PRIVACY

E

PUBBLICAZIONE DEGLI ATTI CONSILIARI

INDICE

PARTE PRIMA

PARTE SECONDA

“Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro. […]

Emerge un legame profondo tra libertà, dignità e privacy, che ci impone di guardare a quest´ultima al di là della sua storica definizione come diritto ad essere lasciato solo.

Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d´essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale dalla società dell’eguaglianza.

Senza una forte tutela dei dati riguardanti le convinzioni politiche o l’appartenenza a partiti, sindacati, associazioni, i cittadini rischiano d´essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione.”[1]

Stefano Rodotà

[1] Tratto da *Privacy, libertà, dignità*, discorso conclusivo della 26^ Conferenza internazionale sulla protezione dei dati, 2004, www.garanteprivacy.it.

PARTE PRIMA

1. Privacy: concetto, legislazione e principi

Secondo alcuni studiosi, le origini del concetto di *privacy* risalgono alla cultura ellenica, mentre la dottrina prevalente tende a ricondurre la nascita della nozione di *privacy* alla fine della società feudale e all'emergere della classe e della cultura borghese.[2]
Nell'evoluzione del concetto di *privacy* e del diritto alla riservatezza, è fondamentale la prima teorizzazione del cosiddetto "diritto a essere lasciati soli", risalente al saggio *The Right to privacy*, apparso il 15 dicembre 1890 sulla *Harvard Law Review*. Gli autori – i due giovani avvocati bostoniani, Samuel Warren e Louis D. Brandeis - furono dunque i primi a concepire il diritto alla solitudine ("*the right to be let alone*"), moderna formula dello "*ius solitudinis*".

Il diritto a essere lasciati soli coincideva con il diritto ad avere uno spazio vitale (anche fisico) dal quale potere escludere gli altri, a loro volta tenuti a rispettare questa individualità. Si trattava, quindi, della teorizzazione di un diritto a contenuto negativo (mantenere riservate alcune informazioni), piuttosto che a contenuto positivo (esercitare un controllo sulle stesse).
Il recente progresso scientifico, sociale, culturale, economico e, soprattutto, tecnologico attraverso il diffuso utilizzo della rete internet, ha modificato profondamente il significato del concetto di *privacy*, che oggi indica il diritto alla protezione delle informazioni che ci riguardano e, quindi, il diritto alla tutela dei dati personali.

Nell'attuale società dell'informazione e della comunicazione – opportunamente definita "webcentrica" – si registra un impatto dirompente sulle modalità e sull'intensità del trattamento dei dati personali. I cosiddetti operatori del *web* possono, invero, ottenere i dati personali degli utenti tramite ogni strumento a loro disposizione (i propri siti *web*, i *browser*, le *app*, ecc.).[3]

---

[2] Per una ricostruzione storica del concetto di privacy, è possibile consultare l'articolo *L'origine della privacy e l'esigenza di tutelare i dati personali*, Fabrizio Carlino, 2020, www.iusinitinere.it.

[3] Per un approfondimento, è possibile consultare l'Indagine conoscitiva sul settore dei servizi internet e sulla pubblicità online dell'Autorità per le garanzie nella comunicazione (AGCOM), 2014, www.agcom.it.

In tale contesto, è evidente che aumenta esponenzialmente la possibilità di analisi, indicizzazione e utilizzo dei dati. Ecco perché si parla di "*big data*": un patrimonio gigantesco di informazioni di diversa natura, in grado di circolare con straordinaria velocità, tale da consentirne un'elaborazione che inevitabilmente incide sui processi decisionali e, talvolta, ne agevola l'automatizzazione, grazie alle grandi possibilità di combinazione di dati e alle analisi predittive dei comportamenti.[4]

Al legislatore spetta quindi il compito di disciplinare le modalità con le quali i singoli possono controllare le informazioni che essi stessi hanno prodotto e condiviso, più o meno consapevolmente. Su quest'ultimo aspetto, è emblematico il cosiddetto "paradosso della *privacy*", ovvero il rapporto - spesso non pienamente congruente - tra i propositi di ciascuno e gli effettivi comportamenti in tema di riservatezza e protezione dei propri dati personali.[5] Dal concetto di privacy, si è quindi giunti alla più ampia nozione di "protezione dei dati" e alla necessità di stabilire regole generali sulla circolazione delle informazioni.

Una disciplina sulla protezione dei dati personali e tutela della riservatezza è, pertanto, utile sia a permettere a ciascuno di decidere se e quali dati fornire, per quali finalità, per quanto tempo, ecc., sia a consentire che i cosiddetti titolari del trattamento possano raccogliere dati veritieri. La legislazione in materia di *privacy* - volta anche a conformare l'impiego delle tecnologie digitali a finalità rispettose dei diritti della persona - consente quindi un pieno sviluppo della personalità, a vantaggio dell'intera collettività e rappresenta una condizione necessaria alla tutela dei valori di libertà, dignità e uguaglianza.

Il diritto alla protezione dei dati personali consiste nella raccolta e nel trattamento lecito delle informazioni su una persona fisica individuata o individuabile, la quale ha facoltà di esercitare un controllo su tali dati e sui flussi informativi che li riguardano; non si esercita,

---

[4] Per un approfondimento, è possibile consultare l'Indagine conoscitiva sui *Big Data* dell'Autorità per le garanzie nella comunicazione (AGCOM), 2020, www.agcom.it.

[5] Per un approfondimento, si rimanda all'analisi *Il prezzo dei dati personali: cosa c'è dietro il "paradosso della privacy"*, Francesca Michetti, 2019, www.agendadigitale.eu.

pertanto, il diritto "negativo" a non subire interferenze nella propria vita privata (diritto alla riservatezza), ma piuttosto il diritto "positivo" a controllare la circolazione delle proprie informazioni personali.

Attraverso le parole di Stefano Rodotà - primo Presidente dell'Autorità Garante per la protezione dei dati personali e già Presidente del Comitato europeo dei Garanti per la *privacy* – si può cogliere appieno l'evoluzione del concetto di *privacy* e del diritto alla riservatezza: "*Con le banche dati, le reti, la tv via cavo e anche le tecnologie genetiche – che sono in gran parte raccolte di informazioni sulle persone – il diritto di privacy non è più soltanto quello di essere lasciato solo, ma anche, e soprattutto, quello di controllare il destino delle informazioni che circolano sul proprio conto.*"

1.1. La legislazione sulla tutela della *privacy*

In Italia, - in virtù del principio della preminenza dell'*acquis* comunitario - le norme europee non solo si aggiungono al diritto interno, ma prevalgono su di esso, a condizione che siano rispettati i principi fondamentali dell'ordinamento e i diritti inalienabili della persona.

Le fonti della legislazione sulla tutela della *privacy* si rinvengono, quindi, sia nell'ordinamento europeo, sia in quello statale. Già nel 1995, il legislatore europeo emana la cosiddetta direttiva madre in materia di *privacy*: la direttiva 95/46/CE del Parlamento europeo e del Consiglio, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, recepita dal legislatore italiano con la legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali). Qualche anno dopo, in considerazione dell'avvento e della diffusione del *web*, il legislatore europeo adotta anche la direttiva cosiddetta *e-privacy*: la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

Conseguentemente, il legislatore italiano provvede ad emanare una normativa di recepimento coordinato di entrambe le direttive, approvando il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), che, tra le altre cose, abroga la legge 675/1996.

Solo nel 2016 l'Unione europea si dota di una nuova normativa sulla *privacy* e lo fa compiendo una scelta significativa: approva ed emana un regolamento che – a differenza

delle precedenti direttive – è direttamente applicabile a tutti gli Stati membri rendendo così la disciplina uniforme in tutta l'Unione europea; il 24 maggio 2016 entra, pertanto, in vigore il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora in poi **GDPR, *General data protection regulation***), che sarà pienamente applicabile dal 25 maggio 2018.

Il GDPR stabilisce norme relative alla protezione di diritti e libertà fondamentali delle persone fisiche, in relazione al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati (art. 1, par. 1 - 3). Si applica al trattamento, automatizzato o meno, di dati personali, con alcune eccezioni espressamente previste, tra le quali si annovera il trattamento di dati anonimi e quello effettuato da persone fisiche nell'ambito di attività esclusivamente personali o domestiche (art. 2, par. 1- 4). Il legislatore italiano ha quindi provveduto ad adeguare la normativa statale al GDPR, aggiornandola e, in parte, abrogandola, in particolare con il decreto legislativo 10 agosto 2018, n. 101 .
La vigente normativa statale in materia di *privacy* è, quindi, recata nel summenzionato decreto legislativo 196/2003, cosiddetto *codice privacy*, come modificato e aggiornato.
Si rammenta, inoltre, che il Comitato europeo per la protezione dei dati (*European Data Protection Board,* EDPB, organo europeo indipendente) emana periodicamente apposite linee guida (comprensive di raccomandazioni e migliori pratiche) proprio ai fini della corretta, coerente e uniforme interpretazione e applicazione delle norme.

Il legislatore europeo, con il GDPR, si prefigge di corroborare il diritto del cittadino alla protezione dei propri dati personali, rendendo ancora più stringenti gli obblighi dei cosiddetti titolari del trattamento e di superare l'obsolescenza delle norme previgenti, non adeguate al mutato contesto.

1.2. La definizione di dato personale e di categorie particolari

Per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile, il cosiddetto interessato (art. 4).

Il legislatore riserva un regime di tutela più pervasivo alle cosiddette categorie particolari di dati personali, afferenti a informazioni che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché a dati

genetici, biometrici e relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona (art. 9, par. 1).

Una maggiore tutela è prevista anche per i dati personali relativi alle condanne penali e ai reati, per i quali il trattamento deve avvenire soltanto sotto il controllo dell'autorità pubblica o, se è autorizzato dal diritto dell'Unione o degli Stati membri, prevedendo garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica (art. 10).

1.3. La definizione di trattamento

Per trattamento si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali. Per trattamento si intende, quindi, la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati (art. 4).

1.4. L'architettura dei ruoli previsti dal GDPR

[6] Immagine tratta dalle schede tecniche fornite nell'ambito del corso *on-line Il nuovo Regolamento europeo 679/2016 sulla protezione dei dati personali*, a cura di Ernesto Belisario, Formazione Maggioli.

Il titolare del trattamento è 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4).

Il titolare del trattamento può designare i **soggetti autorizzati al trattamento**, delegandoli allo svolgimento delle operazioni di trattamento.

