

TRASPARENZA AMMINISTRATIVA, ACCESSO E RIUTILIZZO DEI DATI PUBBLICI

Vademecum per la scelta dei dati da utilizzare
per la creazione di open data, la loro esposizione pubblica
nel rispetto dei limiti stabiliti da leggi e regolamenti
Accessibilità dei dati ed accesso agli atti

Sommario

PREMESSA	2
CAP. 1) EVOLUZIONE NORMATIVA E PRINCIPI FONDAMENTALI	3
<i>A) QUADRO NORMATIVO: DALL'ACCESSO AGLI ATTI ALL'ACCESSIBILITÀ TOTALE, DALL'ISTANZA DI PARTE AGLI OPEN DATA</i>	<i>3</i>
<i>B) PRINCIPIO DI TRASPARENZA</i>	<i>6</i>
<i>C) PRINCIPIO DI PROTEZIONE</i>	<i>7</i>
<i>PROTEZIONE DEI DATI PERSONALI</i>	<i>7</i>
<i>RISPETTO DELLE NORME IN MATERIA DI DIRITTO D'AUTORE.....</i>	<i>8</i>
<i>SEGRETO STATISTICO.</i>	<i>10</i>
<i>SEGRETO D'UFFICIO.....</i>	<i>10</i>
<i>SEGRETO DI STATO.....</i>	<i>11</i>
CAP. 2) DIRITTI DEI CITTADINI E DEI SOGGETTI GIURIDICI, DALL'ACCESSO SU ISTANZA DI PARTE ALL'ACCESSIBILITÀ TOTALE SU INIZIATIVA PUBBLICA	12
<i>A) ACCESSO DOCUMENTALE, ACCESSO CIVICO ED ACCESSO CIVICO GENERALIZZATO</i>	<i>12</i>
<i>B) DISPONIBILITÀ, ACCESSIBILITÀ E RIUTILIZZO SENZA LIMITI DEI DATI.....</i>	<i>13</i>
<i>C) UTILIZZO DI FORMATI CHE GARANTISCONO L'ACCESSO A TUTTI MEDIANTE L'UTILIZZO DI RETI IN FORMATO APERTO</i>	<i>14</i>
CAP. 3) MODALITÀ DI CREAZIONE, GESTIONE ED ORGANIZZAZIONE DELLE BANCHE DATI	16
<i>A) COME STRUTTURARE UN OPEN DATA: UN PERCORSO COMPLESSO TRA IL DOVERE DI RILASCIO DEI DATI (PSI) E IL RISPETTO DEI LIMITI NORMATIVI</i>	<i>16</i>
<i>B) UTILIZZO DI STANDARD CHE GARANTISCONO COMPLETEZZA, TEMPESTIVITÀ INTEROPERABILITÀ, ACCESSIBILITÀ, CONSERVAZIONE A LUNGO TERMINE, SICUREZZA</i>	<i>16</i>
<i>C) UTILIZZO DI DATI ANONIMIZZATI.....</i>	<i>17</i>
<i>D) GARANZIA DEI PRINCIPI DI NECESSITÀ E PROPORZIONALITÀ DELL'UTILIZZO DEI DATI.....</i>	<i>19</i>
CAP. 4) ACCESSO AGLI ATTI NELL'ERA DIGITALE	22
<i>A) ACCESSO DOCUMENTALE EX. ARTT. 22 SS. LEGGE N. 241/1990 E D.P.R N. 184/2006.....</i>	<i>22</i>
<i>B) ACCESSO CIVICO "SEMPLICE", OBBLIGHI DI PUBBLICITÀ E TRASPARENZA AI SENSI DEL D. LGS. 33/2013 E S.M.I.</i>	<i>23</i>
<i>C) ACCESSO CIVICO "GENERALIZZATO" EX D.LGS. 33/2013 COSÌ COME NOVELLATO DAL D.LGS. 97/2016</i>	<i>24</i>
<i>D) PRIVACY COME LIMITE ALL'ACCESSO AGLI ATTI DELLA P.A.</i>	<i>26</i>
<i>E) NORMATIVE A TUTELA DELLA PRIVACY E STRUMENTI GIURIDICI.....</i>	<i>28</i>
<i>F) PROFILI DI RESPONSABILITÀ PER VIOLAZIONE DELLA RISERVATEZZA DEI DATI PERSONALI ...</i>	<i>30</i>
<i>BIBLIOGRAFIA E SITOGRAFIA</i>	<i>32</i>

PREMESSA

Il presente documento si inserisce all'interno del progetto **GIOCO_nDA** (Gestione Integrata e Olistica del ciclo di vita degli open data) di cui Provincia di Brescia è partner insieme a Politecnico di Milano, Regione Lombardia, Provincia di Lecco, EasyGov srl, Fondazione Bruno Kessler, Varese Web, Scuola Universitaria professionale della Svizzera italiana (SUPSI), Università della Svizzera Italiana (USI).

Tale progetto, finanziato con i fondi del programma Interreg V-A Italia Svizzera - Asse 5 "Rafforzamento della Governance Transfrontaliera", ha l'obiettivo realizzare, tramite un portale dedicato e condiviso con il portale svizzero per gli open government data, un quadro informativo comune di dati di pubblico interesse su specifiche tematiche ritenute prioritarie, quali turismo, ambiente, lavoro e istruzione.

Provincia di Brescia, ha aderito al progetto in quanto già attiva nella tematica degli Open Data a seguito del recepimento delle indicazioni fornite dalla normativa nazionale e per adesione ad iniziative della Regione Lombardia.

Con riferimento alle azioni del progetto GIOCO_nDA e ai fini della facilitazione della raccolta del dato e condivisione dello stesso, Provincia ha realizzato un portale dedicato basato su software open source che, oltre alla pubblicazione dei dati, automatizza la raccolta degli stessi utilizzando sia basi dati interne che pubbliche (ad es. open data nazionali). Questo al fine di elaborare delle informazioni da rendere immediatamente e più facilmente disponibili per le azioni relative al progetto e nella fattispecie la piattaforma creata dai partner di progetto.

Gli strumenti prodotti nell'ambito di questa iniziativa (il presente vademecum, il portale e i manuali di utilizzo dello stesso) rappresentano, quindi, un punto di partenza per approfondire ed estendere al territorio il tema del dato e della sua importanza e come questo possa diventare, se ben usato, un elemento fondamentale per la pianificazione di strategie sociopolitiche ed economiche.

Come Pubblica Amministrazione Provincia ritiene che la diffusione di informazioni, utilizzando formati aperti (open data), sia in grado di aprire nuovi scenari e nuove opportunità sia in termini di maggiore trasparenza della pubblica amministrazione che di migliore accesso alle informazioni da parte dei cittadini/imprese.

Cap. 1) EVOLUZIONE NORMATIVA E PRINCIPI FONDAMENTALI

A) Quadro normativo: dall'accesso agli atti all'accessibilità totale, dall'istanza di parte agli Open

Data

- in ambito nazionale ed europeo:
 - Art. 97 Cost.;
 - Legge 633/1941;
 - Legge 241/1990;
 - D.Lgs. 196/2003 modificato dal D.Lgs. 101/2018 in recepimento del Regolamento UE n. 679/2016 - (GDPR);
 - Direttiva 2003/98/CE e norma di recepimento D.Lgs. 36/2006, modificate rispettivamente dalla Direttiva 2013/37/UE e dal D.Lgs. 102/2015; D.Lgs. 82/2005 (CAD) e successive modificazioni;
 - D.L.gs 33/2013 (decreto trasparenza) e successive modificazioni;
 - L. 35/2012; Deliberazione Garante della protezione dei dati personali n. 243/2014;
 - Piano Triennale per l'Informatica nella Pubblica Amministrazione;
- in ambito regionale e locale:
 - DGR Regione Lombardia n. XI/723 del 5.11.2018;
 - Determinazione Dirigenziale Provincia di Brescia n. 99/2015.

Per effetto delle vigenti disposizioni di legge i dati pubblici detenuti dall'Amministrazione e presenti nelle banche dati, prodotti o acquisiti nell'esercizio delle funzioni istituzionali, sono patrimonio della collettività, che ha diritto di accedervi e di riutilizzarli liberamente, nei limiti previsti dalla normativa stessa.

Con la crescita della digitalizzazione e la creazione di sempre più imponenti banche dati per la gestione di procedure riguardanti migliaia di utenti è sorto il problema di **organizzare ed implementare politiche, procedure, strutture, ruoli e responsabilità che delineano ed impongono l'adozione di regole, processi decisionali e responsabilità per una gestione efficace delle risorse informative (DAMA International – The Global Data Management Community).**

In applicazione di tale complesso normativo la Provincia di Brescia rende disponibili i dati pubblici detenuti nelle proprie banche dati, ne favorisce il libero riutilizzo a vantaggio della collettività per la creazione di opportunità economiche e per la promozione della partecipazione consapevole all'attività di gestione dell'interesse pubblico, nei limiti consentiti dalla legge.

A tal fine è stato messo a punto il portale open data “ALL DATA BRESCIA” (www.alldata.provincia.brescia.it) e il presente vademecum che concerne, secondo le disposizioni di legge riportate:

- a) **l’individuazione dei dati oggetto di pubblicazione e dei dati esclusi;**
- b) **la pubblicazione;**
- c) **il riutilizzo dei dati pubblici;**
- d) **le forme di accesso previste dall’ordinamento.**

L’esposizione trasparente di dati permette di dare supporto ad applicazioni con ricadute economiche e sociali con forte carattere di innovazione.

L’approccio basato su Open Data risulta sicuramente innovativo e risponde alle necessità di dare sempre maggiore trasparenza all’azione amministrativa, rafforzare le capacità di coordinamento e collaborazione delle PA e migliorare i processi di partecipazione degli stakeholder - imprese e società civile dei territori.

Tale processo di progressiva esposizione ed implementazione dei dati è oggi possibile grazie alla enorme spinta in avanti a livello normativo in materia di trasparenza amministrativa.

