensibili che verranno trattati, una DPIA tale da poter evidenziare come i suddetti dati vengano trattati. Alla luce di ciò, è richiesta una valutazione d'impatto della protezione dei dati sia per responsabile che per titolare del trattamento dei dati nelle quali viene effettuata un'attenta analisi dei rischi. Tra questi ultimi si ritrova il c.d. rischio privacy legato alla "possibilità che una minaccia possa compromettere la riservatezza di un dato personale"[79], perché sempre di software informatico si tratta. È inoltre riscontrabile un'annessa probabilità e una valutazione delle contromisure da adottare al fine di mitigare il rischio accennato pocanzi. Come molteplici leggi e normative vigenti, anche in questo caso sono previste delle deroghe alle restrizioni appena citate riguardanti il diritto di accesso e nello specifico nel caso in cui un'eventuale contestazione disciplinare (nel software di Venis S.p.A. si parla di difesa dell'incolpato), posta

[78] Venis S.p.A., *Regolamento per la segnalazione di illeciti e irregolarità "whistleblowing",* in Società trasparente, 2021, https://www.venis.it/.
[79] Venis S.p.A., DPIA Whistleblowing.

dal segnalato, abbia, in tutto o in parte, come fondamento l'identità del segnalante; tuttavia, è sempre necessario ci sia consenso alla rivelazione da parte di quest'ultimo e quindi trattasi di mera facoltà del whistleblower.

3.3 Problematiche riscontrabili

L'intero sistema riguardante il GDPR con annessa tutela dei dati personali presenta caratteristiche estremamente sensibili. Come evidenziato, ogni relazione che si configura tra un soggetto privato (che può essere un cittadino piuttosto che un operatore economico quale impresa) e la Pubblica Amministrazione mette in atto una serie di condivisioni di dati che, se non trattati e gestiti come richiesto dalla normativa europea, possono incidere negativamente e quindi ledere la sfera privata dei soggetti interessati. Infatti, in seguito alla rivoluzione digitale che ha riguardato l'intero pianeta, anche l'arena di guerra e le istituzioni (comprese le organizzazioni criminali) hanno effettuato un'immediata traslazione dal classico terreno di battaglia ad uno spazio virtuale indefinito[80]. Un attacco informatico, pur non causando numerose vittime e in un sistema nel quale la vita e l'esistenza di ogni persona è registrata e tracciata attraverso apparecchiature informatiche (si pensi ai banali dispositivi elettronici di domotica[81]), è in grado di procurare ingenti danni alle economie dei diversi paesi. Tornando al tema principale di questo paragrafo, la digitalizzazione apportata ai settori pubblico e privato propri di ogni governo, ha notevolmente incrementato e migliorato l'interoperabilità tra diversi sistemi informatici. Nonostante tale miglioria, è necessario porsi lecite domande in quanto

[80] Falk, *I cyber-attacchi che plasmano la guerra di oggi*, in Insideover, 26 maggio 2020, https://it.insideover.com/.

[81] I rivoluzionari dispositivi elettronici (dallo speaker di casa Amazon alla più comune smart TV) hanno soppiantato il mercato digitale dei dati. Un'inchiesta di Report di Paternesi ha analizzato come la smart tv, successivamente alla semplice apertura dell'app di Netflix (senza possedere un account), contatti non solo il server dell'omonima piattaforma bensì anche server di terze parti (come Google analytics). Vengono così diffusi dati sensibili senza autorizzazione alcuna da parte dell'utenza. In questo modo si prospetta un mercato difficilmente tracciabile e soprattutto incontrollato al quale potrebbero partecipare, ad insaputa dei cittadini, pure le Pubbliche Amministrazioni.