Il titolare del trattamento nomina **il responsabile del trattamento**, vale a dire la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare. Il responsabile del trattamento deve assicurare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. Secondo l'interpretazione della norma da parte della dottrina prevalente, il responsabile del trattamento può essere soltanto esterno. Il responsabile può nominare, se autorizzato dal titolare, sub-responsabili del trattamento. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico, volto a vincolare il responsabile del trattamento al titolare del trattamento e a determinare la materia disciplinata, la durata, la natura e la finalità del trattamento, la tipologia di dati personali e le categorie di interessati, nonché gli obblighi e i diritti del titolare del trattamento (artt. 4 e 28).

Il responsabile della protezione dati (d'ora in poi, RPD), designato a norma dell'articolo 37 del GDPR, può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. Deve essere autonomo e indipendente rispetto al titolare e al responsabile del trattamento e non risponde personalmente in caso di inosservanza del GDPR. I suoi dati di contatto devono essere pubblicati e comunicati all'autorità di controllo. Il RPD è designato in funzione delle qualità professionali e delle conoscenze specialistiche in materia di protezione dei dati, affinché abbia la capacità di assolvere gli specifici compiti ad esso attribuiti dal GDPR. (art. 39).

L'Autorità di controllo è l'autorità pubblica indipendente di cui dispone ogni Stato membro e ha la funzione di sorvegliare l'applicazione del GDPR, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche, con riguardo al trattamento, nonché al fine di agevolare la libera circolazione dei dati personali all'interno dell'Unione (artt. 51-59). In Italia l'Autorità di controllo è rappresentata dal **Garante per la protezione dei dati personali**.

1.5. I principi del GDPR e le misure di sicurezza

Uno dei fondamentali principi sul quale si fonda il GDPR è la cosiddetta ***accountability***, che consiste nella responsabilizzazione di titolari e responsabili, obbligati a tenere comportamenti proattivi che possano dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. D'altronde, la stessa norma sancisce che il titolare del trattamento è competente per il rispetto dei principi previsti dal GDPR, rispetto che deve essere in grado di comprovare (artt. 5, 23-25).

A salvaguardia dell'applicazione corretta della normativa, sono individuati diversi principi sulla base dei quali dare attuazione alle disposizioni di legge.

Il principio di ***privacy by design*** comporta la necessità di definire *ex ante* misure di sicurezza compatibili con il trattamento dati, analizzando il rischio e adottando procedure e processi idonei a garantire la sicurezza. Non si tratta di disposizioni riguardanti esclusivamente gli aspetti tecnologici, ma di misure che influenzano in modo determinante la fase di definizione delle procedure. Il compito del titolare è, dunque, quello di disegnare e organizzare le attività nella modalità più idonea ad attuare il summenzionato principio che si realizza esaminando lo stato dell'arte e le caratteristiche della singola organizzazione, nonché i rischi connessi a tutte le procedure che comportano il trattamento dei dati. Il titolare del trattamento deve adottare politiche interne e attuare misure che soddisfino, in particolare, i principi della protezione dei dati fin dalla progettazione, con il primario scopo di prevenire e non correggere. L'attuazione del principio implica anche libertà e flessibilità di azione da parte del titolare del trattamento che può progettare, nel rispetto della normativa, misure di sicurezza adatte alle caratteristiche della realtà e dei processi che deve gestire.

Il principio di ***privacy by default*** riguarda, invece, l'adozione di misure tecniche e organizzative adeguate per garantire, attraverso una impostazione predefinita, soltanto i dati

personali necessari per ogni specifica finalità del trattamento, assicurando che non siano resi accessibili dati personali a un numero indefinito di persone fisiche (art. 25, c. 2). Ne consegue, quindi, la necessità di trattare solo i dati necessari alla finalità perseguita e solo nella misura strettamente necessaria, al fine di ridurre al minimo il rischio di trattamenti illeciti. Pertanto, nella definizione di un trattamento, il titolare adotta come principio-guida la minimizzazione del dato raccolto. Coerentemente, sono raccolti solo i dati necessari allo scopo perseguito e agli stessi accedono solo i soggetti autorizzati. Alla stessa stregua le persone autorizzate a trattare dati accedono soltanto a quei dati che sono a loro necessari per poter svolgere la propria mansione (principio del *need to know)*.

L'art. 25 del GDPR, infine, indica alcune misure di sicurezza standard (**pseudonimizzazione, minimizzazione**) che dovranno essere integrate da tutte le altre necessarie modalità idonee a soddisfare, nel peculiare contesto di ogni organizzazione, la tutela dei dati e la tutela dei diritti dell'interessato, come richiesto dalla legge.
La pseudonimizzazione, citata espressamente dal GDPR, rappresenta una tecnica diretta a impedire l'identificazione di un individuo e consiste nella conservazione dei dati personali omettendo alcune informazioni aggiuntive rispetto a quelle considerate essenziali. Diversamente, la minimizzazione dei dati, ovvero l'adozione di tutti i principi volti a minimizzare i dati soggetti al trattamento, ma anche a limitare le finalità dello stesso. Tale tecnica implica il trattamento solo dei dati indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati. Il richiamo alle finalità della raccolta rende necessario, di volta in volta, accertare quale sia lo scopo che il titolare del trattamento si prefigge al momento di richiedere i dati personali. La raccolta dei dati non deve mai essere eccessiva rispetto allo scopo del soggetto che li raccoglie e questo implica una valutazione accurata sull'obiettivo da raggiungere e sul trattamento necessario.

Il trattamento dei dati personali, a norma del GDPR, deve essere improntato dunque al rispetto dei seguenti principi: minimizzazione ed esattezza dei dati; integrità e riservatezza; liceità, correttezza e trasparenza; limitazione della finalità.
Nel paragrafo che riguarda i trattamenti relativi agli atti consiliari soggetti a pubblicazione sono descritte le procedure e le misure messe in atto dal Consiglio regionale della Calabria.

2. Privacy contraltare della trasparenza e bilanciamento dei valori

Secondo Alan Westin – uno dei più grandi studiosi di privacy - la vita democratica di uno Stato si basa su due principi: trasparenza e privacy; difatti, Westin considera "*la democrazia come 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*" [7]

L'evoluzione delle normative in materia di trasparenza e di privacy e lo sviluppo tecnologico in continua trasformazione hanno reso sempre più complesso il bilanciamento fra la trasparenza amministrativa da un lato e la protezione dei dati personali dall'altro, ma al di là dell'apparente contrasto e inconciliabilità, i due principi possono e devono tendere a un punto di equilibrio che salvaguardi le contrapposte esigenze.

La trasparenza amministrativa fa concretamente ingresso nel nostro ordinamento soltanto con l'entrata in vigore della legge 7 agosto 1990, n. 241 che istituisce il diritto di accesso ai documenti amministrativi. Si tratta però di un accesso attivabile su istanza, riservato ai soli portatori di un interesse qualificato, diretto, attuale e concreto (**accesso documentale**), vietando espressamente il controllo generalizzato dell'operato della pubblica amministrazione. Il legislatore, però, già all'epoca aveva identificato la salvaguardia della riservatezza dei terzi come limite esplicito all'accesso, stabilendo che i dati o i documenti ottenuti con l'accesso documentale possono essere utilizzati solo dagli interessati e solo per le motivazioni esplicitate nella richiesta d'accesso.

L'entrata in vigore del Decreto Legislativo 27 ottobre 2009, n. 150 segna la seconda fondamentale tappa dell'evoluzione del principio della trasparenza amministrativa. In esso sono presenti un insieme di norme che hanno l'obiettivo di assicurare la totale accessibilità dei dati riguardanti i servizi resi dalla Pubblica Amministrazione tramite la pubblicità e la disponibilità immediata sulle reti internet di tutti i dati su cui si basano le valutazioni operate

[7] *A.Westin, Privacy and Freedom, London, 1970*.

dalla stessa; inoltre è prevista l'adozione da parte di ogni singola amministrazione di programmi triennali per la trasparenza da rendere pubblici proprio attraverso gli appositi siti internet.

Comincia, così, a delinearsi una trasparenza orientata al concetto di ***open data***, funzionale alla realizzazione dell'***open government*** che rappresenta la partecipazione attiva e collaborativa dei cittadini alle scelte amministrative e – quale effetto conseguente - determina lo sviluppo di «forme diffuse di controllo del rispetto dei principi di buon andamento ed imparzialità».

Successivamente, con la Legge 6 novembre 2012, n. 190: «Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione» (in attuazione dell'art. 6 della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione), la trasparenza amministrativa acquisisce una nuova e potenzialmente diversa prospettiva, poiché la conoscibilità totale dei documenti amministrativi si rivela un efficace strumento di prevenzione della corruzione.

Il Decreto Legislativo 14 marzo 2013, n. 33 (cd. decreto trasparenza) - emanato in attuazione di quanto previsto dalla legge n. 190/2012 - disciplina in maniera organica la materia, introducendo per le amministrazioni pubbliche sia l'obbligo di pubblicazione dei dati all'interno delle sezioni denominate "Amministrazione trasparente", sia l'istituto dell'accesso civico.

La trasparenza si configura così da un lato come pubblicità intesa quale obbligo di pubblicazione di dati, informazione e documenti detenuti dalla PA ed individuati per legge, e dall'altro come diritto alla conoscibilità in quanto chiunque ha il potere di richiederne la pubblicazione, nei casi di inerzia delle amministrazioni. Il cittadino da fruitore diventa dunque controllore della legittimità dell'azione amministrativa. Tuttavia, si tratta ancora di un **accesso civico "semplice"** che permette di accedere a "informazioni concernenti l'organizzazione e l'attività della pubblica amministrazione" in caso di mancata pubblicazione degli stessi da parte dell'amministrazione.

Con il Decreto Legislativo 25 maggio 2016 n. 97 - che introduce nell'ordinamento nazionale il cosiddetto modello FOIA (*Freedom of Information Act*) di matrice statunitense - si amplia

lo spettro di conoscibilità dell'azione amministrativa estendendo a chiunque il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni – ovvero a dati *ulteriori rispetto a quelli dovuti dagli obblighi di pubblicazione* - senza alcun limite né dal punto di vista soggettivo, né per quanto riguarda le motivazioni per le quali si vuole effettuare l'accesso; viene dunque stabilita un'ulteriore tipologia di accesso: l'**accesso generalizzato**, definito anche accesso di "terza generazione" dal Consiglio di Stato nell'Adunanza Plenaria n. 10/2020. Si ribalta, infatti, il presupposto di base: le informazioni, i dati e documenti detenuti dalle amministrazioni sono per loro natura pubblici e conoscibili. Le amministrazioni sono tenute a renderli noti su richiesta di chiunque, con obbligo di motivazione in caso di rigetto totale o parziale dell'istanza di accesso. In breve, alla trasparenza di tipo "proattivo", ossia realizzata mediante la pubblicazione obbligatoria sui siti web di determinati enti dei dati e delle notizie indicati dalla legge, viene ad aggiungersi una trasparenza di tipo "reattivo", cioè in risposta alle istanze di conoscenza avanzate dagli interessati.