Prima fra tutte la **Legge n. 241/1990** ha introdotto nel nostro ordinamento giuridico i concetti di pubblicità e di trasparenza della Pubblica Amministrazione, declinandoli esclusivamente nella forma dell’accesso documentale o accesso agli atti, per cui solo chi ha un interesse diretto può visionare atti e documenti che lo riguardano.

La legge in questione, dunque, non prevede rilascio di dati ed informazioni che non siano parte di un documento e non prevede forme di accesso che consentano una conoscenza diffusa delle attività amministrative.

Ha inizio, pertanto, un processo di graduale apertura verso il rilascio sempre più consistente di dati ed informazioni, sia pure nel rispetto di posizioni giuridiche tutelate, quali ad esempio il diritto alla privacy nel trattamento dei dati personali.

Le disposizioni di interesse sono:

- **D.Lgs. 196/2003**, da ultimo modificato ed integrato in recepimento del Regolamento UE n. 679/2016 (GDPR), a norma del quale “Il trattamento dei dati personali avviene [...] nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.” (art. 1);
- **D.Lgs. 36/2006**, di recepimento della Direttiva 2003/98/C, da ultimo modificato dalla Direttiva 2013/37/UE e dal D.Lgs. 102/2015, con cui si stabiliscono “le modalità di riutilizzo dei documenti contenenti dati pubblici nella disponibilità delle pubbliche amministrazioni e degli organismi di diritto pubblico. “2. Le pubbliche amministrazioni e gli organismi di diritto

pubblico provvedono affinché i documenti cui si applica il presente decreto legislativo siano riutilizzabili a fini commerciali o non commerciali” (art. 1);

- **D.Lgs. n. 82/2005, modificato a più riprese e da ultimo con il D.Lgs. 217/2017** (Codice dell'Amministrazione Digitale), a norma del quale le pubbliche amministrazioni:
 - a) “utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione” (art. 12);
 - b) assicurano “la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale” (art. 2);
 - c) garantiscono che “i dati ... sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione da parte delle altre pubbliche amministrazioni e dai privati” (art. 50);
- **D.Lgs 33/2013** (T.U per la Trasparenza e Pubblicità) che ha introdotto l'*accesso civico*, ovvero quello cd. “semplice”, disciplinato dall'art 5, comma 1 e con la modifica di cui al **D.Lgs. 97/2016** (F.O.I.A.) ha introdotto una ulteriore tipologia di accesso civico, equivalente all'anglosassone “Freedom of Information Act”: l'accesso civico “generalizzato”, che costituisce l'espressione più alta del diritto all'informazione del cittadino, nello specifico disciplinato dall'art. 5, comma 2 del CAD, come modificato dal decreto legislativo **13 dicembre 2017, n. 217**, e le norme di recepimento e implementazione della direttiva INSPIRE e della direttiva Public Sector Information (PSI) che ci consentono di definire due ambiti strategici:
 1. condivisione dei dati tra PA, a titolo gratuito, per finalità istituzionali;
 2. riutilizzo dei dati, anche per finalità commerciali, da parte di portatori di interesse.

A completamento di questo percorso e al fine di dare concreta attuazione a questi principi, il Piano Triennale ha individuato due macro aree:

- basi di dati di interesse nazionale: la condivisione di dati delle PA per fini istituzionali va generalmente adottata per tutte le tipologie di dati per i quali tale politica è applicabile, nell'ambito di quanto previsto dall'articolo 50 del CAD;
- dati aperti: comunemente chiamati **Open data**, abilitano il riutilizzo dei dati da parte di chiunque e per qualunque scopo, anche commerciale, purché non vi siano particolari restrizioni (ad es. segreto di stato, segreto statistico, vincoli di protezione dei dati personali come definiti dal Garante della privacy).

B) Principio di trasparenza

La **Legge n. 241/1990** ha avuto il grande merito di sancire la fine del principio di segretezza, dando avvio ad un processo che porta da un sistema chiuso ed incentrato sul principio di riservatezza ad un sistema basato su principi di trasparenza e pubblicità dell'*agere publicum*, la cui espressione più importante è, tuttora, rappresentata dal diritto di accesso agli atti amministrativi.

Dagli anni '90 ad oggi, tuttavia, diverse sono state le modifiche legislative che hanno coinvolto l'istituto dell'accesso agli atti, passando per il D.Lgs. n. 33/2013, fino a giungere al D.Lgs. n. 96/2016.

La trasparenza consiste nella pubblicità di atti, documenti, informazioni e dati propri di ogni amministrazione, oggi facilitata dalla circolazione delle informazioni sulla rete internet a partire dalla loro pubblicazione sui siti istituzionali delle amministrazioni. Lo scopo ultimo è quello di favorire forme diffuse di controllo sull'azione amministrativa, sull'utilizzo delle risorse pubbliche e sulle modalità con le quali le pubbliche amministrazioni agiscono per raggiungere i propri obiettivi.

La norma di riferimento è il D.Lgs. 14 marzo 2013, n. 33 e le sue successive modificazioni, che costituisce un riordino generale delle disposizioni in materia di accesso e pubblicità.

L'art. 1, infatti, sancisce le regole di principio, secondo le quali:

- 1) “la trasparenza è intesa come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.”;
- 2) “la trasparenza, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali, concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione.”;
- 3) “essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino.”.

Tale evoluzione ha comportato il passaggio dall'accesso, tradizionalmente legato all'iniziativa della parte nell'ambito di un procedimento amministrativo ed ancorato a stringenti vincoli di legittimazione, che escludono esplicitamente un controllo generalizzato dell'attività dei pubblici uffici, alla accessibilità totale dei dati e dei documenti della P.A. che, per effetto di iniziativa della stessa Amministrazione, mette in campo un'attività di pianificazione per il rilascio dei dati di cui risulta titolare.

C) Principio di protezione

Disponibilità dei dati pubblici non significa però incondizionata condivisione di tutte le informazioni o accesso indiscriminato alle stesse.

I limiti alla conoscibilità dei dati sono quelli previsti dalle leggi e dai regolamenti vigenti anche con riferimento alla riservatezza dei soggetti a cui i dati si riferiscono (che andrà garantita ai sensi del D. Lgs. n. 196/2003, Codice in materia di protezione dei dati personali così come recentemente modificato ed integrato).

Del resto è la stessa norma sulla trasparenza a dettarne i limiti. In particolare, il già citato comma 2, dell'art. 1, D.Lgs. 33/2013 stabilisce che la trasparenza trova limite “nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali”. L'Amministrazione, quindi, nel processo di esposizione dei dati di cui è titolare per attività istituzionali, è tenuta a garantire, quale necessario contrappeso, la protezione di interessi che risultano meritevoli di attenzione e che, pertanto, vanno a bilanciare il diritto alla trasparenza.

Il principio di protezione impone rispetto della riservatezza degli individui e delle imprese per assicurare che le operazioni di apertura dei dati pubblici non avvengano in maniera indiscriminata.

Protezione dei dati personali.

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è in costante aumento. La tecnologia attuale infatti, consente ad imprese private ed autorità pubbliche di utilizzare in modo rilevante dati personali per lo svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

In materia la norma fondamentale è il D.Lgs. n. 196/2003, da ultimo modificato ed integrato in recepimento del Regolamento UE n. 679/2016 (GDPR), a norma del quale “Il trattamento dei dati personali avviene [...] nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.” (art. 1).

Il suo scopo è la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione Europea poichè, in quanto diritto fondamentale dei cittadini, deve essere garantito allo stesso modo in tutto il territorio dell'Unione.

Col Regolamento Europeo si passa da una visione proprietaria del dato - non lo si può trattare senza consenso -, ad una visione di controllo del dato al fine di favorirne la libera circolazione garantendo, al

contempo, i diritti dell'interessato, il quale deve sempre essere informato se i suoi dati sono usati e come vengono usati, per tutelare lui e l'intera collettività dai rischi insiti nel trattamento dei dati.

In materia di privacy, inoltre, numerosi ed importanti principi che possono guidare le Amministrazioni nella definizione delle soluzioni e delle modalità con cui procedere alla pubblicazione sono contenuti nella Deliberazione n. 88/2011 dell'Autorità Garante per la protezione dei dati personali.

La Deliberazione citata ha definito un primo quadro unitario di misure e accorgimenti che i soggetti pubblici sono tenuti ad applicare in relazione alle ipotesi di pubblicazione dei propri dati sul Web, per assicurare che la pubblicazione delle informazioni sia conforme alla normativa dettata in materia di protezione dei dati personali.

Tuttavia, la gran parte dei dati pubblici non possono essere classificati come personali, cioè non sono riconducibili ad un soggetto. In ogni caso, la privacy può essere efficacemente tutelata pubblicando i dati in forma anonima o comunque adottando tutte le cautele per evitare che i soggetti interessati possano essere identificati.

Per quanto sopra, il Garante ha statuito che “non si ravvisa la necessità di adottare alcuna specifica cautela qualora le pubbliche amministrazioni ritengano di pubblicare sul sito web informazioni non riconducibili a persone identificate o identificabili (ad esempio dati quantitativi aggregati per uffici riguardanti i livelli retributivi ed accessori risultanti dai contratti collettivi o da atti interni di organizzazione; tassi di assenza e di maggiore presenza del personale; informazioni relative alla performance dell'amministrazione; obiettivi assegnati agli uffici insieme ai relativi indicatori e ai risultati complessivi raggiunti; l'ammontare complessivo dei premi collegati alla performance stanziati e di quelli effettivamente distribuiti; dati relativi al grado di differenziazione nell'utilizzo della premialità, informazioni concernenti la dimensione della qualità dei servizi erogati, notizie circa la gestione dei pagamenti e le buone prassi)”.