banalmente, nel momento in cui uno specifico dato, appartenente ad un determinato soggetto, venisse condiviso tra più soggetti è logico sostenere che ci possa essere una sorta di contitolarità nel trattamento dei dati personali; tuttavia, non risulta essere sempre così. Tale problematica si riscontra nel caso in cui dello stesso dato vengono in possesso più amministrazioni contemporaneamente e quindi si possa porre il problema di responsabilità in seguito ad un'eventuale fuoriuscita piuttosto che perdita di dati. Per ovviare a quanto appena detto, il GDPR regolamenta il tutto nell'articolo 26 in cui vengono citati i contitolari del trattamento. Infatti, "allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. […] determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità […], con particolare riguardo all'esercizio dei diritti dell'interessato". Di conseguenza, tale soggetto, potrà esercitare i propri diritti nei confronti di ognuno dei contitolari. Infatti, requisito necessario rimane il fine comune, nel caso in cui i diversi contitolari perseguissero finalità diverse, non ci si troverebbe dinanzi a contitolarità. Quest'ultima sarebbe comunque fittizia anche in considerazione del fatto che possano essere utilizzati mezzi e modalità diversi in relazione alla responsabilità di ogni soggetto contitolare[82]. Dunque, eventuali problematiche ricorrerebbero in relazione, per l'appunto, al tema della responsabilità. È molto importante, in questi casi, cercare di comprendere a priori quale soggetto ricopra questo ruolo in modo tale da evincerne il possibile responsabile nel caso di violazione di dati personali. Per citare un esempio, in conseguenza al conflitto che, mentre si scrive, ha coinvolto Russia e Ucraina, Comune e Città Metropolitana di Venezia hanno implementato un portale online (affidandosi a soggetti esterni per la realizzazione) nel quale qualsiasi cittadino che avesse contribuito ad ospitare cittadini ucraini o comunque persone in fuga dalla guerra e giunte nel territorio comunale potesse

[82] Chiozzi, *La contitolarità o co-titolarità*, in PrivacyLab, 7 aprile 2022, https://www.privacylab.it/.

iscriversi tramite form per ricevere informazioni e agevolazioni (per esempio riguardanti il servizio di trasporti del Veneziano)[83].

Quanto appena analizzando rientra nella giurisdizione del Regolamento generale sulla protezione dei dati (EU), tuttavia un problema potrebbe sorgere nel caso in cui la condivisione di dati si attui in ottica extra-istituzionale e quindi verso paesi non comunitari (nei quali la disciplina del GDPR non è ovviamente applicabile). In questo frangente, non si può non fare riferimento alla c.d. sentenza Schrems II del 16 luglio 2020 che ha evidenziato la problematica relativa al fatto che i dati trattati da un paese europeo e successivamente inviati oltre il confine, risulterebbero di difficile (se non impossibile) controllo in chiave di trattamento. Tale sentenza prende il nome da un signore austriaco, tale Maximilian Schrems, che negli anni ha promosso campagne contro i colossi statunitensi come Google, Apple e Facebook impugnando il trattamento dei dati da loro effettuato, secondo lui non esente da violazioni rispetto alla normativa in materia di protezione dei dati personali[84]. Effettivamente, come sottolineato anche dal Commissario per la privacy della Columbia Britannica (Canada), il trattamento dei dati, una volta entrati in possesso di società statunitensi, sarebbe stato suscettibile di violazioni. Tutto ciò, con l'istituzione e l'introduzione del c.d. Patriot Act (acronimo di Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001[85]), quale legge federale in grado di rafforzare i poteri di spionaggio statunitensi in modo tale da intaccare la privacy dei cittadini, dopo l'attentato alle Torri Gemelle dell'11 settembre 2001, ora rimane ancor di più concettualmente lontano da quello che rappresenta il GDPR. Si pensi che nel maggio 2020 fu consentito all'FBI di acquisire la cronologia di navigazione di un soggetto senza la preventiva

[83] Dime, la città di Venezia per te, *Emergenza Ucraina*, in Comune di Venezia, 8 marzo 2022, https://live.comune.venezia.it/.
[84] Gruppo Privato del Comitato Scientifico ASSO DPO, *Schrems II: la sentenza che ha confermato la centralità del GDPR nella globalizzazione*, in Asso dpo, 22 dicembre 2020, https://www.assodpo.it/.
[85] Wikipedia, *USA PATRIOT Act*, in Wikipedia.org, 23 ottobre 2021, https://www.wikipedia.it/.