Ma l'apertura di un patrimonio informativo sempre più crescente, se non adeguatamente gestito, comporta seri rischi per la sfera di riservatezza dei singoli individui e al contempo può rivelarsi inutile ai fini del controllo sull'esercizio del potere. La possibilità conoscitiva del cittadino nel suo rapporto con la pubblica amministrazione incontra un limite nel momento in cui si scontra con il diritto dell'interessato al trattamento dei dati personali contenuti negli atti amministrativi pubblicati o accessibili. L'art 5 bis del d. lgs. 33/2013 stabilisce che l'accesso civico deve essere rifiutato, fra l'altro, se il diniego è necessario per evitare un pregiudizio concreto alla tutela della protezione dei dati personali, in conformità alle disposizioni vigenti in materia.

Il richiamo espresso alla disciplina legislativa sulla protezione dei dati personali da parte dell'art. 5 bis del d. lgs. 33/2013 comporta che, nella valutazione del pregiudizio concreto, si faccia riferimento a tutta una serie di parametri rinvenibili sia nella legislazione nazionale ed europea in materia di protezione dei dati (regolamento (UE) n. 2016/679 - GDPR e decreto legislativo n. 101/2018), sia nella giurisprudenza nazionale ed europea.

La Corte di Giustizia dell'Unione europea ha esplicitato ripetutamente che "*le esigenze di controllo democratico non possono travolgere il diritto fondamentale alla riservatezza delle persone fisiche, dovendo sempre essere rispettato il principio di proporzionalità, definito cardine della tutela dei dati personali: deroghe e limitazioni alla protezione dei dati personali*

devono perciò operare nei limiti dello stretto necessario, e, prima di ricorrervi occorre ipotizzare misure che determinino la minor lesione, per le persone fisiche, del suddetto diritto fondamentale e che, nel contempo, contribuiscano in maniera efficace al raggiungimento dei confliggenti obiettivi di trasparenza, in quanto legittimamente perseguiti"[8]*.*

Il giusto equilibrio tra i concetti di privacy e trasparenza emerge con chiarezza dal considerando 4 del Regolamento europeo sulla privacy n. 679/2016 secondo cui" il *diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con gli altri diritti fondamentali in ossequio al principio di proporzionalità".* Le Linee guida approvate dall'ANAC d'intesa con il Garante per la protezione dei dati personali, nel tracciare i limiti e le esclusioni di cui all'art. 5 bis del d. lgs. n. 33/2013, rinviano a un'attività valutativa che deve essere effettuata dalle amministrazioni con la tecnica del bilanciamento tra l'interesse pubblico conoscitivo e la tutela di altrettanti validi interessi considerati dall'ordinamento. È pertanto l'amministrazione che è tenuta a decidere - caso per caso - se l'ostensione degli atti può determinare un pregiudizio concreto e probabile agli interessi indicati dal legislatore.

Tra le valutazioni da effettuare in ordine alla possibile esposizione di documenti che contengono dati personali deve essere, inoltre, tenuto in considerazione che i dati e i documenti che si ricevono a seguito di un'istanza di accesso civico divengono "*pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente e di utilizzarli e riutilizzarli ai sensi dell'articolo 7"* (art. 3, d. lgs 33/2013).

Nel disciplinare il riutilizzo dei dati pubblicati, il d. lgs n. 33/2013 dispone, inoltre, che gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono l'indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'art. 7 nel rispetto dei principi sul trattamento dei dati personali.

---

[8] *Sentenze 20 maggio 2003, nelle cause riunite C-465/00, C-138/01 e C-139/01, Osterreichischer Rundfunk e altri, e 9 novembre 2010, nelle cause riunite C-92/09 e 93/09, e Volker und Markus Schecke e Eifert*

Pertanto, l'ente destinatario dell'istanza dovrà valutare se la conoscenza da parte di chiunque del dato personale richiesto possa arrecare un pregiudizio concreto alla protezione dei dati personali, come ad esempio future azioni da parte di terzi nei confronti dell'interessato o situazioni che potrebbero determinare l'estromissione o la discriminazione dello stesso individuo, o altri svantaggi personali o sociali, minacce, intimidazioni, ritorsioni o furti d'identità. La ritenuta sussistenza di un pregiudizio concreto comporterà - come ricordato dalle summenzionate Linee guida Anac - il rigetto dell'istanza o, nel caso in cui si consideri di poterla accogliere, l'amministrazione dovrà procedere all'oscurazione relativa ai dati personali e alle informazioni personali di dettaglio che risultino comunque sproporzionate, eccedenti e non pertinenti.

Per procedere correttamente, le amministrazioni, innanzitutto, devono verificare che esista una norma di legge o di regolamento che preveda l'obbligo di pubblicare on line sui propri siti informazioni, atti e documenti amministrativi contenenti dati personali; bisogna poi ricordare che è sempre vietata la pubblicazione di dati sulla salute e sulla vita sessuale, mentre i dati c.d. sensibili (etnia, religione, appartenenze politiche etc.) possono essere diffusi solo laddove indispensabili al perseguimento delle finalità di rilevante interesse pubblico. Occorre, infine, anche adottare misure per impedire l'indicizzazione dei dati sensibili da parte dei motori di ricerca e il loro riutilizzo.

Il nuovo GDPR definisce quindi la complementarità dei diritti fondamentali della persona e della trasparenza: i primi anzi sono gli strumenti per rendere possibile la seconda. In questa prospettiva va dunque rigettata qualunque visione oppositiva o antagonista del diritto alla *privacy* nei confronti della trasparenza.

2.1. I principi di trasparenza e privacy nella pubblicità dei lavori parlamentari

Al principio di trasparenza - così come disciplinato dal d. lgs n. 33/2013 e ss. mm. Ii - si affianca quello relativo alla pubblicità dei processi di formazione delle volontà politiche, requisito essenziale per conferire legittimità all'agire politico nei sistemi di governo democratici. Si tratta di un elemento fondamentale per rafforzare le basi dello Stato di diritto, in quanto la trasparenza del processo decisionale contribuisce a consolidare il carattere democratico delle stesse Istituzioni e ad accrescere la fiducia dei cittadini nei confronti dello Stato.

La questione della pubblicità dei lavori parlamentari è stata ritenuta dall'Assemblea costituente talmente connaturata all'istituto stesso della democrazia rappresentativa che ad essa non venne dedicato un particolare approfondimento. La Costituzione, infatti, di per sé non prevede l'obbligo esplicito di informare i cittadini, ma si limita a stabilire - all'articolo 64 - che le sedute sono pubbliche, offrendo la possibilità a tutti coloro che ne facciano richiesta di assistervi; mentre - all'articolo 72 – introduce una riserva di Regolamento per quanto riguarda le forme di pubblicità dei lavori delle Commissioni. Si tratta, invero, di disposizioni riguardanti un aspetto intrinseco al processo decisionale democratico, attraverso il quale viene garantito il diritto politico dei cittadini alla conoscenza dell'attività dei loro rappresentanti in Parlamento e, dunque, alla concreta possibilità di partecipare alla gestione delle politiche e delle attività pubbliche.

Per quanto riguarda l'attività del Consiglio regionale della Calabria, la documentazione a fini di pubblicità è costituita dai resoconti stenografici e sommari dei lavori assembleari e dai resoconti dei lavori delle Giunte e delle Commissioni permanenti, liberamente consultabili, dopo lo svolgimento della seduta, sul sito istituzionale del Consiglio regionale.

Oltre ad assolvere all'importante funzione conoscitiva nei confronti della collettività, tale documentazione rappresenta anche uno strumento a supporto dell'attività giornalistica e, inoltre, fornisce agli operatori del diritto gli atti e i documenti necessari a ricostruire la *"ratio legis*" e l'intenzione effettiva del legislatore. Degna di nota è, inoltre, la dimensione storica che caratterizza i resoconti e la documentazione prodotta (leggi, mozioni, interpellanze, risoluzioni, interrogazioni e tutti gli atti di iniziativa legislativa che sono allegati ai resoconti integrali delle sedute di Consiglio), poiché si rivela elemento indispensabile per tracciare un ponderato *excursus* dell'attività politico - legislativa della nostra regione e poterne ricavare una lettura critica maggiormente esaustiva.

Nell'era digitale che ci contraddistingue, il binomio trasparenza – pubblicità sottende a un concetto di libertà di informazione più aderente alle sollecitazioni della società moderna e, al contempo, rispondente ai principi fondamentali dell'ordinamento che «*la implicano necessariamente e quindi la garantiscono*» (Loiodice). Occorre aggiungere che anche la Corte costituzionale, con le decisioni più recenti, ha contribuito notevolmente ad affermare questo principio; è bene evidenziare che anche le Regioni hanno riconosciuto il diritto dei cittadini e delle organizzazioni sociali all'informazione sull'attività regionale e, difatti, gli

Statuti regionali (sia delle regioni a statuto ordinario, sia a statuto speciale) prevedono forme precise di pubblicità dei lavori assembleari, spesso ulteriormente definite all'interno dei rispettivi regolamenti.

Le amministrazioni pubbliche sono, quindi, incoraggiate ad estendere il più possibile la pubblicità degli atti sui loro siti istituzionali e, al contempo, obbligate *ex lege* a favorire la conoscibilità dei loro lavori, per consentire ai cittadini di vigilare sullo svolgimento delle attività amministrative. La sempre maggiore diffusione e quantità di questi dati si inserisce nel contesto in rapida evoluzione della *e-democracy*, in cui trasparenza e costante necessità di comunicazione tra amministrazione e cittadino acquisiscono rilievo centrale. Questo facile accesso presenta indiscutibili vantaggi in termini di informazione totale sui lavori nell'assemblea regionale. Tuttavia, occorre considerare che queste la fluidità informativa può potenzialmente danneggiare soggetti terzi interessati dagli atti parlamentari e da essi rammentati nel corso dei lavori. Difatti, soprattutto nella premessa di interrogazioni e interpellanze, talvolta sono incluse indicazioni personali relative a dati sensibili, privati e giudiziari. La menzione del proprio nome negli atti assembleari, rintracciabili con l'ausilio di qualunque motore di ricerca, rischia di condannare il soggetto citato ad essere perennemente associato all'episodio della propria vita discusso nelle aule parlamentari. La pubblicazione di tali dati non è di per sé illecita, ma lo è la permanenza senza vincoli temporali di notizie erronee, non aggiornate e decontestualizzate perché relative ad avvenimenti passati che potrebbero essersi diversamente evoluti o perché possono ledere il diritto alla riservatezza delle persone coinvolte. Si pone pertanto l'esigenza di bilanciare la necessaria pubblicità istituzionale con il diritto all'oblio[9], per evitare che gli strumenti di garanzia non si trasformino in conduttori di pregiudizio.