In conclusione, le Amministrazioni – nell'attività di apertura dei dati che detengono – sono tenute ad adottare tutte le cautele necessarie per evitare la diffusione di dati personali non consentita dalla legislazione vigente, tuttavia senza pregiudicare le finalità di trasparenza e di comunicazione alla base dell'Open Data.

Rispetto delle norme in materia di diritto d'autore

Ulteriore profilo normativo in merito ai limiti da rispettare nell'ambito del processo di liberazione delle informazioni del settore pubblico è quello relativo alla legislazione in materia di diritto d'autore (Legge n. 633/1941).

Il diritto d'autore tutela le opere dell'ingegno dotate di creatività: dalle forme espressive di opere letterarie (come lettere, rapporti e guide), a quelle grafiche (come cartografie e grafici), passando per le raccolte ordinate di dati e informazioni o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo (banche dati o database). La normativa in materia di diritto d'autore si applica anche ai contenuti prodotti dal settore pubblico, salvo le eccezioni previste normativamente.

Per le banche dati, il legislatore dispone una doppia tutela, ovvero:

- A) il diritto esclusivo di eseguire o autorizzare la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo o forma, la traduzione, l'adattamento, e le modifiche, nonché qualsiasi tipo di distribuzione al pubblico dell'originale o di copie;
- B) il diritto di vietare le operazioni di estrazione o reimpiego di parti o della totalità della banca dati (c.d. diritto sui generis).

Particolare attenzione merita, inoltre, la norma dedicata alle opere realizzate dalle Amministrazioni con impegno di denaro pubblico: l'art. 11 Legge n. 633/1941 statuisce che "alle amministrazioni dello stato, alle province ed ai comuni spetta il diritto d'autore sulle opere create e pubblicate sotto il loro nome e a loro conto e spese".

L'applicabilità della normativa in materia di diritto d'autore ai dati generati e gestiti dalle Amministrazioni rappresenta un limite alla diffusione e al riutilizzo degli stessi sotto un duplice profilo:

- in primo luogo, l'Amministrazione dovrà porre particolare attenzione alla titolarità delle informazioni che intende pubblicare, evitando di ledere i diritti d'autore e/o altri diritti di privativa di soggetti terzi;
- in secondo luogo, nella pubblicazione l'Amministrazione dovrà adottare le licenze necessarie a evitare che l'esistenza del diritto d'autore e dei diritti connessi possa impedire, o comunque limitare, la possibilità utilizzare i dati stessi per scopi diversi da quelli istituzionali.

Segreto statistico; segreto d'ufficio; segreto di stato

Non esiste una definizione univoca e specifica del concetto di segreto. Il segreto è la relazione che intercorre tra la conoscenza di cose o fatti ed un determinato soggetto e, dunque, va inteso come il rapporto esclusivo di una persona con determinate informazioni.

Esistono nel nostro ordinamento delle figure codificate.

Segreto statistico.

Il segreto statistico, con lo scopo di aumentare la qualità dell'informazione statistica è regolamentato dall'art. 9 del DL n.322 del 6 settembre 1989, a norma del quale "I dati raccolti nell'ambito di rilevazioni statistiche comprese nel programma statistico nazionale da parte degli uffici di statistica non possono essere esternati se non in forma aggregata, in modo che non se ne possa trarre alcun riferimento relativamente a persone identificabili e possono essere utilizzati solo per scopi statistici. I dati di cui al comma 1 non possono essere comunicati o diffusi, se non in forma aggregata e secondo modalità che rendano non identificabili gli interessati ad alcun soggetto esterno, pubblico o privato, né ad alcun ufficio della pubblica amministrazione. In ogni caso, i dati non possono essere utilizzati al fine di identificare nuovamente gli interessati. In casi eccezionali, l'organo responsabile dell'amministrazione nella quale è inserito l'ufficio di statistica può, sentito il comitato di cui all'art.17, chiedere al Presidente del Consiglio dei Ministri l'autorizzazione ad estendere il segreto statistico anche a dati aggregati."

Inoltre al terzo comma dell'art.10 del DL n.281 del 30 luglio 1999, è specificato che "I dati personali trattati per scopi statistici e di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura".

Infine, l'art. 623 c.p. prevede il segreto scientifico o industriale ossia l'obbligo di mantenere la riservatezza su notizie relative a scoperte, invenzioni scientifiche o applicazioni industriali aventi natura di segreto di cui si ha conoscenza in ragione della propria funzione e punisce tali rivelazioni con la reclusione fino a due anni.

Segreto d'ufficio.

La legge 241/1990, all'art. 28, modificando l'art. 15, T.U. 3/1957 ha stabilito che "L'impiegato deve mantenere il segreto d'ufficio. Non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o concluse, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso. Nell'ambito delle proprie attribuzioni, l'impiegato preposto ad un ufficio rilascia copie ed estratti di atti e documenti di ufficio nei casi non vietati dall'ordinamento".

Nell'ambito dei delitti contro la Pubblica Amministrazione, contenuti nel Titolo II del Libro II del Codice Penale, l'art. 326 c.p. punisce, quando possa derivarne danno per l'amministrazione o per terzi, la rivelazione ed utilizzazione del segreto d'ufficio, ossia di tutte le informazioni o comunicazioni relative ad operazioni amministrative di qualsiasi natura e delle quali si sia venuto a conoscenza a causa del suo servizio o della sua funzione.

Segreto di Stato.

Nonostante la massima apertura, per interessi di rilievo superiore alcuni dati e/o documenti e/o provvedimenti che riguardano lo Stato devono essere esclusi dalla visione.

In tal senso si tratta di una limitazione stabilita per legge, ovvero ai sensi dell'art. 38, legge 124/2007, "Sono coperti dal segreto di Stato le informazioni, i documenti, gli atti, le attività, le cose o i luoghi la cui conoscenza, al di fuori degli ambiti e delle sedi autorizzate, sia tale da ledere gravemente le finalità di cui al comma 1."

E, pertanto, ai sensi del medesimo articolo, "Le informazioni, i documenti, gli atti, le attività, le cose e i luoghi coperti da segreto di Stato sono posti a conoscenza esclusivamente dei soggetti e delle autorità chiamati a svolgere rispetto ad essi funzioni essenziali, nei limiti e nelle parti indispensabili per l'assolvimento dei rispettivi compiti e il raggiungimento dei fini rispettivamente fissati. Tutti gli atti riguardanti il segreto di Stato devono essere conservati con accorgimenti atti ad impedirne la manipolazione, la sottrazione o la distruzione."

Rientrano in tale definizione gli atti, i documenti, le notizie, le attività e ogni altra cosa la cui diffusione sia idonea a recare danno all'integrità della Repubblica, anche in relazione ad accordi internazionali, alla difesa delle istituzioni poste dalla Costituzione a suo fondamento, all'indipendenza dello Stato rispetto agli altri Stati e alle relazioni con essi, alla preparazione e alla difesa militare dello Stato. La durata del vincolo è fissata in 15 anni, ulteriormente prorogabili dal Presidente del Consiglio, la durata complessiva non può essere superiore a 30 anni. La rivelazione di segreti di stato e la rivelazione di notizie di cui sia stata vietata la divulgazione sono punite penalmente.

Cap. 2) DIRITTI DEI CITTADINI E DEI SOGGETTI GIURIDICI, DALL'ACCESSO SU ISTANZA DI PARTE ALL'ACCESSIBILITÀ TOTALE SU INIZIATIVA PUBBLICA

A) Accesso documentale, accesso civico ed accesso civico generalizzato

L'**accesso documentale**, disciplinato dagli artt. 22 e ss. della L.241/1990, riconosce il diritto di visionare gli atti (ed eventualmente estrarne copia) del procedimento ai soggetti che detengono un interesse giuridicamente qualificato.

Si tratta, cioè, di un accesso ad atti, documenti, provvedimenti, inseriti in un procedimento amministrativo, la cui visione può essere riconosciuta solo a chi abbia una posizione di interesse qualificata, mediante attivazione di un procedimento specifico che viene avviato esclusivamente su istanza di parte (ad es. istanza di accesso agli atti nell'ambito di una Gara di Appalto da parte di un'impresa che vi ha partecipato; istanza di accesso alle prove concorsuali da parte di un candidato escluso dalla procedura; istanza di accesso agli atti di una procedura di trasferimento per un dipendente che non abbia ottenuto una assegnazione di sede pur avendone fatto richiesta).

Pertanto, alla luce dell'art. 22 co. 1 b) l. 241/90, la facoltà di accedere ai documenti detenuti dalla Pubblica Amministrazione non è attribuita a chiunque, ma unicamente ai soggetti titolari di una posizione differenziata e collegata ai documenti di cui si chiede la visione.

L'**accesso civico** è disciplinato dal D.Lgs. n. 33/2013 che ne ha introdotto nell'ordinamento italiano due tipologie: l'accesso civico "semplice", previgente alla Riforma del 2016 e l'accesso civico "generalizzato" introdotto dal decreto legislativo n. 97/2016.

L'accesso civico c.d. "semplice" è disciplinato dal comma 1 dell'art. 5 D.Lgs. 33/2013.

Diversamente dall'accesso documentale, in tale caso in capo al richiedente non vi è alcun onere di motivare l'istanza poiché oggetto della richiesta di ostensione sono quei documenti che devono essere pubblicati, per legge, dalle Pubbliche amministrazioni all'interno dell'apposita sezione "*Amministrazione trasparente*" presente sui siti istituzionali di ciascuna di esse. Si tratta cioè dell'accesso a quegli atti e a quei documenti di per sé pubblici ed in quanto tali conoscibili e fruibili gratuitamente da parte di "ogni cittadino" (ad es. in capo alle Pubbliche amministrazioni grava l'obbligo di pubblicare il *Curriculum Vitae* dei propri dirigenti per cui di fronte all'eventuale inadempienza "qualsiasi cittadino" è legittimato ad effettuare l'accesso civico al fine di richiedere che quel *Curriculum Vitae* sia definitivamente reso pubblico).