approvazione attraverso mandato del giudice. Alla luce di ciò, la Corte costituzionale europea ha stabilito che sia tra gli obblighi dell'esportatore (in tal caso paese europeo) verificare che, nel paese terzo in cui i suddetti dati saranno trasferiti, non vi sia violazione inerente al trattamento dei dati personali; è necessario, quindi, che vi sia una sorta di garanzia da parte di quest'ultimo al che venga fornito un confacente livello di protezione. In materia, in mancanza di adeguatezza, l'articolo 49 del GDPR ne disciplina l'esecuzione prevedendo deroghe in specifiche situazioni e condizioni, tra le quali se ne menzionano solo alcune[86]:

- L'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti;
- Il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento;
- Il trasferimento sia importante per motivi di interesse pubblico.

In altri termini, i dati personali delle persone interessate i quali vengano trasferiti da un Paese comunitario ad un Paese terzo, devono essere garantiti nel trattamento allo stesso modo sia dall'uno che dall'altro.

3.3.1 Caso Google Analytics: problematica trasversale in tema di tutela dei dati personali

Problematica di non poca rilevanza e soprattutto correlata con quanto detto nel precedente paragrafo è la questione riguardante i c.d. Google Analytics (GA) implementati dall'omonima azienda statunitense. Prima di continuare, è necessario analizzare con una breve disamina il ruolo che questi strumenti hanno nel panorama digitale legato ai dati personali. Principalmente, si tratta di un servizio gratuito offerto dal colosso Google a tutti i possessori di siti internet (ed in particolare, come si vedrà, utilizzato anche all'interno delle pagine web di enti

[86] Algolia, *GDPR*, https://gdpr.algolia.com/.

pubblici italiani) che si dirama in una serie di strumenti analitici (volti a generare analisi statistiche) atti a captare e annotare svariate informazioni con fini legati prettamente al marketing. Ci si riferisce, per esempio, al tracciamento dell'attività di un qualsiasi soggetto effettuata all'interno di un sito internet, dalla semplice ricerca del portale web alle pagine e servizi da questo cliccati con annessa individuazione di una molteplicità di dati riferiti alla persona stessa (dall'età anagrafica al luogo di provenienza). Tenendo conto di tutto ciò e in ottemperanza del Regolamento europeo sul trattamento dei dati personali, le informazioni fornite da Google Analytics potrebbero costituire fonte di incertezza con riguardo alle finalità che perseguono le Pubbliche Amministrazioni una volta entrati in possesso di questo tipo di dati. Dopo questa breve ma concisa introduzione ed esplicazione del ruolo di GA, è opportuno menzionare la nota diffida operata da MonitoraPA (Osservatorio Automatico Distribuito sulla PA). Tale soggetto vuole essere in grado di vigilare sul rispetto di quanto previsto dal GDPR per quanto riguarda la totalità dei portali istituzionali delle PA italiane[87]; successivamente all'emanazione della sentenza (Schrems II), ha deciso di segnalare illiceità in materia di trattamento dei dati personali (il Garante per la privacy italiano non si è ancora esposto, a differenza delle autorità francesi e austriache). Più nel dettaglio, sono quasi ottomila le Pubbliche Amministrazioni sollecitate da MonitoraPA tramite PEC, nel maggio 2022, sull'utilizzo illecito di GA e sulla loro successiva rimozione, altrettanti i diversi DPO (Data Protection Officer) che hanno dovuto rivedere alcune scelte riguardo alla composizione dei vari portali online istituzionali. La particolare colpa che si addossa all'azienda statunitense sull'utilizzo del proprio servizio è quella di trasferire i dati degli utenti al di fuori del territorio europeo (precisamente e in questo caso negli USA) senza quindi essere conformi a quanto disciplinato nel GDPR. Google Analytics,

[87] Tremolada, *La Pubblica amministrazione che usa Google Analytics rispetta le regole della privacy? L'iniziativa MonitoraPA spiegata bene*, in IlSole24Ore, 20 maggio 2022, https://www.infodata.ilsole24ore.com/.