[9] *Per approfondimento sul diritto all'oblio si legga il paragrafo dedicato*.

3. Il diritto all'oblio

L'oblio è un diritto che oltrepassa la mera tutela della privacy e che solo recentemente ha trovato legittimazione nell'ordinamento nazionale ed europeo. Si tratta di un principio cardine del Regolamento europeo per la protezione dei dati personali e consiste nel diritto di ogni persona di rettificare i dati personali che la riguardano nonché il "diritto alla cancellazione e all'oblio", se la conservazione di tali dati non è conforme al Regolamento. Con questo strumento si vuole tutelare l'immagine pubblica di un individuo attraverso l'attualizzazione - che include anche la cancellazione - di dati pregressi o riferiti a fatti passati che non corrispondono o sono superati, arrecando così un danno all'immagine del soggetto interessato. Tuttavia, data l'esistenza di programmi di ricerca e di analisi sempre più performanti e con capacità quasi illimitate di memorizzazione, il diritto all'oblio, inteso come la cancellazione completa e definitiva dei dati, è spesso un concetto illusorio. Le informazioni, infatti, vengono diffuse su internet a livello mondiale e ciò complica la possibilità di far valere giuridicamente i propri diritti, anche per la difficoltà di determinazione del foro e del diritto applicabili.

Il diritto all'oblio costituisce frutto di elaborazioni dottrinarie e giurisprudenziali[10], principalmente delle Autorità Garanti europee, e si colloca nel quadro dei diritti della personalità come una particolare forma di garanzia connaturata al diritto alla riservatezza. Esso costituisce un'applicazione concreta dei principi di finalità e di proporzionalità, affinché l'elaborazione dei dati non abbia una durata superiore a quella necessaria per raggiungere gli obiettivi previsti. Si tratta dunque di un diritto non assoluto, considerato che, a seconda delle circostanze, occorre effettuare un bilanciamento degli interessi tra il rispetto della sfera privata e l'interesse all'elaborazione dei dati derivante dalla libertà di manifestazione del pensiero e dal dovere di informazione e di memoria. In altri termini, a seconda delle circostanze specifiche, occorre sempre chiedersi se le lesioni della personalità derivanti dall'elaborazione o dalla pubblicazione dei dati siano giustificate da un interesse superiore.

[10] *In Italia assumono rilevanza talune decisioni della Corte di Cassazione quali Cass., 9/4/1998, n. 3679; Cass., 25/6/2004, n. 11864; Cass., 05/04/2012, n. 5525; Cass. 26/06/2013, n. 16111; Cass. 24/06/2016, n. 13161*

Attualmente il diritto all'oblio è previsto dall'articolo 17 del GDPR, rubricato 'Diritto alla cancellazione («diritto all'oblio»)', in cui sono elencati i motivi in presenza dei quali l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo; fra le varie ipotesi, l'interessato può chiedere la cancellazione quando i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati, o quando abbia revocato il consenso al trattamento o i dati siano stati trattati illecitamente. Tuttavia, sempre l'art. 17 stabilisce che il diritto alla cancellazione non sussiste quando il trattamento dei dati è necessario per soddisfare alcune esigenze, quali l'esercizio del diritto alla libertà di espressione e di informazione oppure, nell'ambito della ricerca scientifica o storica, per fini di archiviazione nel pubblico interesse. Al di là di questi principi generali, l'individuazione dei casi in cui il trattamento dei dati personali risulta in concreto "necessario" spetta all'interprete, cioè all'autorità (garante privacy o giudice) chiamata a decidere se, in una certa vicenda sottoposta al suo esame, la persona possa legittimamente pretendere che una notizia che la riguarda, pur legittimamente diffusa in passato, non resti esposta a tempo indeterminato alla possibilità di nuova divulgazione.
Il diritto all'oblio si esercita mediante proposizione di un'istanza al titolare del trattamento dei dati. Nell'ipotesi di risposta negativa alla richiesta e, altresì, nel caso di totale assenza di risposta, l'interessato potrà esperire reclamo al Garante della Privacy, ai sensi dell'art. 77 del GDPR o, in alternativa, procedere con ricorso innanzi all'autorità giudiziaria.

Un'importantissima svolta in tema di tutela della riservatezza è stata rappresentata dalla pronunzia Costeja della Corte (Grande Sezione) del 13 maggio 2014, resa nella causa C-131/12 (caso Google Spain), che ha segnato il riconoscimento del diritto all'oblio nell'Unione Europea e ha comportato l'introduzione del diritto medesimo (articolo 17 del GDPR) al fine di tenere conto del diritto di richiedere la deindicizzazione, come stabilito dalla sentenza medesima. Con la suddetta sentenza viene riconosciuto "il diritto a opporsi all'indicizzazione dei propri dati personali ad opera del motore di ricerca, qualora la diffusione di tali dati tramite quest'ultimo le arrechi pregiudizio" e, in particolare, "qualora i dati risultino inadeguati, non siano o non siano più pertinenti". Per la prima volta viene stabilito che il motore di ricerca è titolare del trattamento dei dati personali delle pagine che indicizza e che i soggetti possono rivolgersi direttamente ai fornitori del servizio di motore di ricerca per chiedere una cancellazione (che, in realtà, altro non è che una rottura del link tra la ricerca

del nome dell'interessato e la pagina web in cui è stata pubblicata l'informazione sull'interessato); qualora il gestore rimanga inerte, l'interessato può rivolgersi alle autorità competenti, in presenza di certe condizioni, per esercitare il suo diritto.[11]

Sulla scia delle pronunzie susseguitesi e a seguito dell'entrata in vigore del GDPR, sono state adottate le Linee Guida 5/2019 (aggiornate nella versione 2.0 dopo la consultazione pubblica del 7 luglio 2020) sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca (il «diritto di richiedere la deindicizzazione»). Il documento affronta due temi: il primo riguarda i motivi che un interessato può invocare per chiedere la deindicizzazione a un fornitore di motore di ricerca ai sensi dell'articolo 17, paragrafo 1, del GDPR; il secondo riguarda le eccezioni al diritto di richiedere la deindicizzazione ai sensi dell'articolo 17, paragrafo 3, del GDPR.

Un'applicazione particolare del diritto all'oblio si ha con riferimento agli atti del Parlamento italiano, mutuabile agli atti delle assemblee legislative regionali, e in particolare agli atti di inchiesta e di sindacato ispettivo che vedono coinvolti singoli cittadini, nei quali il nome dell'interessato è associato a vicende di cronaca di interesse generale sulle quali il Parlamento chiede al Governo di far luce o prendere posizione (interrogazioni, interpellanze e mozioni) o sulle quali indagano le stesse Camere, nel caso delle Commissioni monocamerali o bicamerali d'inchiesta, previste dall'articolo 82 della Costituzione.

L'art. 64 della Costituzione - che prevede la pubblicità dell'attività conoscitiva e legislativa del Parlamento - ha indotto le Camere a mettere in atto un'imponente opera di digitalizzazione e pubblicazione degli atti parlamentari sui siti istituzionali; analogamente il Consiglio regionale della Calabria provvede alla pubblicità degli atti ispettivi, di controllo e legislativi attraverso il sito web istituzionale, ai sensi del proprio Statuto e del proprio Regolamento.

A differenza dei due rami del Parlamento, che svolgono le loro funzioni in regime di autodichia, le Assemblee legislative regionali soggiacciono alle disposizioni del GDPR.

---

[11] *Con pronunzia della Corte di Giustizia del 24 settembre 2019 (caso C-507/17), la Corte UE ha affermato che il gestore di un motore di ricerca non è obbligato a effettuare la deindicizzazione in tutte le versioni del suo motore di ricerca, ma soltanto nelle versioni del motore di ricerca corrispondenti agli Stati membri.*

4. Il principio di minimizzazione dei dati.

Il principio di minimizzazione dei dati è enunciato dall'articolo 5 del Regolamento europeo 679/2016 (GDPR) e, nello specifico, dalla lettera c) che testualmente recita: "1. I dati personali sono: … c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". Il principio in esame era già stato previsto dal D. L.gs 196/2003 (c.d. Codice della privacy) e, precisamente nell'articolo 3, rubricato "Principio di necessità nel trattamento dei dati" e nell'articolo 11 lett. d), che stabiliva il rispetto del principio di pertinenza, completezza e non eccedenza dei dati rispetto alle finalità per cui sono raccolti e trattati. Entrambi i predetti articoli del Codice della privacy sono stati abrogati con l'entrata in vigore del D. lgs. 101/2019, che reca le disposizioni per l'adeguamento dell'ordinamento nazionale al nuovo Regolamento.
Attualmente, il riferimento normativo è costituito dall'articolo 5 del GDPR nel combinato disposto con l'articolo 6 del Regolamento europeo, da cui si desumono i principi generali che il titolare del trattamento deve seguire nella raccolta dei dati personali degli utenti.

Il **principio di minimizzazione** si articola in vari sotto-principi:

- **il principio di adeguatezza** in base al quale i dati sono adeguati se si presentano in una quantità completa e sufficiente rispetto alle finalità che vogliono raggiungere;
- **il principio di pertinenza** ossia i dati raccolti e trattati devono essere strettamente collegati alle finalità del trattamento. Pertanto, non devono essere raccolti e trattati dati non necessari al raggiungimento dello scopo cui tendono e si dovrebbe evitare del tutto l'utilizzo dei dati personali qualora per il raggiungimento dell'obiettivo sia possibile utilizzare dati anonimizzati o pseudo anonimizzati;
- **il principio di limitazione** – che potrebbe anche essere definito come principio di non eccedenza – in base al quale la quantità di dati non deve essere eccedente rispetto agli scopi che si intendono raggiungere;
- **il principio di proporzionalità** che si desume dal rispetto dei principi di pertinenza e non eccedenza e consiste nel trattare i dati in modo proporzionale ai dati stessi.
- **il principio di finalità** che stabilisce che un trattamento di dati personali è legittimo in relazione, appunto, al fine del trattamento stesso. Il Regolamento europeo sancisce, infatti, la necessità che i dati personali vengano raccolti per finalità

determinate, esplicite e legittime e, quindi, trattati secondo modalità compatibili con tale finalità;

- **il principio di limitazione della conservazione** secondo cui i dati sono conservati dal titolare del trattamento in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Pertanto, la conservazione per un periodo di tempo troppo lungo costituirà anch'essa una diretta violazione del Regolamento europeo, poiché anche l'arco temporale deve essere rapportato al perseguimento delle specifiche finalità per le quali i dati sono stati raccolti e trattati.