L'**accesso civico "generalizzato"** è frutto del riordino della disciplina sulla *trasparenza* operato dal Decreto Legislativo n. 97/2016, con cui il legislatore ha ritenuto opportuno introdurre una tipologia accesso civico, equivalente all'anglosassone *Freedom of information act* (FOIA) ed è disciplinato dal comma 2 dell'art. 5 del D.Lgs. 33/2013, come modificato dal D.Lgs. n. 97/2016.

Per effetto di tale norma chiunque e senza alcun onere motivazionale ha diritto di accedere ai dati ed ai documenti detenuti dalla P.A., ma che siano **ulteriori rispetto a quelli oggetto di obbligo di pubblicazione** ai sensi del D.Lgs. 33/2013 (ad es. secondo recentissima giurisprudenza dell'Adunanza plenaria del Consiglio di Stato si ritiene che anche gli atti di una gara di Appalto, con le eccezioni di cui all'art. 5-bis, commi 1 e 2 del d.l.gs 33/2013, possono essere oggetto di accessibilità totale da parte del cittadino – C.d.S. – A.P., Sent. n. 10/2020; ancor più recente il decreto del Consiglio di Stato, Sez. III, il quale, pur rinviando ad una discussione collegiale, ha già anticipato che qualora determinati atti non siano inclusi espressamente dal legislatore tra quelli sottratti all'accesso, la loro ostensibilità “secondo la regola generale, deve essere consentita” – C. di S. – Sez. III, n. 4574/2020).

Trattasi, dunque, di dati e documenti in relazione ai quali pur non sussistendo alcun obbligo di renderli pubblici, su richiesta devono essere forniti, nel rispetto dei limiti espressamente sanciti dal co. 5-bis del decreto citato.

Con l'accesso civico cambia la prospettiva ed il focus si sposta dalla tutela degli interessi individuali al controllo da parte del cittadino sull'attività amministrativa.

Il principio di accessibilità e pubblicità assume in tal modo rilevanza costituzionale in quanto attua i principi democratici di uguaglianza, buon andamento, efficacia e efficienza.

B) Disponibilità, accessibilità e riutilizzo senza limiti dei dati

Con la dottrina dell'Open Government tutte le attività dei Governi e delle Amministrazioni dello Stato devono essere aperte e disponibili, per favorire un controllo diffuso sulla gestione della cosa pubblica.

Per effetto di tale impostazione, si ridisegna il rapporto tra Pubblica Amministrazione e cittadino, passando da un approccio in cui il cittadino è fruitore di prestazioni erogate dall'Amministrazione ad uno basato su un processo di collaborazione reale, in cui il cittadino partecipa alle scelte di governo.

In tal senso, l'Open Government si basa su tre elementi:

- **Trasparenza:** le informazioni delle quali dispongono le Amministrazioni devono essere facilmente reperibili, riutilizzabili e aperte.
- **Partecipazione:** i cittadini devono essere coinvolti nei processi decisionali e potervi contribuire attivamente, anche grazie al ricorso alle tecnologie di comunicazione attualmente disponibili e diffuse.
- **Collaborazione:** coinvolgimento diretto dei cittadini nelle attività dell'Amministrazione.

In tale ottica l'Amministrazione rilascia dati aperti, ovvero “dati che presentano le seguenti caratteristiche:

- 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;
- 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti, sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;
- 3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione” art. 1, comma 1, lett. L ter, D.Lgs. 82/2005.

Inoltre, “I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico” (art. 50, comma 1, D.Lgs. n. 82/2005).

Per raggiungere gli obiettivi indicati le Amministrazioni:

- “utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione” (art. 12 D.Lgs. n. 82/2005);
- sono tenute ad assicurare “la disponibilità, la gestione, l’accesso, la trasmissione, la conservazione e la fruibilità dell’informazione in modalità digitale” (art. 2 D.Lgs. n. 82/2005).

I dati devono essere forniti a condizioni tali da permetterne il riutilizzo e la ridistribuzione. Ciò comprende la possibilità di combinarli con altre basi di dati.

Affinché i dati siano effettivamente aperti, gli utenti devono essere messi in condizione di riutilizzarli e integrarli, fino a creare nuove risorse, applicazioni e servizi di pubblica utilità.

C) Utilizzo di formati che garantiscono l'accesso a tutti mediante l'utilizzo di reti in formato aperto

I dati devono essere resi disponibili al maggior numero possibile di utenti senza barriere all'utilizzo, quindi preferibilmente attraverso il solo protocollo Hypertext Transfer Protocol (HTTP) e senza il ricorso a piattaforme proprietarie. Devono essere inoltre resi disponibili senza alcuna sottoscrizione di contratto, pagamento, registrazione o richiesta. Per garantire agli utenti la piena libertà di accesso e soprattutto di utilizzo e integrazione dei contenuti digitali, è necessario che i dati siano processabili in automatico dal



computer. I dati devono essere codificati in formati aperti e pubblici, sui quali non vi siano entità (aziende o organizzazioni) che ne abbiano il controllo esclusivo. Sono preferibili i formati con le codifiche più semplici e maggiormente supportati. Liberi da licenze che ne limitino l'uso, la diffusione o la redistribuzione.

Cap. 3) MODALITÀ DI CREAZIONE, GESTIONE ED ORGANIZZAZIONE DELLE BANCHE DATI

A) Come strutturare un open data: un percorso complesso tra il dovere di rilascio dei dati (PSI) e il rispetto dei limiti normativi

Ai sensi dell'art. 50, comma 2 bis, D.Lgs. n. 82/2005, "Le pubbliche amministrazioni, nell'ambito delle proprie funzioni istituzionali, procedono all'analisi dei propri dati anche in combinazione con quelli detenuti da altri soggetti di cui all'articolo 2, comma 2, fermi restando i limiti di cui al comma 1. La predetta attività si svolge secondo le modalità individuate dall'AgID con le Linee guida Indicazione delle fonti".

Il concetto di apertura dei dati va ben oltre quello di trasparenza. I dati pubblici hanno un potenziale enorme, che però non può esprimersi a pieno se i dati non vengono veramente aperti (full open data).

Con l'espressione dati aperti si fa riferimento alle informazioni detenute, prodotte e aggiornate dalle Pubbliche Amministrazioni rese disponibili gratuitamente per chiunque abbia interesse a riusarle.

Tutti i dati detenuti dagli enti pubblici e non soggetti a limitazioni per una delle ragioni previste dalle norme vigenti, possono essere esposti in formato aperto, attraverso l'attribuzione di una licenza aperta che ne permetta il riuso e la scelta di un formato tecnologico che sia a sua volta aperto e standardizzato.

L'accesso ai dati governativi aperti abilita la possibilità di trasformare la conoscenza detenuta dalle pubbliche amministrazioni in servizi immediatamente utilizzabili dai cittadini.

Per fare ciò non basta pubblicarli, ma occorre anche eliminare qualunque limitazione (giuridica, finanziaria o tecnologica) al loro riutilizzo da parte di altri.

B) Utilizzo di standard che garantiscano completezza, tempestività interoperabilità, accessibilità, conservazione a lungo termine, sicurezza

Nell'Art. 1 del Codice dell'Amministrazione Digitale (CAD), modificato dal D. Lgs. 217/2017, viene sancito al comma 1-ter che i dati si intendono open se "presentano le seguenti caratteristiche:

1. sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;
2. sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera l-bis), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;

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

Inoltre, per definirsi tali gli open data devono essere:

- ✓ **Completi**. Devono comprendere tutte le componenti che consentano di esportarli, utilizzarli online e offline, integrarli e aggregarli con altre risorse e diffonderli in rete;
- ✓ **Primari**. Devono essere presentati in maniera sufficientemente disgregata, per poter essere utilizzati dagli utenti per integrarli e aggregarli con altri dati e contenuti in formato digitale;
- ✓ **Tempestivi**. Devono essere resi pubblici tanto velocemente quanto è necessario per preservarne il valore;
- ✓ **Accessibili**. Devono essere trasmissibili e interscambiabili tra tutti gli utenti in rete direttamente attraverso i protocolli Internet, senza alcuna sottoscrizione di contratto, pagamento, registrazione o richiesta ufficiale;
- ✓ **Leggibili da computer**. Machine-readable, ovvero processabili in automatico dal personal computer;
- ✓ **Non proprietari**. Gli utenti devono poter utilizzare e processare i dati attraverso programmi, applicazioni e interfacce non proprietarie;
- ✓ **Liberi da licenze che ne limitino l'uso**. Ai dati non possono sottendere copyright o diritti intellettuali, né tantomeno brevetti che possano limitarne l'accesso e soprattutto l'utilizzo e il riuso degli utenti. Inoltre, i dati sono “aperti” se viene garantita agli utenti qualsiasi modalità di utilizzo, anche a scopi commerciali;
- ✓ **Riutilizzabili**. Gli utenti devono essere messi in condizione di riutilizzare e integrare i dati, sino a creare nuove risorse, applicazioni, programmi e servizi di pubblica utilità per la comunità di utenti;
- ✓ **Ricercabili**. Gli utenti devono poter ricercare con facilità e immediatezza dati e informazioni mediante strumenti di ricerca ad hoc, come database, cataloghi e motori di ricerca;
- ✓ **Permanenti**. Le peculiarità sino ad ora descritte devono caratterizzare i dati nel corso del loro intero ciclo di vita sul web.

C) Utilizzo di dati anonimizzati

Secondo il considerato n. 26 del Regolamento UE n. 679/2016 (GDPR) “È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su

una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca”.

Per quanto sopra, prima del loro utilizzo/rilascio i dati devono subire un trattamento per renderli anonimi.

Il GDPR si limita a definire (art. 32) alcuni punti per garantire la sicurezza dei trattamenti, ma lascia ai titolari e ai responsabili del trattamento una certa libertà di scelta in merito agli accorgimenti tecnici da impiegare.