precisamente, attua dei meccanismi di pseudonimizzazione in modo tale da oscurare una parte degli indirizzi IP[88] agli eventuali destinatari dei dati. Il problema sollevato dal gruppo di hacker, supportati dal Centro Hermes per la Trasparenza e i Diritti umani digitali[89] e da Copernicani[90], riguarda il fatto che tale procedura oscura gli indirizzi IP solamente nel momento in cui i dati giungono a destinazione. Rimane dunque evidente un possibile trattamento illecito di dati qualche istante prima che venga apportata la modifica agli indirizzi dei mittenti[91]. Concretamente, il problema era già stato sollevato nel gennaio scorso dalla società Venis S.p.A. (per mezzo del proprio DPO) in quanto si enunciava in una nota che, Google LLC violasse la normativa GDPR in quanto la tanto declamata anonimizzazione del soggetto privato e utente navigatore su un sito web, apportata dallo stesso Google, non risultava di fatto perfezionata; l'azienda statunitense sarebbe potuta risalire al soggetto in questione identificandolo grazie alla profilazione di (per citarne alcune) informazioni sul browser, selezione della lingua e indirizzo IP. È inoltre possibile, stando a quanto disposto dalle autorità, poter riconoscere un utente di un portale attraverso l'identificazione delle abitudini caratteristiche operata dai c.d. cookies. Viene quindi in rilievo come la materia analizzata possa essere relativamente sensibile. Stando al fatto che la molteplicità delle amministrazioni pubbliche (compresi soggetti privati ma comunque controllati da enti pubblici come è il caso di Venis S.p.A.), rilevate in circa 22 mila realtà da un report di MonitoraPA, usufruisca per la gran parte dei servizi suddetti, l'illecito trattamento o, per meglio dire, la non conformità di quest'ultimo al Regolamento europeo per la tutela dei dati

[88] Con indirizzo IP (dall'inglese Internet Protocol address) si intende un numero di pacchetto che identifica univocamente un dispositivo detto host collegato ad una rete informatica che utilizza l'Internet Protocol come protocollo di rete, fonte: Wikipedia.org.

[89] Organizzazione italiana per i diritti civili, promotore della consapevolezza alla trasparenza e all'accountability, https://www.hermescenter.org/.

[90] Advocacy group, di costituzione no-profit (2018), che ha un ruolo di impulso sui temi dell'innovazione, https://copernicani.it/.

[91] Ciurcina, *MonitoraPA, primo passo via Google Analytics dagli enti: cosa cambia*, in Cybersecurity360, 7 giugno 2022, https://www.cybersecurity360.it/.

personali creerebbe non pochi disagi in un futuro non molto lontano. Nonostante ciò, è stata suggerita una valida alternativa all'utilizzo di Google Analytics, ovvero Web Analytics Italia (WAI), che opera allo stesso modo. Si tratta di una piattaforma di raccolta e analisi di dati al fine di generare statistiche con riguardo al traffico generato dagli utenti fruitori di servizi digitali erogati dalla Pubblica Amministrazione, come i "cugini" GA, ma che, a differenza di questi ultimi, rispetterebbe il GDPR (essendo di base nazionale, i dati raccolti non verrebbero trasmessi fuori dal continente europeo, aspetto distintivo rispetto a GA). In conseguenza al molteplice invio delle PEC (menzionate prima), alcune PA hanno deciso di rivolgersi proprio a questo tipo di servizio di struttura nazionale perché, per l'appunto, figurato e indicato dalla stessa MonitoraPA.