Da tali considerazioni preliminari emerge come siano molteplici gli obblighi di tutela dei dati personali che incombono sul titolare del trattamento, che deve predisporre adeguate misure tecniche e organizzative in grado di ridurre al minimo tale trattamento.
Innanzitutto, diventa prioritario individuare, già prima dell'acquisizione, quali dati siano essenziali per lo specifico trattamento che ci si propone di effettuare, quindi, stabilire se quel determinato trattamento sia effettivamente necessario al raggiungimento della finalità prestabilita e, inoltre, verificare che lo scopo prefissato, di volta in volta, non sia conseguibile con altri mezzi ragionevolmente utilizzabili nel contesto di riferimento quali, ad esempio, la **pseudonimizzazione**. Qualora, infatti, lo scopo possa essere conseguito attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, esso deve essere raggiunto in tal modo. Soltanto analizzando lo scopo è possibile stabilire se i dati raccolti rispettino le condizioni di liceità indicate nell'art. 6 del GDPR (cioè se rispettino finalità determinate, esplicite e legittime) e se la loro raccolta sia strettamente necessaria al raggiungimento dello stesso.

Il principio di minimizzazione costituisce uno dei concetti chiave del GDPR, in considerazione, peraltro, della sempre maggiore attenzione rivolta alla protezione dei dati personali nella società contemporanea, caratterizzata dalla circolazione nel web di una quantità enorme di informazioni, anche personali, delle quali, spesso, è impossibile controllare provenienza ed autorevolezza. L'utilizzo non corretto di tali strumenti può, infatti, anche comportare la lesione di diritti di rango costituzionale come il diritto all'integrità morale, all'immagine, all'onore, al decoro personale e alla reputazione. Dalla lettura del considerando 39 del GDPR emerge la necessità di sensibilizzare la collettività non solo sulle

norme, le garanzie e i diritti relativi al trattamento dei dati personali, ma anche sui rischi, nonché sulle tutele stabilite dalla legge contro questi rischi.

All'interno dei Consigli regionali, i consiglieri regionali hanno la responsabilità di provvedere alla minimizzazione dei dati personali nella redazione degli atti consiliari di loro competenza e soggetti a pubblicazione, limitandosi a riportare i dati strettamente necessari a svolgere le loro funzioni nell'interesse pubblico. In ogni caso, sarà comunque competenza degli uffici consiliari competenti - in base all'organizzazione precedentemente programmata - provvedere alla pseudonimizzazione o minimizzazione dei dati ulteriori, ove possibile. In merito a tale profilo, occorre evidenziare che sono state molteplici le sanzioni comminate dal Garante della privacy. Ricordiamo, in proposito, l'ordinanza ingiunzione emessa in data 8 luglio 2021 nei confronti del Consiglio regionale della Valle d'Aosta per la diffusione on line di dati e informazioni personali contenuti in un'interrogazione a risposta scritta, in violazione del principio di minimizzazione.

Nello specifico, l'Autorità riceveva un reclamo con il quale veniva contestata una violazione della normativa in materia di protezione dei dati personali, e precisamente, lamentata la diffusione – attraverso la pubblicazione sul sito web istituzionale del Consiglio regionale della Valle d'Aosta – di un'interrogazione a risposta scritta contenente dati personali dei reclamanti e informazioni di dettaglio inerenti a compensi e indennità ricevuti dal Consorzio del quale erano dipendenti. I reclamanti, attraverso una nota inviata al Consiglio regionale e al Responsabile della protezione dei dati personali della Regione Valle d'Aosta, hanno dunque esercitato il proprio diritto in materia di protezione dei dati personali nei confronti del predetto Ente che, tuttavia, non ha accolto la richiesta di rimozione dei dati personali dal sito web.

L'Autorità ha previsto il «riconoscimento delle funzioni di controllo, di indirizzo politico e di sindacato ispettivo tra le attività di rilevante interesse pubblico per il cui perseguimento è consentito il trattamento di categorie particolari di dati personali» (cfr. 2-sexies, comma 2, lett. h); tuttavia, ha contestato che il Consiglio regionale non ha tenuto conto del necessario rispetto delle regole e dei principi in materia di protezione dei dati personali di provenienza europea (che si applicano anche ai dati personali non rientranti nelle categorie particolari di cui agli artt. 9 e 10 del GDPR) come, ad esempio, quello di «minimizzazione» in base al quale i dati personali, anche nel caso in cui siano contenuti in atti o documenti la cui

diffusione online sia prevista da una specifica base normativa, devono essere non solo «adeguati» e «pertinenti», ma anche «limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, par. 1, lett. c, GDPR). Alla luce di tale principio, il Garante non ha accordato, nel caso in esame, alcun automatismo rispetto alla diffusione online di dati e informazioni personali, anche se non appartenenti a categorie particolari oppure a condanne penali o reati.

A parere del Garante, il Consiglio regionale avrebbe dovuto ritenere che, per l'esercizio delle proprie funzioni istituzionali, la diffusione dei dati personali dei reclamanti non era necessaria e pertanto avrebbe dovuto provvedere a un semplice oscuramento dei dati personali (nominativo, incarico e data di assunzione) dei soggetti interessati contenuti negli atti pubblicati online, salvaguardando in tal modo anche il principio di pubblicità degli atti di sindacato ispettivo.

5. Le autorità di controllo

Il Capo VI del GDPR prevede la costituzione di un’"Autorità di controllo" per ciascuno Stato membro (art. 54) e fissa identici compiti e poteri per le Autorità in tutti i Paesi membri. In Italia tale ruolo è assunto dal Garante per la protezione dei dati personali (Garante Privacy).

Le autorità di controllo assicurano l’attuazione della normativa secondo i principi di congruità e coerenza. Una decisione emessa da un'autorità nazionale diventa automaticamente valida per tutto il territorio dell'Unione europea, salvo particolari eccezioni che vengono risolte dal Comitato europeo per la protezione dei dati. Un esempio è dato dai trasferimenti di dati personali all'estero ammessi dalle autorità nazionali, le cui decisioni acquistano valore nell'intero territorio dell'Unione. L'autorità di controllo di un Paese, qualora intenda adottare una misura tale da produrre effetti giuridici con riguardo all'attività di trattamento che incida su interessati presenti in vari Stati dell'Unione europea, dovrà cooperare con le autorità degli altri Stati e con l'autorità di controllo dove ha sede l'azienda, la quale funge da *leading authority*. Tale procedura è volta a evitare che le autorità nazionali di controllo possano emettere decisioni contrastanti tra loro.

L'Autorità Garante Privacy italiana è un organo collegiale composto da 4 membri, due dei quali eletti dalla Camera e agli altri due dal Senato. Al suo interno si provvede alla nomina di un presidente e di un vicepresidente, che sostituisce il primo in caso di impedimento o assenza. Il mandato ha una durata di 7 anni e non è rinnovabile. I soggetti nominati a comporre questo organo devono garantire indipendenza ed essere in possesso di una comprovata esperienza nella protezione dei dati personali in ambito informatico e giuridico. Come le altre autorità amministrative indipendenti italiane, anche il Garante della privacy presenta una relazione annuale al Governo e al Parlamento sull’attività svolta.

Tra le attività svolte dal Garante rientrano:

1. **I provvedimenti collegiali di tipo prescrittivo o sanzionatorio**;
2. **Le decisioni su ricorsi**: gli utenti possono far valere i propri diritti in tema di trattamento di dati personali facendo ricorso all’autorità giudiziaria o reclamo al garante per la privacy.
   Nel reclamo andrà indicato: la circostanza da cui si ricava la competenza del Garante italiano; gli estremi identificativi del titolare del trattamento, del responsabile e del

D.P.O. se noto; una dettagliata ricostruzione dei fatti e delle circostanze della violazione privacy su cui si fonda il reclamo, comprese eventuali richieste già rivolte sulla questione al titolare del trattamento; le disposizioni del Regolamento o di legge che si ritengono violate; infine, il provvedimento che si chiede di applicare nei confronti del titolare/responsabile del trattamento.

Ricevuto il reclamo, il Garante dovrebbe trattarlo entro il termine di 3 mesi, ma tale tempistica non sempre viene rispettata, in considerazione della mole delle segnalazioni da trattare e dell'inadeguata dotazione di personale dell'ufficio del Garante. È così previsto il diritto dell'interessato di proporre ricorso giurisdizionale contro il Garante, qualora quest'ultimo non abbia trattato il reclamo o non lo abbia informato entro 3 mesi dello stato o dell'esito del reclamo proposto. Il medesimo diritto sussiste anche contro le decisioni assunte dal Garante su un reclamo trattato. Va precisato che la procedura di reclamo non è un mero strumento finalizzato unicamente a irrogare sanzioni, ma permette anche di interpretare e di conseguenza rendere più leggibili le regole in vigore per tutti gli intervenenti al processo di trattamento dei dati;

3. **Pareri**: il parere dell'Autorità è obbligatorio in diversi ambiti, tra cui: l'adozione di norme a livello statale, regionale e locale che riguardino la materia di sua competenza; la pubblicazione di atti contenenti dati sensibili da parte delle pubbliche e amministrazioni; il trattamento di dati a fini di ricerca medica ed epidemiologica;
4. **Ordinanze-Ingiunzioni**: l'autorità può tutelare i diritti degli utenti ordinando ai trasgressori di conformarsi alle proprie direttive a pena di sanzione;
5. **Segnalazioni all'autorità giudiziaria**: qualora il garante venga a conoscenza di reati penali nel corso della sua attività, è tenuto a comunicarlo celermente all'autorità giudiziaria;
6. **Accertamenti e controlli *in loco***: il garante ha la facoltà di richiedere l'accesso agli archivi e ai data base e può disporre anche ispezioni in loco.

I Compiti del Garante sono definiti dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101, oltre che da vari altri atti normativi italiani e internazionali. L' articolo 57 del GDPR chiarisce che, fatti salvi gli altri compiti specifici attribuiti da altre disposizioni dello stesso

testo, sul proprio territorio ogni autorità deve promuovere la consapevolezza e la comprensione delle regole europee in materia di privacy nei confronti dei cittadini, dei titolari e dei responsabili del trattamento, fornire informazioni su richiesta, svolgere indagini e trattare i reclami. L'informazione al pubblico viene considerata da parte del legislatore europeo come la chiave di volta per sensibilizzare tutti i soggetti, pubblici e privati, tenuti all'applicazione del Regolamento, all'adozione di tutte quelle buone prassi che permettono la riduzione del rischio di trattamento non corretto dei dati. Nell'ambito del rapporto tra autorità e titolare/responsabile del trattamento, all'autorità di controllo sono conferiti poteri di indagine (art. 58, co. 1), correttivi (art. 58, co.2), autorizzativi e consultivi (art. 58, co.3), nonché il potere di infliggere sanzioni amministrative pecuniarie nel caso in cui da questa operatività e dall'esercizio dei predetti compiti dovesse emergere la necessità di ulteriori approfondimenti, ossia nel caso in cui dovesse essere riscontrato un operato non conforme al Regolamento; ma il potere dell'autorità di controllo può estendersi anche a una sfera più ampia di dati, ordinando la rettifica, la cancellazione di dati personali o la limitazione del trattamento.