Per anonimizzazione si intende una tecnica che viene applicata ai dati personali in modo tale che le persone fisiche non possano più essere identificate in nessun modo: l'obiettivo è ottenere una de-identificazione irreversibile. Requisito fondamentale è che i dati personali siano stati inizialmente raccolti, trattati e conservati in conformità alla normativa vigente, con riferimento ai principi applicabili al trattamento e alla liceità dello stesso, ai sensi degli artt. 5 e 6 del GDPR.

Se l'anonymizzazione è andata a buon fine, i dati oggetto dell'operazione non sono più classificati come dati personali e quindi non sono più soggetti alla normativa sulla protezione dei dati personali.

La pseudonimizzazione è definita, nel disposto dell'art. 4 Punto 5 del GDPR come “il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive [...]”.

Con questa operazione si sostituiscono alcuni identificatori con pseudonimi realistici, ma non veritieri. I dati originali vengono conservati in un database separato costituito da una tabella delle corrispondenze al fine di poter risalire (di re-identificare) le persone fisiche. Si tratta di un processo reversibile che, pertanto, comporta l'applicazione del GDPR.

La pseudonimizzazione non è un metodo di anonimizzazione e l'art. 32, comma 1, lett. a) del GDPR cita questa misura tecnica, definendola appropriata “per garantire un livello di sicurezza adeguato al rischio”.

D) Garanzia dei principi di necessità e proporzionalità dell'utilizzo dei dati

Il principio di necessità, insieme a quello di proporzionalità, è parte integrante della struttura del GDPR ed informa ogni attività di elaborazione dei dati personali. Ciò significa che i dati utilizzati devono essere limitati a quelli strettamente necessari rispetto allo scopo per cui gli stessi sono raccolti (scopo che deve, inoltre, essere stato precisamente comunicato prima della raccolta agli interessati). Se dei dati personali non servono, non devono neppure essere raccolti.

Il GDPR invece non parla esplicitamente di principio di necessità, ma di minimizzazione del trattamento, che ne costituisce una sottocategoria, e che richiede che i dati personali debbano sempre essere “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati”. Ne consegue che in ogni trattamento dovranno essere raccolti solo i dati strettamente indispensabili. Questo non significa che i titolari non possano raccogliere altri dati o trattarli in modo diverso, ma per ciascuno di essi occorrerà ottenere il consenso dell'interessato o basarsi su un'altra delle condizioni di liceità previste dal Regolamento.

Di fatto, i confini di ciascun trattamento vanno tracciati facendo riferimento ad una serie di elementi strettamente connessi tra loro, tra cui le finalità perseguite, la quantità e la tipologia di dati raccolti, il periodo e le modalità di conservazione degli stessi, e sostanzialmente riassunti nei principi elencati all'art. 5 del GDPR, il quale fa espresso riferimento alla necessità di limitare, sotto diversi aspetti volta per volta rilevanti, i dati trattati.

Poiché la finalità perseguita va comunicata all'interessato, il titolare, prima ancora di raccogliere i dati, dovrà individuare con estrema precisione:

- 1) quali sono i dati essenziali per quello specifico trattamento;
- 2) che quel trattamento sia effettivamente necessario per il raggiungimento dello scopo;
- 3) che quella finalità non sia raggiungibile con altri mezzi, ragionevolmente applicabili nel contesto di riferimento.

Fatta questa attenta analisi, il titolare dovrà fare in modo, anche avvalendosi di apposite misure tecniche e organizzative, di ridurre al minimo il trattamento dei dati personali nel suo complesso.

Dunque, una volta raggiunto lo scopo per cui i dati sono stati raccolti, il titolare non potrà più conservare tali informazioni.

Di conseguenza, ogni utilizzo di dati superfluo o eccedente, perché non essenziale per le finalità previste ed espressamente comunicate all'interessato o non necessario per integrare una delle condizioni di liceità del trattamento (ad esempio, per adempiere un preciso obbligo di legge) o, ancora, perché esteso a dati non rilevanti o per un periodo di tempo eccessivo, sarà quindi considerato illecito e violativo del GDPR ed esporrà il titolare alle pesanti sanzioni previste dal Regolamento.

E) Portale open data ALL DATA BRESCIA - note tecniche

Il portale alldata.provincia.brescia.it è stato realizzato utilizzando la piattaforma DKAN, strumento drupal-based per la pubblicazione, catalogazione la visualizzazione di open data.

TECNOLOGIA UTILIZZATA

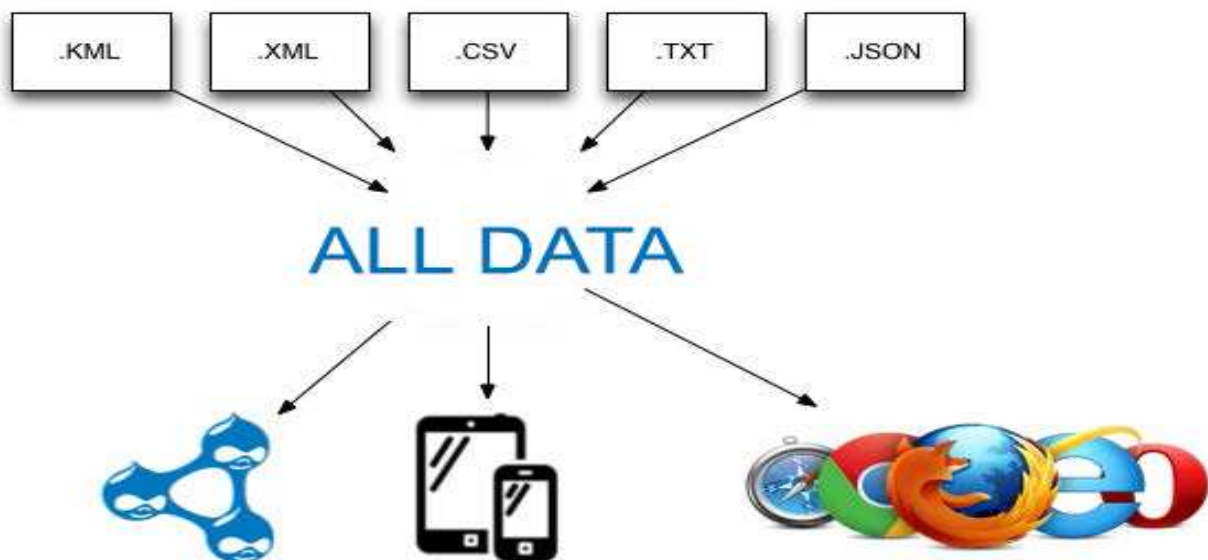
- Drupal-based
- Drupal Entity API
- JQuery,Drupal AJAX framework.
- MySQL, MariaDB, PostrgeSQL
- Licenza GNU GPL

DKAN + DRUPAL

La piattaforma DKAN è un potente strumento di pubblicazione dati in formato open, integra funzionalità di catalogo open data e i dataset sono trattati come contenuti dal CMS (Content Management System) e possono essere gestiti come tali.

Drupal offre agli amministratori un'interfaccia utente per tutte le attività di gestione del portale, mentre i redattori dei contenuti hanno la possibilità di inserire i dati open utilizzando un solo tool.

OVERVIEW SUI COMPONENTI



- Utilizza google flotcharts per la manipolazione on site dei dati (grafici).
- SEO Ready.
- Save as draft dei datasets.
- Gestione completa delle revisioni dei datasets e delle risorse.

- Possibilità di categorizzare i redattori e i datasets per gruppi (es. dataset turismo).
- Possibilità di gestire dei dati di grandi dimensioni con l'utilizzo della libreria plupload.
- Front end in responsivedesign basato sul framework bootstrap 3
- Integrazione Drupal - APACHE Solr Search
- Implementazione copertura area geografica dei dati e filtro per area geografica.

In merito alle modalità di funzionamento del portale, si rinvia allo specifico Manuale Utente che viene pubblicato e reso disponibile sul portale.

Cap. 4) ACCESSO AGLI ATTI NELL'ERA DIGITALE

A) Accesso documentale ex. artt. 22 ss. Legge n. 241/1990 e D.P.R n. 184/2006

Il diritto di accesso documentale è riconosciuto a chiunque abbia un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento oggetto della richiesta di accesso, ed è consentito in conformità a quanto previsto dalla Legge, dai Regolamenti, dal Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003 e s.m.i. — Regolamento UE 2016/679).

Costituiscono oggetto del diritto di accesso tutti i documenti amministrativi materialmente esistenti al momento della richiesta e detenuti alla stessa data dall'Amministrazione, in originale o in copia, fermi restando i casi di differimento e/o di esclusione.

In merito al differimento, il Responsabile del procedimento può posticipare temporaneamente l'accesso agli atti o documenti qualora dalla diffusione possa derivare pregiudizio alla riservatezza di persone fisiche o giuridiche, indicandone le ragioni e il termine massimo di differimento, ovvero per salvaguardare specifiche esigenze dell'Amministrazione, sia nella fase preparatoria dei provvedimenti, sia in relazione a documenti a cui conoscenza possa compromettere il buon andamento dell'azione amministrativa.

Tra i documenti per i quali è previsto il differimento, si intendono ricompresi tutti quelli che possono essere resi temporaneamente non accessibili nei seguenti casi:

- a) quando risulta una necessità oggettivamente comprovata di non pregiudicare la predisposizione o l'attuazione di atti e provvedimenti anche in relazione ad attività di verifica, di ispezione, di contestazione o di applicazione di sanzioni;
- b) nelle ipotesi previste dal Codice dei contratti (art. 53, comma 2, del D.Lgs. 50/2016 e s.m.i.);
- c) relativamente a procedure concorsuali, selettive o di avanzamento, fino all'esaurimento dei relativi procedimenti, quando il differimento è necessario per non pregiudicare o ritardare li loro svolgimento;
- d) quando i documenti contengono dati personali in relazione ai quali, in conformità alla normativa vigente in materia di trattamento e libera circolazione dei dati personali e tutela della privacy, risulti necessario non pregiudicare lo svolgimento di investigazioni difensive o l'attività necessaria per far valere o difendere un diritto in sede giudiziaria;
- e) quando concernono attività di controllo interno ed attività ispettive, fino alla conclusione dei relativi procedimenti.