Conclusioni

L'analisi che è stata fornita in questo testo ha portato e potrebbe portare in futuro a numerosi studi in ambito sia giuridico che informatico. Da una parte prospettando una tutela sempre più agguerrita e rigida della persona intesa come soggetto privato dotato di propria "privacy" che però tenga conto dei limiti imposti finora dalle differenze normative che si individuano tra legislatore italiano, che sembra voler restringere il campo d'azione del riutilizzo dei dati pubblici, e legislatore europeo, il quale sembra voler puntare sempre più al c.d. petrolio digitale (quest'ultimo però ritiene ancora necessario affidare eventuali decisioni sul consenso al trattamento ai vari Stati facenti parte della Comunità) e dall'altra riflettendo su un panorama, per certi versi futuristico, nel quale i diversi aspetti della vita di ogni individuo siano strettamente interconnessi tra di loro. È apparso chiaro come il tema della trasparenza amministrativa, quasi opposto a ciò che concerne il diritto di privacy, abbia sollevato numerose critiche che hanno però dato luogo a successivi aggiornamenti normativi. Tuttavia, tale principio, soprattutto in Italia, rimane ancora confuso in quanto se permangono delle differenze a livello di testi di legge tra ciò che prevede la normativa interna e ciò che invece propone il legislatore europeo, è altresì difficoltoso tentare di assimilare il tutto sotto un'unica visione comune. Per citare un esempio individuato da giuristi e inerente alle differenze normative tra i due legislatori summenzionati "l'imprecisione del coordinamento si manifesta in modo clamoroso nel curioso equivoco dei linguaggi: per la legge n. 241/1990 l'interessato è colui che chiede l'accesso, mentre il controinteressato è il titolare del diritto alla riservatezza; ma nel Codice della privacy l'interessato è proprio il soggetto cui si riferiscono i dati personali"[92]. Con ciò risulta necessaria una

[92] Sanna, *Il riutilizzo dei dati pubblici*, in Dalla trasparenza amministrativa ai dati aperti, Giappichelli Editore, Torino, 2018, p. 277.

rivisitazione dei testi normativi nell'ottica di ottenere, successivamente, una discrepanza minima tra i decreti interni e il Regolamento europeo.

Interessante è stato comprendere come anche in un semplice strumento di offerta di servizi quale è il portale Dime, persista un "dietro le quinte" che presenta numerose insidie. Dovendo gestire un'ampia mole di dati personali necessita di un apparato che sia capace di operare e gestire proattivamente eventuali minacce esterne. Il Dpo si è rivelato un soggetto fondamentale che, insieme allo strumento Dpia, si attiene ad obblighi specifici in grado di ricostruire la dinamica per la quale sono richieste determinate tipologie di dati.

Inoltre, con queste ultime righe, si vuole porre l'attenzione sui limiti che uno studio su privacy e trattamento dei dati possano incontrare. Paradossale quanto, allo stesso tempo, metaforicamente ricorsivo (privacy sulla privacy) è il fatto che comunque l'analisi su trasparenza e diritto al trattamento dei dati personali possa comportare la creazione di ostacoli, in termini di dati e informazioni richiesti ai quali non è consentito alcun tipo di accesso (o per lo meno, non valutabile in una tesi di laurea magistrale). Di conseguenza non è stato possibile procedere più approfonditamente con l'analisi. Nel terzo capitolo sarebbe stato utile esaminare ulteriormente il rapporto di "collaborazione" instaurato tra società in house e Pubblica Amministrazione. In quest'ultimo caso il limite temporale, inerentemente al tirocinio frequentato durante gli studi, ha giocato un ruolo importante poiché trattatosi di una cooperazione non instaurata in tempi recenti, lo studio non è riuscito a coprirne tutto l'arco duraturo del rapporto contrattuale tra Comune di Venezia e Venis S.p.A. Tuttavia, si è dedotto (anche attraverso documenti in possesso della società a cui si è fatto riferimento), contestualmente al titolo del corrente testo, come la nuova normativa sul trattamento dei dati personali, introdotta con il Regolamento UE n. 2016/679, abbia influito ampiamente sull'operato collaborativo apportando sostanziali novità; ad esempio lo strumento DPIA (Data Protection Impact Assessment) analizzato nel

terzo capitolo capace di fornire una prospettiva in termini preventivi di quali possano essere i rischi incombenti dal trattamento di dati richiesti da/in un servizio.

Da ultimo, rileva il fatto che la singola PA necessita quindi, al fine di salvaguardarsi e tutelarsi nei confronti di possibili ricorsi effettuati per istanza di soggetti privati e visto il susseguirsi delle obbligatorietà in termini di pubblicazione dei documenti, di un superlativo controllo su quanto verrà pubblicato. Una verifica effettuabile, fin dall'origine, attraverso diversi strumenti: dal privacy by design e by default alla completa gestione di un portale di accesso ai servizi digitali sempre più presente. In concreto, per evitare illecite fuoriuscite, si dovrà perciò prestare maggiore attenzione a tipologia e quantità di dati, contenuti nei documenti (richiesti), vista la loro possibile e successiva fruibilità da parte di un'illimitata platea.