Sussiste, poi, il potere dell'autorità di infliggere una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento. In effetti tanto la sanzione, quanto le funzioni correttive, sono frutto di un enorme potere riconosciuto all'autorità di intervento sul titolare/responsabile del trattamento, potere che di certo può essere positivamente inteso alla luce del fondamentale principio di indipendenza che connota la stessa istituzione e organizzazione delle autorità di controllo.

PARTE SECONDA

6. Documentazione delle attività istituzionali del Consiglio regionale della Calabria e degli organi consiliari

La base giuridica del trattamento, cioè ciò che autorizza legalmente il trattamento dei dati sotto riportati, è rinvenibile dal combinato disposto di diverse norme di rango sia nazionale sia regionale. Lo Statuto della Regione Calabria, infatti, all'articolo 9 sancisce il diritto del cittadino ad una informazione costante sull'attività istituzionale, giudicandola presupposto fondamentale della partecipazione ed un aspetto essenziale dei diritti del cittadino e, per tali ragioni, la Regione Calabria assicura la più ampia informazione sugli atti, sui programmi e sulle iniziative di propria competenza, nonché sul funzionamento dei propri organi ed uffici attraverso l'impiego di strumenti di informazione e di comunicazione di massa. In armonia con tale norma, il Regolamento interno del Consiglio regionale della Calabria, agli articoli 44 e 85, disciplina le forme di pubblicità dei lavori sia dell'Assemblea sia delle Commissioni consiliari.

Il trattamento è poi consentito espressamente dall'articolo 2 *sexies,* lett. f) del Codice Privacy (D.Lgs. 196/2003 e ss.mm.ii.) che riconosce un rilevante interesse pubblico, che autorizza il trattamento di particolari categorie di dati (ai sensi dell'articolo 9, paragrafo 2, lettera g) del GDPR), in materia di documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, di Commissioni e di altri organi collegiali o assembleari. A ciò si aggiunga l'interesse di archiviazione storica sotteso alle attività di assemblee rappresentative.

6.1 Resoconto sommario sedute di Consiglio regionale

Il resoconto sommario delle sedute pubbliche del Consiglio regionale, redatto ai sensi dell'articolo 44 del Regolamento interno del Consiglio regionale della Calabria, consiste nella sintesi completa, immediata e simultanea dei dibattiti assembleari redatta in forma imparziale e in terza persona. Esso riporta gli interventi dei consiglieri, dei componenti di Giunta e, nei casi particolari previsti dal Regolamento interno (art. 47, comma 5), di soggetti esterni, dando conto anche delle fasi procedurali, degli atti approvati e degli esiti delle

votazioni. Viene pubblicato a fine seduta nell'apposita sezione del sito web istituzionale del Consiglio regionale, all'indirizzo www.consiglioregionale.calabria.it/portale, ed è consultabile al link "attività istituzionale" cliccando sulla voce "resoconti sommari". È "conservato" nell'archivio dell'Ufficio Resoconti stenografici e sommari posto all'interno del Segretariato generale.

Nello specifico quadro di garanzie a tutela dei diritti e delle libertà degli interessati in materia di privacy, il resoconto sommario sarà il risultato di un'attività organizzativa basata sui principi di **"privacy by design"** e **"privacy by default",** volti a prevenire la diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività delle Assemblee legislative. Pertanto, il resoconto sarà redatto procedendo preventivamente alla minimizzazione dei dati degli interessati, nel caso dovessero emergere nel corso del dibattito, o alla loro esclusione ex ante, laddove non fossero necessari per garantire una fedele e completa sintesi dei lavori assembleari.

A titolo di esempio: se nel corso della seduta di Consiglio regionale il consigliere Caio dovesse citare i dati personali di un cittadino, detti dati non saranno riportati nella sintesi del dibattito o saranno riportati soltanto nei limiti necessari a garantire, da un lato, una corretta pubblicità dei lavori e, dall'altro, la tutela dei diritti degli interessati, attraverso un bilanciamento e valutazione preventiva degli interessi prevalenti.

6.2 Resoconto integrale delle sedute di Consiglio regionale

Il resoconto integrale, redatto ai sensi dell'articolo 44 del Regolamento interno del Consiglio regionale della Calabria, riporta l'intera seduta, quindi ogni singolo intervento degli oratori, le schede relative alle votazioni per appello nominale con l'indicazione precisa di chi ha votato "sì" e di chi ha votato "no" e, in allegato, riporta sia le comunicazioni del Presidente del Consiglio (annunci di interrogazioni, ecc…), sia il testo integrale di tutti gli atti approvati nel corso della seduta, compresi gli atti di sindacato ispettivo (vedasi paragrafo dedicato). I funzionari resocontisti sottopongono a revisione ogni intervento, nel rispetto assoluto dei concetti espressi e dello stile oratorio di ogni consigliere, allo scopo di ricondurlo, ove necessario, al linguaggio parlamentare.

Per prassi, il singolo consigliere ha facoltà, nel caso in cui rinunciasse a parlare, di chiedere che il suo intervento scritto, da consegnare entro la fine della seduta alla Presidenza, sia pubblicato nel resoconto integrale. L'intervento sarà riportato in corsivo.

Tutti i resoconti integrali sono pubblicati nell'apposita sezione del sito web istituzionale del Consiglio regionale, all'indirizzo www.consiglioregionale.calabria.it/portale, e sono consultabili al link "attività istituzionale" cliccando sulla voce "resoconti integrali". Ogni resoconto è "conservato" nell'archivio dell'Ufficio Resoconti stenografici e sommari posto all'interno del Segretariato generale.

Nello specifico quadro di garanzie a tutela dei diritti e delle libertà degli interessati in materia di privacy, il resoconto integrale sarà anch'esso il risultato di un'attività organizzativa basata sui principi di **"privacy by design"** e **"privacy by default"** volti a prevenire la diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività delle Assemblee legislative.

I singoli funzionari resocontisti, cui spetta la revisione di primo livello del resoconto integrale, sono investiti della responsabilità di valutare, volta per volta, la presenza negli interventi di dati personali ulteriori e non necessari e, al fine di tutelare i diritti e le libertà degli interessati, provvederanno direttamente in fase di revisione alla minimizzazione dei predetti ulteriori dati.

Un ulteriore controllo sarà effettuato in fase di revisione di secondo livello prima del visto per la pubblicazione sul sito istituzionale.

Particolare attenzione sarà posta alla minimizzazione di dati riguardanti riferimenti alla salute dell'interessato, al suo stato patrimoniale o a casi di cronaca giudiziaria che, rintracciabili con l'ausilio di qualunque motore di ricerca, rischiano di condannare il soggetto citato ad essere perennemente associato all'episodio della propria vita discusso nelle aule assembleari. Si pone pertanto l'esigenza di bilanciare la necessaria pubblicità istituzionale con il diritto all'oblio, ostacolato dall'intrinseca atemporalità della rete, nel tentativo di tutelare i soggetti nominati sia nei dibattiti, sia negli atti consiliari, per evitare che il regime di

pubblicità diventi, da strumento di garanzia a tutela di consiglieri e cittadini, potenziale pregiudizio per il futuro di questi ultimi.

Medesima procedura sarà applicata nel caso in cui il consigliere dovesse rinunciare al suo intervento orale e consegnasse alla Presidenza, entro la fine della seduta, il suo intervento scritto.

A titolo di esempio: se, nel corso della seduta di Consiglio regionale, il consigliere Caio dovesse citare i dati personali di un cittadino, detti dati saranno riportati soltanto nei limiti necessari a garantire da un lato una corretta pubblicità dei lavori e dall'altro la tutela dei diritti degli interessati, attraverso un bilanciamento e valutazione preventiva degli interessi prevalenti.

6.3 Resoconto sommario sedute delle Commissioni permanenti e speciali

Il resoconto sommario delle sedute di Commissione è lo strumento che assicura la pubblicità dei lavori. Difatti, ai sensi del Regolamento interno del Consiglio regionale della Calabria (art. 85), le sedute delle Commissioni non sono pubbliche e la pubblicità di tutti i lavori è assicurata mediante sia la pubblicazione dei resoconti sommari, sia di servizi telematici sul progredire dei lavori e sulle decisioni assunte. Il resoconto sommario dà conto degli interventi dei consiglieri regionali, dei componenti della Giunta regionale e per prassi dei rappresentanti dei Settori di Giunta e Consiglio regionale nonché delle fasi procedurali, degli atti approvati e degli esiti delle votazioni.

Nel corso delle sedute di Commissione, ai sensi dell'articolo 31 dello Statuto della Regione Calabria e dell'articolo 117 del Regolamento interno, possono essere auditi soggetti esterni all'amministrazione regionale, i cui interventi non saranno riportati in sintesi nel resoconto sommario.

Nello specifico quadro di garanzie a tutela dei diritti e delle libertà degli interessati in materia di privacy, il resoconto sommario sarà il risultato di un'attività organizzativa basata sui principi di **"privacy by design"** e **"privacy by default",** volti a prevenire la diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività delle Assemblee legislative. Pertanto, il resoconto sarà redatto procedendo preventivamente alla

minimizzazione dei dati degli interessati, nel caso dovessero emergere nel corso del dibattito, o alla loro esclusione ex ante, laddove non fossero necessari per garantire una fedele e completa sintesi dei lavori degli organi assembleari. Nel caso specifico di audizioni di soggetti esterni all'amministrazione regionale, si darà conto dell'avvenuta audizione, riportando esclusivamente il ruolo (qualità, appartenenza ad associazioni, comitati, sigle sindacali) da essi rivestito.

A titolo di esempio: se nel corso della seduta di Commissione il consigliere Tizio dovesse citare i dati personali di un cittadino, detti dati non saranno riportati nella sintesi del dibattito o saranno riportati soltanto nei limiti necessari a garantire, da un lato, una corretta pubblicità dei lavori e, dall'altro, la tutela dei diritti degli interessati, attraverso un bilanciamento e valutazione preventiva degli interessi prevalenti.

6.4 Resoconto integrale Commissioni

Il resoconto integrale delle sedute di Commissione è predisposto per la sua pubblicazione su richiesta del Presidente della Commissione medesima e riporta ogni singolo intervento degli oratori, compresi quelli di soggetti estranei alla pubblica amministrazione, come nel caso di audizioni in corso di seduta. I funzionari resocontisti sottopongono a revisione ogni intervento, nel rispetto assoluto dei concetti espressi e dello stile oratorio di ogni intervenuto.