Per quanto riguarda i documenti sottratti all'ostensione, l'accesso è escluso con provvedimento motivato nei casi indicati dall'art. 24, comma 1, della L. 241/1990 e s.m.i., nei casi cioè in cui una norma di legge, sulla base di una valutazione preventiva e generale, per tutelare interessi prioritari e

fondamentali di terzi, persone, gruppi e imprese, dispone sicuramente la non ostensibilità di dati, documenti e informazioni ovvero la consente secondo particolari condizioni, modalità e/o limiti.

Tali esclusioni possono essere assolute e ricorrono: a) in caso di documenti oggetto di segreto di Stato o di classifica ai sensi della L. 124/2007 e s.m.i., del D.P.C.M 0611.2015 n. 5 e di ulteriori disposizioni attuative; b) nei procedimenti tributari; c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione; d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

Le esclusioni possono essere relative e consistono nei limiti posti a tutela di interessi pubblici e privati di particolare rilievo giuridico elencati ai commi 1 e 2 dell'art. 5-bis del Decreto Trasparenza, nonché nelle ipotesi previste dal Codice dei contratti (artt. 53⁹ commi 5 e 162 — cd. contratti secretati - del D.Lgs. 50/2016 s.m.i.). Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dalla normativa vigente in materia di trattamento e libera circolazione dei dati personali e tutela della privacy.

Sono sempre escluse le istanze di accesso preordinate a un controllo generalizzato dell'operato dell'Ente.

In caso di diniego dell'accesso, espresso o tacito, o di differimento dello stesso ai sensi dell'articolo 24, comma 4, della L. 241/90 e s.m.i., l'istante può presentare ricorso al Tribunale Amministrativo Regionale competente nel termine di trenta giorni dalla conoscenza della decisione impugnata o dalla formazione del silenzio rigetto secondo quanto disposto dall'art. 116 del Codice del processo amministrativo (D.Lgs. n. 104/2010).

B) Accesso civico “semplice”, obblighi di pubblicità e trasparenza ai sensi del d. lgs. 33/2013 e s.m.i.

L'Amministrazione garantisce, attraverso il sito istituzionale, l'accessibilità dei dati e dei documenti detenuti ai fini della trasparenza delle informazioni e del controllo diffuso sulle attività istituzionali e sull'utilizzo delle risorse pubbliche.

L'istituto è disciplinato dal comma 1 dell'art. 5, D.Lgs. 33/2013, che stabilisce che l'obbligo in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.

L'esercizio dell'accesso civico non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente; chiunque può esercitare tale diritto indipendentemente dall'essere cittadino italiano.

Il Responsabile verifica la fondatezza dell'istanza di accesso civico semplice ed è tenuto a concludere il procedimento con provvedimento espresso e motivato nel termine di trenta giorni dalla presentazione della istanza, con la comunicazione al richiedente.

In caso di istanza fondata l'Amministrazione provvede alla pubblicazione del dato/documento/informazione richiesto, indicandone all'interessato il relativo collegamento ipertestuale.

Nel caso in cui il dato/documento/informazione richiesto risulta essere già pubblicato sul sito dell'Ente nel rispetto della normativa vigente, l'Amministrazione comunica la già avvenuta pubblicazione, indicando il collegamento ipertestuale al dato/documento/informazione pubblicato.

Il Responsabile del procedimento ha l'obbligo di segnalare, in relazione alla loro gravità, i casi di inadempimento o adempimento parziale all'Ufficio disciplina, ai fini dell'eventuale attivazione del procedimento disciplinare; la segnalazione degli inadempimenti viene effettuata anche al vertice politico dell'amministrazione e all'organismo indipendente di valutazione ai fini dell'attivazione delle altre forme di responsabilità.

Nell'ipotesi di accesso civico semplice in caso di ritardo o mancata risposta o diniego il richiedente può ricorrere al titolare del potere sostitutivo, che conclude il procedimento di accesso civico semplice, entro i termini di cui all'art. 2, comma 9-ter della legge 241/1990.

In caso di persistente inerzia e comunque avverso la decisione dell'Amministrazione, il richiedente potrà proporre ricorso al Tribunale Amministrativo Regionale ai sensi dell'art. 116 del decreto legislativo 2 luglio 2010, n. 104".

C) Accesso civico "generalizzato" ex D.Lgs. 33/2013 così come novellato dal D.Lgs. 97/2016

L'accesso civico generalizzato, ai sensi dell'art. 5 co. 2, D.Lgs. 33/2013 prevede che "allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti."

In merito a tale ultima disposizione si è fatto riferimento ad un *Freedom of Information Act*, per sottolineare il cambio di rotta effettuato in materia di trasparenza amministrativa.

L'istanza di accesso civico, la quale può essere trasmessa anche in via telematica, pur non richiedendo alcuna motivazione, in ogni caso, deve indicare i dati, le informazioni o documenti richiesti.

Il Responsabile del procedimento se individua soggetti controinteressati, ai sensi dell'art. 5 bis comma 2 del Decreto Trasparenza, ne dà comunicazione agli stessi. La predetta comunicazione avviene mediante invio di copia dell'istanza.

Sono controinteressati tutti i soggetti (persone fisiche o giuridiche) che, anche se non indicati nel documento cui si vuole accedere, potrebbero vedere pregiudicati interessi coincidenti con quelli indicati dal comma 2 dell'articolo 5-bis del Decreto Trasparenza (protezione dei dati personali, libertà e

segretezza della corrispondenza, interessi economici e commerciali, come chiarito dalle Linee guida ANAC).

E' opportuno che il Responsabile del procedimento indichi nella comunicazione ai controinteressati le modalità di presentazione dell'eventuale opposizione all'accesso. Il Responsabile del procedimento deve dare informazione al richiedente l'accesso civico generalizzato della individuazione di soggetti controinteressati e della sospensione del termine di 10 giorni, decorrenti dalla ricezione della comunicazione da parte dei predetti controinteressati.

Il soggetto controinteressato può presentare una eventuale e motivata opposizione, anche con modalità telematiche, all'istanza di accesso civico generalizzato, entro 10 giorni dalla ricezione della comunicazione della predetta richiesta di accesso.

Il procedimento di accesso civico generalizzato deve concludersi - in caso di accoglimento, diniego, differimento o limitazione - con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza, con la comunicazione del relativo esito al richiedente e agli eventuali soggetti controinteressati. Il predetto termine resta sospeso nel caso di comunicazione dell'istanza di accesso civico generalizzato ai controinteressati durante il tempo stabilito dalla norma per consentire agli stessi di presentare eventuale opposizione.

In caso di accoglimento dell'istanza, il Responsabile del procedimento provvede alla comunicazione dell'accoglimento ed alla trasmissione al richiedente dei dati, delle informazioni o dei documenti richiesti.

Qualora i controinteressati presentino opposizione e l'Amministrazione ritenga, anche sulla base della valutazione del bilanciamento degli interessi contrapposti, comunque di accogliere la richiesta di accesso, ne dà avviso ai controinteressati medesimi e provvede a trasmettere al richiedente i dati e/o i documenti richiesti, decorsi almeno 15 gg dalla ricezione della comunicazione da parte del controinteressato.

L'accesso civico generalizzato è rifiutato qualora ciò sia necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici riguardanti:

- a) la sicurezza pubblica e l'ordine pubblico;
- b) la sicurezza nazionale;
- c) la difesa e le questioni militari;
- d) le relazioni internazionali;
- e) la politica e la stabilità finanziaria ed economica dello Stato;
- f) la conduzione di indagini sui reati e il loro perseguimento;
- g) il regolare svolgimento di attività ispettive.

L'accesso civico è, altresì, rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi privati relativi a:

- a) la protezione dati personali, in conformità con la disciplina legislativa in materia;
- b) la libertà e la segretezza della corrispondenza;
- c) gli interessi economici e commerciali di persona fisica e giuridica compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

L'accesso civico generalizzato è, inoltre, escluso nei casi di segreto di Stato e negli altri casi di divieti di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della Legge n. 241 del 1990 e s.m.l..

Se i limiti citati riguardano soltanto alcuni dati o alcune parti del documento richiesto, deve essere consentito l'accesso agli altri dati o alle altre parti.

Per la definizione delle esclusioni all'accesso generalizzato si applicano, inoltre, le Linee guida recanti indicazioni operative adottate dall'Autorità Nazionale Anticorruzione ai sensi dell'art. 5-bis del Decreto Trasparenza.

Il differimento dell'accesso civico generalizzato — previsto dall'ad. 5-bis, comma 5, del Decreto Trasparenza — è ammesso soltanto quando ricorrano cumulativamente due condizioni: a) che l'accesso possa comportare un pregiudizio concreto a uno degli interessi pubblici o privati di cui ai commi 1 e 2 dell'art. 5-bis del Decreto Trasparenza; b) che quel pregiudizio abbia carattere transitorio. Il differimento dell'accesso deve essere motivato con riferimento ai casi e ai limiti stabiliti dall'art. 5-bis del Decreto Trasparenza.

Il rifiuto, il differimento e la limitazione dell'accesso civico, al di fuori delle ipotesi previste dall'articolo 5-bis del Decreto Trasparenza, costituiscono elemento di valutazione della responsabilità dirigenziale, eventuale causa di responsabilità per danno all'immagine dell'Amministrazione.

Nell'ipotesi di accesso civico generalizzato, nei casi di diniego totale o parziale o di mancata risposta entro il termine previsto dalla legge il richiedente può proporre, entro 30 gg. dalla conoscenza della determinazione impugnata o dalla formazione del silenzio, ricorso al Tribunale Amministrativo Regionale ai sensi dell'articolo 116 del decreto legislativo 2 luglio 2010, n. 104.