Elenco delle figure

Bibliografia e sitografia

(s.d.). Tratto da La Pubblica Amministrazione digitale: https://www.lapadigitale.it

360, C. S. (2019, Maggio 3). *Servizi cloud e compliance GDPR: obblighi e soluzioni*. (M. Cosmi, A cura di) Tratto da CyberSecurity360: https://www.cybersecurity360.it

Algolia. (2022). *GDPR*. Retrieved from Algolia: https://gdpr.algolia.com

Altalex. (2019, Gennaio 14). *Art. 25 GDPR - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*. Tratto da Altalex: https://www.altalex.com

Andriani, G. (2020). *Il principio della trasparenza amministrativa tra nuove tecnologie e contrasto ai fenomeni corruttivi.* Roma: Aracne Editrice.

Assodpo. (2020, Dicembre 22). *Schrems II: la sentenza che ha confermato la centralità del GDPR nella globalizzazione*. (G. p. DPO, A cura di) Tratto da Assodpo: https://www.assodpo.it

Avvocato360. (2022). *Data breach: cosa significa e quali sono i rimedi?* Tratto da Avvocato360: https://avvocato360.it

Bolognini, L. (2021). *Privacy e libero mercato digitale.* Milano: Giuffrè Francis Lefebvre.

Bombardelli, M. (2017). *Istituzioni del Federalismo, rivista di studi giuridici e politici.* Maggioli Editore.

Butti , G. (2021, Maggio 11). *Le misure di sicurezza nel GDPR: quali sono, come applicarle, costi di attuazione*. Tratto da Network Digital 360: https://www.cybersecurity360.it

Camera dei deputati - Temi dell'attività parlamentare. (s.d.). Tratto da Diritto di accesso e trasparenza della pubblica amministrazione: https://temi.camera.it

Carta, A., & La Selva, P. (2019, Marzo 03). *Il responsabile trasparenza e anticorruzione (RPCT)*. Tratto da Ius in Itinere: https://www.iusinitinere.it

Chiozzi, A. (2022, Aprile 7). *La contitolarità o co-titolarità*. Tratto da Privacy Lab: https://www.privacylab.it

Colapietro, C. (2020, Maggio 13). Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione. *Federalismi.it - Rivista di diritto pubblico italiano, comparato, europeo*.

Compagnucci, C. (2022, Giugno 14). *Smart city 2020-2021 in Italia quali sono attualmente e in via di sviluppo*. Tratto da Business Online: https://businessonline.it

Coppola , S. (2018, Ottobre 24). *Il nuovo codice della privacy*. Tratto da La legge per tutti: https://www.laleggepertutti.it

D'Alterio , E. (2019, Gennaio). Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto". *Giornale di diritto amministrativo*.

Emanuele, L. G., & Pieremilio, S. (2019). *Privacy Digitale, riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy.* (E. Tosi, A cura di) Milano: Giuffrè Francis Lefebvre.

europea, C. (2022, Agosto 22). *European commission*. Tratto da Commissione europea: https://ec.europa.eu

Faini, F. (2016, Luglio 11). *Trasparenza della PA, tutto ciò che c'è da sapere sui nostri diritti*. Tratto da Agenda Digitale: http://www.agendadigitale.eu

Galetta, D. U., & Perin, R. C. (2020). *Il diritto dell'amministrazione pubblica digitale.* Giappichelli Editore.

Giustozzi, C. (2022). PA digitale talks. *Cosa devono fare le PA per contrastare gli attacchi ransomware?* (E. Belisario, Intervistatore, & B. Ernesto, A cura di) Tratto da https://www.spreaker.com

Hilbert, M., & Lopez , P. (2011). *The world's technological capacity to store.* California.

Il "nuovo" codice in materia di protezione dei dati personali. (s.d.).

Ius in itinere. (2020, Luglio 4). *L'origine della privacy e l'esigenza di tutelare i dati personali*. (F. Carlino, A cura di) Tratto da Iusinitinere.