Tutti i resoconti integrali per i quali è stata richiesta la pubblicazione sono riportati sul sito web istituzionale del Consiglio regionale, all'indirizzo www.consiglioregionale.calabria.it/portale, nelle apposite sotto sezioni di ogni singola Commissione, all'interno della sezione "Attività legislativa", cliccando sulla voce "resoconti integrali". Ogni resoconto integrale è "conservato" nell'archivio dell'Ufficio Resoconti stenografici e sommari posto all'interno del Segretariato generale.

Nello specifico quadro di garanzie a tutela dei diritti e delle libertà degli interessati in materia di privacy, il resoconto integrale sarà anch'esso il risultato di un'attività organizzativa basata sui principi di **"privacy by design"** e **"privacy by default"**, volta a prevenire la diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività delle Assemblee legislative.

I singoli funzionari resocontisti, cui spetta la revisione di primo livello del resoconto integrale, sono investiti della responsabilità di valutare, volta per volta, la presenza negli interventi di dati personali ulteriori e non necessari e, al fine di tutelare i diritti e le libertà degli interessati, provvederanno direttamente in fase di revisione alla minimizzazione dei predetti ulteriori dati.

Un ulteriore controllo sarà effettuato in fase di revisione di secondo livello prima del visto per la pubblicazione sul sito istituzionale.

Come per i resoconti integrali delle sedute di Consiglio regionale, particolare attenzione sarà posta alla minimizzazione di dati riguardanti riferimenti alla salute dell'interessato, al suo stato patrimoniale o a casi di cronaca giudiziaria che, rintracciabili con l'ausilio di qualunque motore di ricerca, rischiano di condannare il soggetto citato ad essere perennemente associato all'episodio della propria vita discusso nelle aule degli organi assembleari. Non di meno sarà tutelata la privacy dei soggetti esterni alla pubblica amministrazione che, a differenza delle sedute di Consiglio, possono prendere parte e intervenire nel corso delle sedute di Commissione.

A titolo di esempio: se nel corso della seduta di Commissione il soggetto esterno "Livio" dovesse presentarsi elencando oltre al nome ed alla qualifica anche, ad esempio, luogo e data di nascita, detti ultimi dati non saranno riportati. Saranno, quindi, esclusivamente riportati quei dati necessari a garantire, da un lato, una corretta pubblicità dei lavori e, dall'altro, la tutela dei diritti degli interessati, attraverso un bilanciamento e valutazione preventiva degli interessi prevalenti.

7. Attività politica, di indirizzo e di controllo - sindacato ispettivo

La base giuridica del trattamento, cioè ciò che autorizza legalmente il trattamento dei dati sotto riportati, è rinvenibile dal combinato disposto di diverse norme di rango sia nazionale sia regionale. Lo Statuto della Regione Calabria all'articolo 9 sancisce il diritto del cittadino ad una informazione costante sull'attività istituzionale, giudicandola presupposto fondamentale della partecipazione ed un aspetto essenziale dei diritti del cittadino e, per tali ragioni, la Regione assicura la più ampia informazione sugli atti, sui programmi e sulle iniziative di propria competenza, nonché sul funzionamento dei propri organi ed uffici attraverso l'impiego di strumenti di informazione e di comunicazione di massa.

Nello specifico, gli atti di sindacato ispettivo (di indirizzo e di controllo) - rientranti tra le prerogative dei consiglieri regionali ai sensi dell'art. 24, comma 2, dello Statuto – sono disciplinati dagli articoli 86, comma 2, 91, 119, 120, 121, 122 e 123 del Regolamento interno del Consiglio regionale, che ne prevede anche le diverse forme di pubblicazione.

Il trattamento è poi consentito espressamente dall'articolo 2 *sexies,* lett. f) e h) del Codice Privacy (D.Lgs. 196/2003 e ss.mm.ii.) che riconosce un rilevante interesse pubblico, autorizzativo del trattamento di particolari categorie di dati (ai sensi dell'articolo 9, paragrafo 2, lettera g) del GDPR), sia in materia di documentazione delle attività istituzionali di organi pubblici, sia per lo svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo. A ciò si aggiunga l'interesse di archiviazione storica sotteso alle attività di assemblee rappresentative.

7.1. Atti di indirizzo e di controllo

Ogni consigliere può presentare una serie di atti di indirizzo e di controllo rivolti all'organo di governo (la Giunta regionale). Tali atti, che rientrano tra le prerogative dei consiglieri indicate all'art. 24, comma 2, dello Statuto, assumono la forma di:

- mozioni, risoluzioni e ordini del giorno (atti di indirizzo);

- interpellanze, interrogazioni (atti del c.d. sindacato ispettivo o di controllo).

Gli atti di indirizzo e controllo sono disciplinati, per quanto attiene forme e procedure, nel Regolamento interno del Consiglio regionale.

Mozioni: La mozione è un documento motivato, sottoscritto da uno o più consiglieri, che ha lo scopo di promuovere una deliberazione del Consiglio per concorrere a determinare l'indirizzo politico, sociale ed economico della Regione.

Risoluzioni: La risoluzione è un atto diretto a manifestare orientamenti su particolari questioni o a definire indirizzi su specifici argomenti per la propria attività e per l'attività della Giunta. Alle risoluzioni si applicano le norme sulle mozioni, per l'espresso rinvio operato dall'articolo 86, comma 2, del Regolamento interno.

Ordini del giorno: L'ordine del giorno è un atto con il quale si promuove un pronunciamento del Consiglio sul contenuto di una legge sottoposta alla votazione dell'Aula (articolo 91 del Regolamento interno).

Interpellanze: L'articolo 120 del Regolamento interno prevede le interpellanze, quale strumento a disposizione di ciascun Consigliere per interpellare la Giunta sui motivi o gli intendimenti della sua condotta al fine di riscontrarne la coerenza con l'indirizzo politico e il programma di governo.

Interrogazioni: consistono principalmente in una o più domande rivolte alla Giunta regionale su materie che ne investano la competenza. Con le interrogazioni ogni consigliere può rivolgersi al Presidente e alla Giunta regionale per avere informazioni o spiegazioni su una questione determinata o per sapere se e quali provvedimenti siano stati adottati o si intendano adottare in relazione alla questione medesima. I consiglieri devono specificare se chiedono risposta scritta o risposta immediata. L'articolo 10 comma 2 dello Statuto della Regione Calabria (LR 19/10/2004, n. 25), prevede che anche <<*I Comuni e le Province possono rivolgere interrogazioni alla Regione su questioni di loro interesse, con le procedure previste nel Regolamento interno del Consiglio regionale*>>. La procedura ivi prevista ricalca quanto sancito in materia di interrogazioni a risposta scritta secondo quanto disciplinato all'articolo 123 del Regolamento interno del Consiglio regionale (Interrogazioni presentate dagli Enti locali).

Solo nel caso delle interrogazioni, secondo le disposizioni contenute nel Regolamento interno, siano esse a riposta scritta o immediata, si procede al loro repentino inoltro alla Giunta regionale, che provvederà ad assegnarle al dipartimento competente per materia.

Gli atti sopra descritti vengono acquisiti al protocollo dell'Ente e, una volta assegnato un numero progressivo, il loro contenuto viene pubblicato nella rispettiva sezione dedicata sul sito web del Consiglio regionale, all'indirizzo www.consiglioregionale.calabria.it/ portale, e sono consultabili al link "banche dati e documentazione" cliccando sulla voce "atti di indirizzo e controllo".

Tutti gli atti sono "conservati" nell'archivio posto all'interno del Settore Segreteria Assemblea e Affari Generali e nell'archivio documentale del Consiglio regionale della Calabria ai sensi del suo manuale di conservazione.

Per quanto attiene il rispetto della normativa in materia di privacy, posto che anche i consiglieri regionali sono tenuti ad osservare quanto prescritto dalla normativa in materia di minimizzazione dei dati, la fase antecedente alla pubblicazione online degli atti di indirizzo e controllo è il risultato di un'attività organizzativa basata sui principi di **"privacy by design"** e **"privacy by default",** volti a prevenire l'eventuale diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività di indirizzo e controllo esercitata dai consiglieri regionali. Pertanto, si procederà preventivamente alla pseudonimizzazione dei dati presenti nel testo, provvedendo al loro opportuno oscuramento.

Tale attività sarà svolta anche con riferimento alle risposte alle interrogazioni provenienti dalla Giunta regionale.

A titolo di esempio: la pseudonimizzazione dei dati avrà ad oggetto gli eventuali riferimenti alla salute di un soggetto, al suo stato patrimoniale, a casi di cronaca giudiziaria citati nel testo dell'atto di indirizzo e controllo, o a procedimenti disciplinari in corso, o ai dati personali di un cittadino, ecc.

Vengono sempre oscurate le firme autografe dei proponenti.

8. Proposte/disegni di legge, proposte di provvedimento amministrativo, pareri su deliberazioni di Giunta regionale

La base giuridica del trattamento, e cioè ciò che autorizza legalmente il trattamento dei dati sotto riportati, è rinvenibile dal combinato disposto di diverse norme di rango sia nazionale, sia regionale. Lo Statuto della Regione Calabria, all'articolo 9, sancisce il diritto del cittadino ad una informazione costante sull'attività istituzionale, giudicandola presupposto fondamentale della partecipazione ed un aspetto essenziale dei diritti del cittadino e per tali ragioni la Regione assicura la più ampia informazione sugli atti, sui programmi e sulle iniziative di propria competenza, nonché sul funzionamento dei propri organi ed uffici attraverso l'impiego di strumenti di informazione e di comunicazione di massa.

In relazione al trattamento sotto descritto lo Statuto della Regione Calabria, all'articolo 39, prevede a chi competa l'iniziativa legislativa e il Regolamento interno del Consiglio regionale della Calabria all'articolo 63, commi 2 e 3, ne indica le modalità di esercizio.

Il trattamento è poi consentito espressamente dall'articolo 2 *sexies,* lett. f) e g) del Codice Privacy (D.Lgs. 196/2003 e ss.mm.ii.), che riconosce un rilevante interesse pubblico, autorizzativo del trattamento di particolari categorie di dati (ai sensi dell'articolo 9, paragrafo 2, lettera g) del GDPR), sia in materia di documentazione delle attività istituzionali di organi pubblici, sia in materia di esercizio del mandato degli organi rappresentativi. A ciò si aggiunga l'interesse di archiviazione storica sotteso alle attività di assemblee rappresentative.

8.1. Proposte/disegni di legge

Ai sensi dell'articolo 39 dello Statuto della Regione Calabria, l'iniziativa legislativa compete "*alla Giunta, a ciascun Consigliere regionale, a ciascun Consiglio provinciale, a ciascun Consiglio comunale dei capoluoghi di Provincia, a non meno di tre Consigli comunali, la cui popolazione sia complessivamente superiore a diecimila abitanti, agli elettori della Regione in numero non inferiore a cinquemila, nonché al Consiglio delle Autonomie Locali*".