D) Privacy come limite all'accesso agli atti della P.A.

Trasparenza e riservatezza costituiscono i due estremi tra cui è necessario trovare un difficile punto di equilibrio che soddisfi interessi, apparentemente, inconciliabili.

Diritto d'accesso e diritto alla riservatezza condividono il medesimo ambito di applicazione, costituendo l'uno il limite dell'altro.

Il diritto di accedere ai dati in possesso della Pubblica Amministrazione contrasta con il diritto dei terzi a non veder divulgate informazioni a loro inerenti, almeno quando non sia possibile adoperare forme che garantiscano la irriducibilità delle stesse ad un soggetto determinato o determinabile. Tale diritto al riserbo, pur essendo riferibile anche a persone giuridiche (si pensi all'interesse a mantenere segreti alcuni dati che costituiscono il *know how* dell'impresa), assume ben più delicata pregnanza in relazione a persone fisiche.

Il legislatore, nel tentativo di risolvere tale rapporto dicotomico, ha emanato una serie di principi-guida, contenuti nella L. 241/1990 e nel c.d. Codice sulla *privacy* (D.Lgs. 196/2003 così come modificato dal D.Lgs. 1010/2018), con cui ha fissato un punto di equilibrio dinamico, e non statico, tra i due contrapposti interessi.

Infatti, dal combinato disposto delle due normative emerge una graduazione del diritto d'accesso, calibrata sulla tipologia di dati personali oggetto di tutela.

L'art. 24 co. 7 della L. 241/1990 riconosce in via generale la prevalenza del diritto d'accesso, disponendo appunto che "deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici", prevedendo tuttavia che "nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'art. 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale".

Di contro, il richiamato art. 60 del Codice della *privacy* dispone che "quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale". Questa impostazione trova ulteriore conferma anche nell'art. 59 del medesimo Codice, a tenore del quale "fatto salvo quanto previsto dall'art 60, i presupposti, le modalità, i limiti per l'esercizio del diritto d'accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990 n. 241, [...]. I presupposti, le modalità e limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33."

Dunque, le facoltà concesse dal diritto di accesso diminuiscono proporzionalmente al crescere del carattere strettamente personale dei dati, fino ad imbattersi in stringenti limiti innanzi a quelli che vengono comunemente definiti "dati super sensibili" o "sensibilissimi". L'altalenante equilibrio tra gli interessi in gioco riveste un ruolo sempre più cruciale in una società altamente variegata e iperconnessa come quella (post) moderna, di cui l'amministrazione deve farsi abile interprete.

E) Normative a tutela della privacy e strumenti giuridici

Nell'alluvionale, spesso caotica, produzione legislativa inerente alla tutela della riservatezza, un solido cardine normativo è individuato nell'art. 2 della Costituzione, il quale, pur non disciplinando espressamente la materia qui in oggetto, essendo qualificato come norma a "fattispecie aperta", si presta a fungere da argine ad ogni tipo di situazione che possa ledere i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali.

La lungimiranza dei Costituenti si adatta alla contemporaneità ove, l'imperante uso di nuove tecnologie, ha reso il tema della tutela della *privacy* una tra le problematiche più ostiche, sia dal punto di vista economico che morale, cui la società è chiamata a fornire una soluzione.

Preliminarmente è opportuna una precisazione terminologica, *privacy* e riservatezza non sono sinonimi. Il diritto alla riservatezza consiste nel diritto di escludere che terzi vengano a conoscenza dei propri dati personali in senso lato, *ius excludendi alios*.

Il diritto alla *privacy*, invece, costituisce un'estensione ed una specificazione del primo, tutela infatti quei dati che possono rilevare l'identità di un individuo, la sua sfera più intima.

Il rapporto tra i due termini, ed i relativi concetti, è "di genere a specie".

Ciò specificato, punto di riferimento nella normativa regolante la tutela della *privacy* è il già citato Regolamento europeo n. 679/2016 (GDPR), un atto, dunque, *self executing*, dotato di efficacia diretta all'interno degli ordinamenti degli stati membri dell'UE, a seguito del quale è stato emanato il D.Lgs. n. 101/2018, col dichiarato intento di armonizzare il già vigente Codice della *privacy* (D.Lgs. n. 196/2003) con la normativa sovranazionale.

Anche il Garante della *privacy*, autorità indipendente introdotta con la L.674/1996, il quale svolge funzioni di vigilanza sulle attività inerenti al trattamento dei dati personali, posto a presidio delle pretese che i titolari dei medesimi possono avanzargli, ha visto modificata, ampliata, la propria sfera di operatività a seguito dell'adeguamento alla normativa europea, al fine anche di addivenire ad una collaborazione attiva tra soggetti regolanti e regolati. L'interessato, persona fisica, infatti, in quanto titolare dei dati, vanta una ampia gamma di strumenti giuridici tesi a garantire che le informazioni ad esso inerenti siano trattate in ottemperanza alle stringenti regole europee, dal cui mancato rispetto deriva la facoltà, oltre a quella di ricorrere alle ordinarie forme di tutela amministrative e giudiziarie, di rivolgersi al Garante stesso. Innanzi a quest'ultima autorità l'interessato può far ricorso a due strumenti di tutela: il reclamo e la segnalazione.

Mediante il reclamo, ai sensi dell'art. 77 GDPR e degli artt. 14 bis e ss. del Codice della *privacy*, attraverso un'esposizione dettagliata dei fatti e delle norme che si presumono violate, può chiedere una verifica all'Autorità, a cui fa seguito un'istruttoria preliminare, prodromica ad un eventuale procedimento amministrativo formale.

Secondo il disposto dell'art. 144 del Codice della *privacy*, invece, "chiunque può rivolgere una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui

all'articolo 58 del Regolamento”, norma, quest’ultima, ove si disciplinano gli ampi poteri di indagine, correttivi, autorizzativi e consultivi concesse all’autorità di controllo.

Tutto ciò premesso e considerato, il più importante dei diritti di cui l’interessato è titolare è quello di esprimere il proprio consenso al trattamento dei dati, a seguito di un’esaustiva informativa di cui egli deve essere destinatario. L’interessato infatti attraverso la manifestazione della propria volontà acconsente affinché le informazioni ad esso inerenti possano essere oggetto di trattamento, consenso che può essere revocato in qualsiasi momento.

Inoltre, gli artt. da 15 a 22 del GDPR prevedono una serie di diritti che completano lo spettro di facoltà riconosciute al titolare dei dati, nello specifico è previsto un:

- a) **diritto di accesso**, ossia ad ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali, oltre ad una serie di informazioni espressamente individuate;
- b) **diritto alla portabilità dei dati**, dunque il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento, con conseguente diritto di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li aveva originariamente forniti. Tale diritto è esercitabile solo se il trattamento è basato sul consenso o su un contratto, e sia effettuato con mezzi automatizzati;
- c) **diritto di opposizione**, attraverso cui è possibile opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano;
- d) **diritto a non essere sottoposto a decisioni automatizzate**, ossia il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che sia in grado di produrre effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Stringenti eccezioni tuttavia ne limitano l’area di operatività.

Se i summenzionati diritti e facoltà possono essere facilmente azionabili con risultati soddisfacenti, ben più complesso e arduo è far valere quello che è stato definito diritto all’oblio. Con questa espressione si fa riferimento al diritto di veder cancellate le informazioni presenti sul *web* che possano in vario modo ledere la dignità e la reputazione di un individuo, chiedendo pertanto la rimozione dai motori di ricerca di ogni *link* ricollegabile all’argomento in questione. E’ facilmente intuibile che nonostante le intenzioni dei legislatori una siffatta richiesta incontra ostacoli tecnici difficilmente sormontabili affinché si addivenga ad una piena soddisfazione della stessa.

F) Profili di responsabilità per violazione della riservatezza dei dati personali

Il GDPR pone grande attenzione al tema della responsabilizzazione di coloro i quali sono, a vario titolo, coinvolti nella gestione di dati personali, infatti dedica l'intero capo IV, intitolato "Titolare del trattamento e responsabile del trattamento", a questo fondamentale argomento.

La figura apicale in tale contesto è rappresentata dal titolare del trattamento, il quale ai sensi dell'art.4 viene definito come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

Il titolare del trattamento, dunque, assume un'ampia e piena responsabilità sulla trattazione dei dati, egli è tenuto a mettere in atto "misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al [...] regolamento", adottando "misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati", dovendo garantire, inoltre, che vengano adoperati "solo dati personali necessari per ogni specifica finalità del trattamento" (artt. 24-25).

Il titolare del trattamento è coadiuvato da una figura dallo stesso nominata, il responsabile del trattamento, ossia "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i dati personali per conto del titolare" (art. 4).

Il responsabile è una figura tecnica, in possesso di quelle competenze professionali che gli consentono di assolvere i propri compiti rispettando gli standard fissati dal GDPR, ha obblighi distinti da quelli del titolare, in particolare egli deve occuparsi:

- a) della tenuta del registro dei trattamenti svolti (art. 30);
- b) dell'adozione di idonee misure tecniche ed organizzative per garantire la sicurezza dei trattamenti (art. 32);
- c) la degnazione di un RDP – DPO (Responsabile Protezione dei Dati), nei casi previsti (art. 37).

Il GDPR ha introdotto, altresì, la facoltà per il responsabile di nominare un **sub-responsabile** per lo svolgimento di specifiche attività, del cui operato egli risponde, salvo che riesca a dimostrare che l'evento dannoso non gli sia in alcun modo imputabile.

Il Regolamento, pertanto, come esaurientemente esposto sul sito istituzionale del Garante della privacy, pone l'accento sull'accountability (responsabilizzazione) «di titolari e responsabili, ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento. Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (articolo 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto previsto dall'articolo 25, paragrafo 1, del Regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari: ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati».