Lexdo.it. (s.d.). *Chi è il Rappresentante del titolare e quando va nominato*. Tratto da Lexdo.it: https://www.lexdo.it

Marino, F. (2016, luglio 8). *I dati sono il nuovo oro nero, ecco cos'è per le aziende il petrolio digitale*. Tratto da Digitalic: https://www.digitalic.it

Ministero dell'Interno. (s.d.). Tratto da Ministero dell'Interno: https://www.interno.gov.it

Musci, A. (2022, Aprile 27). *L'accesso agli atti della PA è legittimo se sussista un interesse diretto e non leda la privacy.* Tratto da Anci, Associazione Nazionale Comuni Italiani: https://www.anci.it

O. Falk, T. (2020, Maggio 26). *I cyber-attacchi che plasmano la guerra di oggi*. Tratto da Insideover: https://it.insideover.com

PA, F. (2021, Novembre 23). *ICityRank, Rapporto annuale 2021, indice di trasformazione digitale*. Tratto da Forum PA: https://www.forumpa.it

Pizzetti , F. (2012). *Sette anni di protezione dati in Italia, un bilancio e uno sguardo sul futuro.* (F. Pizzetti, A cura di) Torino: Giappichelli Editore.

Prineos. (2022, Gennaio 28). *Breve storia della Privacy*. Tratto da Prineos: https://prineos.com

privacy, G. (s.d.). *Garante per la protezione dei dati personali, Valutazione d'impatto della protezione dei dati (DPIA)*. Tratto da Garante Privacy: https://www.garanteprivacy.it

Privacy.it. (s.d.). *Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006*. Tratto da Privacy.it: https://www.privacy.it

Report. (2021, 12 27). Report. *Smart TV: chi guarda chi?* (L. Paternesi, A cura di)

s.p.a., V. (2021). *Società trasparente*. Tratto da Venis S.p.a.: https://www.venis.it

s.p.a., V. (2022). *DPIA Whistleblowing.* Venezia.

Saetta, B. (2018, Giugno 14). *European Data Protection Board (ex WP29)*. Tratto da Protezione dati personali: https://protezionedatipersonali.it

Sanna, R. (2018). *Dalla trasparenza amministrativa ai dati aperti, opportunità e rischi delle autostrade informatiche.* Torino: Giappichelli Editore.

School, R. B. (2021, Giugno 17). *Privacy by design e by default*. Retrieved from Almalaboris: https://www.almalaboris.com

security, P. (2021, Settembre 23). *Attacco hacker alla Regione Lazio: cosa sappiamo e cosa ci insegna*. Tratto da Pandasecurity: https://pandasecurity.com

Simone, E. (s.d.). Tratto da Edizioni Simone: https://www.dizionari.simone.it

Simone, E. (2016, Febbraio 27). *Il diritto alla riservatezza*. Tratto da Laleggepertutti: https://www.laleggepertutti.it

Soldioggi. (2022). *Società in house 2022: cos'è e come funziona, requisiti, differenze*. Tratto da Soldioggi: https://www.soldioggi.it

Soro, A. (2021). La protezione dei dati personali nella PA digitale. (E. Belisario, Intervistatore, & E. Belisario, A cura di) Tratto da https://www.spreaker.com

Ufficiale, G. (s.d.). *Gazzetta ufficiale della Repubblica Italiana*. Tratto da Gazzetta ufficiale: https://gazzettaufficiale.it

Venezia, C. d. (2022, Marzo 8). *Emergenza Ucraina*. Tratto da Dime, La città di Venezia per te: https://live.comune.venezia.it

Venis S.p.A. (s.d.). *Privacy policy*. Tratto da Dime, La città di Venezia per te: https://dime.comune.venezia.it

Village, C. (2020, Marzo 29). *Big data e open data: definizione e figure professionali che se ne occupano*. Tratto da Communication village: https://www.communicationvillage.com

Wikipedia. (s.d.). *Wikipedia Italia*. Tratto da Wikipedia Italia: https://www.wikipedia.org

Zuddas, P., & Scagliarini, S. (2019). *Il "nuovo" codice in materia di protezione dei dati personali.* (S. Scagliarini, A cura di) Torino: Giappichelli Editore.