Nel caso in cui si verifichi una violazione dei dati personali, un c.d. data breach, tale da pregiudicarne la riservatezza e l'integrità, il titolare deve darne comunicazione al Garante della privacy entro 72 ore dal momento in cui ne abbia avuto conoscenza.

La previsione delle responsabilità menzionate trova compimento nell'art. 82 GDPR, il cui tenore letterale prevede espressamente che "chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento."

Da quanto sopra esposto, risulta chiaro come l'articolato impianto normativo adottato in sede europea abbia come fine l'adeguamento delle tutele predisposte a protezione della privacy alla mutevole società digitale.

BIBLIOGRAFIA E SITOGRAFIA

1. Agid.gov.it. 2020. *Il Piano Triennale Per L'informatica Nella PA 2019-2021* | Agenzia Per L'italia Digitale. [online] Available at: <<https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/08/12/il-piano-triennale-linformatica-nella-pa-2020-2022>> [Accessed 8 July 2020].
2. Agid.gov.it. 2020. *Piano Triennale - Razionalizzazione Del Patrimonio ICT*| Agenzia Per L'italia Digitale. [online] Available at: <<https://www.agid.gov.it/it/infrastrutture/razionalizzazione-del-patrimonio-ict>> [Accessed 6 July 2020].
3. Autorità Nazionale Anticorruzione, delibera del 28 dicembre 2016, n. 1309. Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del D.Lgs. 33/2013.
4. Azienditalia, 2018. *Disambiguazione e post verità nelle comunicazioni degli Enti Pubblici*. [online] (6/2018), pp.861-868. Available at: <<http://www.edicolaprofessionale.com/azienditalia>> [Accessed 1 July 2020].
5. Bobbio, N. and Revelli, M., 2011. *Democrazia E Segreto*. Torino: Einaudi.
6. Cantone, R., 2020. *Il Sistema Della Prevenzione Della Corruzione*. 1st ed. Giappichelli, 2020.
7. Carloni, E. and Falcone, M., 2017. *L'EQUILIBRIO NECESSARIO PRINCIPI E MODELLI DI BILANCIAMENTO TRA TRASPARENZA E PRIVACY*. Diritto pubblico, (3).
8. Colapietro, C., 2016. *La "Terza Generazione" Della Trasparenza Amministrativa*. Napoli: Editoriale scientifica.
9. Colapietro, C. and Ruotolo, M., 2014. *Diritti E Libertà*. Torino: G. Giappichelli.
10. Consiglio di Stato, Sent. 2 aprile 2020, n. 10. Accesso agli atti della fase esecutiva di un contratto pubblico da parte di un concorrente alla gara – Ammissibilità dell'accesso civico generalizzato. Available at: https://www.giustizia-amministrativa.it/web/guest/dcsnpr?p_p_id=GaSearch_INSTANCE_2NDgCF3zWBwk&p_p_state=normal&p_p_mode=view&_GaSearch_INSTANCE_2NDgCF3zWBwk_javax.portlet.action=searchProvvedimenti&p_auth=vvWYKxEX&p_p_lifecycle=0 [Accessed 4 July 2020].
11. Consiglio di Stato, sez. III, decreto del 31 luglio 2020, n. 4574. Giustizia Amministrativa - DCSNPRR. [online] Available at: https://www.giustizia-amministrativa.it/web/guest/dcsnpr?p_p_id=GaSearch_INSTANCE_2NDgCF3zWBwk&p_p_state=normal&p_p_mode=view&_GaSearch_INSTANCE_2NDgCF3zWBwk_javax.portlet.action=searchProvvedimenti&p_auth=vvWYKxEX&p_p_lifecycle=0 [Accessed 1 September 2020].
12. Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Art. 10. *Libertà di espressione*.
13. Corrado, A. and Cerasaro, E., 2018. *Conoscere Per Partecipare*. Napoli: Edizioni Scientifiche Italiane.
14. Corte Costituzionale, Sent. 21 febbraio 2019, n. 20. *Giudizio di legittimità costituzionale in via incidentale – Dirigenti delle pubbliche amministrazioni - Dirigenti delle pubbliche amministrazioni - Obblighi di pubblicazione dei compensi di qualsiasi natura percepiti nonche' di dati relativi al reddito e al patrimonio personali e degli stretti congiunti. - Decreto legislativo 14 marzo 2013, n. 33 (Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni), art. 14, commi 1-bis e 1-ter. - (T-190020). GU 1° Serie Speciale, Corte Costituzionale n.9 del 27-02-2019*

15. Corte Costituzionale, Sent. 3 luglio 1956, n. 11. *Giudizio di legittimità costituzionale in via incidentale – leggi anteriori alla costituzione - competenza esclusiva della corte.* GU 1° Serie Speciale, Corte Costituzionale n.168 del 7-7-1956
16. Decreto legislativo del 25 Maggio 2016, n.97, *recante revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza correttivo della legge 6 novembre 2012, n. 190 e del decreto 14 marzo 2013, n.33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.* GU Serie Generale n.132 del 08-06-2016
17. Decreto legislativo del 2 luglio 2010, n. 104, *Attuazione dell'articolo 44 della legge 18 giugno 2009, n. 69, recante delega al governo per il riordino del processo amministrativo.* GU Serie Generale n. 156 del 07-07-2010
18. Decreto legislativo del 14 marzo 2013, n. 33, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.* GU Serie Generale n.80 del 05-04-2013
19. *dirittodellinformatica.it - Rivista telematica su diritto e tecnologia.* 2018. *GDPR: Quando Un Trattamento È Necessario E Come Minimizzare I Dati Trattati* (Guida Al GDPR 2.5) - *Dirittodellinformatica.It - Rivista Telematica Su Diritto E Tecnologia.* [online] Available at: <<http://www.dirittodellinformatica.it/privacy-e-sicurezza/gdpr/gdpr-quando-un-trattamento-e-necessario-e-come-minimizzare-i-dati-trattati-guida-gdpr-2-5.html#:~:text=Il%20GDPR%20invece%20non%20parla,5%2C%20co.>> [Accessed 8 July 2020].
20. *Federalismi.it - Rivista di diritto pubblico italiano, comparato, europeo.* 2015. *Fascicolo N. 10/2020.* [online] Available at: <<https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=41987>> [Accessed 07 July 2020].
21. *Federalismi.it - Rivista di diritto pubblico italiano, comparato, europeo.* 2016. *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del D. Lgs. n. 33/2013.* [online] Available at: <<https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=31502>> [Accessed 5 July 2020]
22. Foà, S., 2017. *La nuova trasparenza amministrativa.* *Diritto amministrativo*, (1), pp.65-99.
23. *Foia.gov.it.* 2020. *Pareri Garante Privacy In Tema Di Accesso Civico Generalizzato | FOIA Centro Nazionale Di Competenza.* [online] Available at: <<https://www.foia.gov.it/pareri/>> [Accessed 6 July 2020].
24. *Foia.gov.it.* FOIA- Centro Nazionale Di Competenza. *FOIA: la trasparenza come regola* [online] Available at: <<https://www.foia.gov.it/>> [Accessed 3 July 2020].
25. Gardini, G. and Magri, M., 2019. *Il FOIA Italiano.* Santarcangelo di Romagna (Rimini): Maggioli.
26. *Giurdanella.it.* 2018. *Accesso Civico Generalizzato E Accesso Tradizionale, Le Differenze.* [online] Available at: <<https://www.giurdanella.it/2018/07/24/accesso-civico-semplific-generalizzato-accesso-tradizionale-la-differenza/>> [Accessed 4 July 2020].
27. Loiodice, A., 1969. *Contributo Allo Studio Sulla Libertà D'informazione.* Napoli: Jovene.
28. Mattarella, B., 2018. *Lezioni Di Diritto Amministrativo.* Torino: G. Giappichelli.
29. Miele, G., 1959. *Questioni vecchie e nuove in materia di distinzione del diritto dall' interesse nella giustizia amministrativa.* Tipografia del Babuino.

30. Mise. n.d. *Cosa Sono Gli Open Data*. [online] Available at: <<https://www.mise.gov.it/index.php/it/open-data/cosa-sono-gli-open-data>> [Accessed 1 September 2020].
31. Open Government Partnership Italia. 2020. *Il 4° Piano D'Azione Nazionale Per L'Open Government 2019 – 2021*. [online] Available at: <<http://open.gov.it/attuazione-quarto-nap/>> [Accessed 9 July 2020].
32. Pagnanelli, V., 2020. Immuni: spunti per una riflessione privacy-oriented. *Questione Giustizia*, [online] (5/2020). Available at: <<http://www.questionegiustizia.it/stampa.php?id=2506>> [Accessed 1 September 2020].
33. Pagnanelli, V., 2016. Accesso, accessibilità, Open Data. Il modello italiano di Open Data pubblico nel contesto europeo (*Giornale di Storia Costituzionale* n. 31/2016). *giornale di storia costituzionale / journal of constitutional history*, (31), pp.205-219.
34. Sandulli, M. A. , 2000. *L'accesso alle notizie e ai documenti amministrativi*, in *Enc. del dir. Aggiornamento*, Milano, Giuffrè, 2000.
35. Sandulli, A. M., 1978. *La libertà d'informazione. Iustitia*. 1, pp. 1-33.
36. Spasiano, M. R., 2015. *Riflessioni in tema di trasparenza anche alla luce del diritto di accesso civico*. *Nuove autonomie*. n. 1/2015, p. 63-80
37. TAR Lazio, sez. II Bis, sentenza del 02 luglio 2018, n. 7326. *Giustizia Amministrativa - DCSNPRR*. [online] Available at: <https://www.giustizia-amministrativa.it/web/guest/dcsnpr?p_p_id=GaSearch_INSTANCE_2NDgCF3zWBwk&p_p_state=normal&p_p_mode=view&_GaSearch_INSTANCE_2NDgCF3zWBwk_javax.portlet.action=searchProvvedimenti&p_auth=BM7wSOoB&p_p_lifecycle=0> [Accessed 4 July 2020].