L'articolo 63, commi 2 e 3 del Regolamento interno del Consiglio dispone che la suddetta iniziativa si esercita "*mediante la presentazione al Presidente del Consiglio di proposte redatte in articoli, illustrate da una relazione descrittiva e, nel caso comportino spese a*

carico del bilancio regionale, da una relazione tecnico-finanziaria". Le proposte di iniziativa dell'esecutivo regionale devono essere corredate anche dalla relativa delibera di Giunta.

Tutte le proposte legislative, una volta acquisite al protocollo dell'Ente, sono contrassegnate da un numero progressivo e assegnate alle Commissioni consiliari competenti. Successivamente sono pubblicate nell'apposita sezione del sito web del Consiglio regionale, all'indirizzo www.consiglioregionale.calabria.it/, e consultabili al link "proposte di legge" cliccando sulla voce corrispondente. Il cartaceo di ciascun provvedimento è "conservato" in appositi fascicoli tenuti nell'archivio del Settore Segreteria Assemblea e Affari generali.

Nel rispetto dei principi di "**privacy by design"** e **"privacy by default"** che mirano a prevenire la diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività delle Assemblee legislative, ciascuna proposta di legge è pubblicata sul sito istituzionale procedendo preventivamente alla pseudonimizzazione dei dati presenti nel testo, tramite il loro opportuno oscuramento.

A titolo di esempio, vengono oscurate le firme dei proponenti, laddove autografe, incluse quelle dei componenti della Giunta regionale e dei dirigenti dei dipartimenti regionali riportate nella delibera di Giunta allorquando l'iniziativa legislativa competa all'esecutivo regionale, nonchè gli eventuali riferimenti, nell'articolato e/o nelle relazioni illustrativa e tecnico finanziaria a corredo di una proposta di legge, a dati di persone fisiche o giuridiche (nel caso si tratti di ditte individuali) nei cui confronti la Regione o il Consiglio regionale dovrà corrispondere un debito fuori bilancio derivante da una delle fattispecie di cui all'articolo 73, comma 1 del d.lgs 118/2011, la cui legittimità deve essere riconosciuta con legge regionale.

Da ultimo, per le proposte di legge di iniziativa popolare, si evidenzia che, nel sottoscrivere la proposta, i firmatari sono informati ai sensi del GDPR e prestano il consenso al trattamento dei dati personali. Consentono, altresì, alla loro comunicazione e diffusione ai soggetti promotori ed aderenti alla proposta di legge regionale di iniziativa popolare, al Consiglio regionale ed agli Uffici elettorali per le finalità inerenti all'iniziativa.

8.2. Proposte di provvedimento amministrativo

Le proposte di provvedimento amministrativo riguardano prevalentemente atti di programmazione regionale (ad esempio, il DEFR) ed europea (Programmi operativi regionali FESR-FSE, FEASR, PAC), documenti contabili di enti strumentali regionali (bilanci di previsione e rendiconti), la cui iniziativa compete alla Giunta regionale. Rientrano nel novero di tali proposte anche le proposte di legge alle Camere ai sensi dell'art. 121, comma 2, Costituzione, di iniziativa di Consiglieri regionali o della Giunta regionale, nonché i provvedimenti rientranti nell'autonomia contabile e funzionale dell'Assemblea (bilancio di previsione, rendiconto, assestamento, variazioni al bilancio, riaccertamento dei residui attivi e passivi), la cui iniziativa compete all'Ufficio di Presidenza, sentita, ove previsto da specifiche norme regolamentari, la Conferenza dei Presidenti dei Gruppi (art. 63, comma 5, Regolamento interno del Consiglio regionale).

Infine, le proposte di provvedimento amministrativo di iniziativa d'ufficio afferiscono a procedure previste da leggi regionali (ad esempio, le nomine di competenza del Consiglio regionale ai sensi della legge regionale n. 39/1995) oppure dal Regolamento interno (ad esempio, elezione del Presidente e dell'Ufficio di Presidenza del Consiglio e delle Commissioni consiliari permanenti e speciali; sostituzioni di Consiglieri regionali dimissionari; nomine e incarichi di Consiglieri regionali all'interno di un determinato organo, collegio o commissione, in base a disposizioni di legge o statutarie).

Le proposte di provvedimento amministrativo, una volta acquisite al protocollo dell'Ente, sono contrassegnate da un numero progressivo e assegnate alle Commissioni consiliari competenti, ad eccezione dei provvedimenti di iniziativa dell'Ufficio di Presidenza e d'ufficio. Successivamente sono pubblicate nell'apposita sezione del sito web del Consiglio regionale, all'indirizzo www.consiglioregionale.calabria.it/, e consultabili al link "proposte di provvedimento amministrativo" cliccando sulla voce. Il cartaceo di ciascun provvedimento è "conservato" in appositi fascicoli tenuti nell'archivio del Settore Segreteria Assemblea e Affari generali.

Nell'ambito del quadro di garanzie a tutela dei diritti e delle libertà degli interessati in materia di privacy, nel rispetto dei principi di "**privacy by design"** e **"privacy by default"** che mirano a prevenire la diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il

perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività delle Assemblee legislative, ciascuna proposta di provvedimento amministrativo è pubblicata sul sito istituzionale procedendo preventivamente alla pseudonimizzazione dei dati presenti nel testo, tramite il loro opportuno oscuramento.

A titolo di esempio, vengono oscurate le firme, laddove autografe, dei componenti della Giunta regionale e dei dirigenti dei dipartimenti regionali riportate nella delibera di Giunta, o dei componenti dell'Ufficio di Presidenza del Consiglio, nonchè gli eventuali dati personali e firme autografe di rappresentanti legali di enti strumentali regionali per le proposte riguardanti documenti contabili di detti enti.

8.3. Pareri su deliberazioni di Giunta regionale

A mente dell'articolo 87, comma 1 del Regolamento interno del Consiglio regionale, "*qualora specifiche disposizioni legislative prevedano il parere di una Commissione consiliare su di un regolamento o provvedimento amministrativo della Giunta regionale, il Presidente del Consiglio assegna la pratica alla Commissione competente, che la esamina nella prima seduta utile e comunque entro il termine di scadenza previsto dalle vigenti disposizioni legislative*".

Una volta acquisiti al protocollo dell'Ente, i suddetti provvedimenti sono contrassegnati da un numero progressivo e assegnati alla/e Commissione/i consiliare/i competente/i e successivamente pubblicati nell'apposita sezione del sito web del Consiglio regionale, all'indirizzo www.consiglioregionale.calabria.it/, e consultabili al link "Pareri" cliccando sulla voce. Il cartaceo di ciascun provvedimento è "conservato" in appositi fascicoli tenuti nell'archivio del Settore Segreteria Assemblea e Affari generali.

Nell'ambito del quadro di garanzie a tutela dei diritti e delle libertà degli interessati in materia di privacy, nel rispetto dei principi di "**privacy by design"** e **"privacy by default"** che mirano a prevenire la diffusione di dati personali ulteriori rispetto a quelli necessari a garantire il perseguimento dell'interesse pubblico all'attuazione dei principi di trasparenza, pubblicità e informazione dell'attività delle Assemblee legislative, ciascun parere su deliberazione di Giunta è pubblicato sul sito istituzionale procedendo preventivamente alla pseudonimizzazione dei dati presenti nel testo, tramite il loro opportuno oscuramento.

A titolo di esempio, vengono oscurate le firme, laddove autografe, dei componenti della Giunta regionale e dei dirigenti dei dipartimenti regionali riportate nella delibera di Giunta, nonché gli eventuali dati personali di soggetti menzionati all'interno del provvedimento.

9. Istanza per l’esercizio del diritto di cancellazione dei dati personali (diritto all’oblio)

L’articolo 17 del GDPR (General Data Protection Regulation), sotto la rubrica “Diritto alla cancellazione”, disciplina il c.d. diritto all’oblio, vale a dire i casi in cui l’interessato può richiedere la cancellazione dei propri dati personali, nonché le specifiche deroghe all’obbligo di cancellazione.

Precisamente, il paragrafo 1 del citato articolo sancisce il diritto di ottenere dal titolare del trattamento, la cancellazione dei propri dati se sussiste uno dei seguenti motivi:

“a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; [(27)]

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.”

Inoltre, ai sensi del successivo **paragrafo 2**, se i dati personali risultano pubblicati sul sito internet del titolare del trattamento, quest’ultimo, oltre a cancellarli, è tenuto a comunicare l'avvenuta cancellazione (**c.d. deindicizzazione indiretta**) della pagina anche ai motori di ricerca, per far sì che essi, a loro volta, come titolari del trattamento, provvedano a cancellare qualsiasi link, copia o riproduzione dei dati personali del richiedente.

A tal proposito, si precisa che è possibile per l'interessato, al fine di impedire il facile accesso ad una notizia che lo riguardi, invece che rivolgersi al titolare del sito in cui è pubblicata l'informazione con i dati personali, presentare la diversa **istanza di deindicizzazione diretta** (c.d. de-listing) direttamente al motore di ricerca (indicando specificamente gli URL che si intendono allontanare dal proprio nome), che andrà ad effettuare la dissociazione delle ricerche sul web collegate con il nome dell'interessato, cioè rimuoverà il riferimento indesiderato dai risultati di ricerca, senza incidere sulla presenza del dato sul web.

In merito a tale possibilità, Google, ad es., ha istituito un "*Advisory Council on the right to be forgotten"*, con il compito di valutare le istanze di deindicizzazione. La procedura prevista per ottenere la deindicizzazione è stata strutturata in modo semplice per l'interessato, il quale si limiterà ad indicare le pagine indesiderate associate al proprio nome compilando un modulo online. Deve però sussistere la particolare connessione tra il proprio nome e il dato e vanno indicate le ragioni che giustificano l'obsolescenza e l'irrilevanza della sua presenza su internet.

Tuttavia, sia nel primo, sia nella seconda ipotesi, il **paragrafo 3** dell'articolo 17 del GDPR, elenca i casi in cui non si può far luogo alla cancellazione, "*nella misura in cui il trattamento sia necessario*:

a) *per l'esercizio del diritto alla libertà di espressione e di informazione;*

b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria".

Si precisa che, nel caso in cui il **Consiglio regionale della Calabria, quale titolare del trattamento, non proceda** alla cancellazione o non comunichi l'avvenuta cancellazione all'interessato, quest'ultimo può rivolgersi all'**autorità di controllo** (Garante della privacy) o a quella giudiziaria per far valere il proprio diritto all'oblio.

La richiesta di cancellazione **non deve avere una forma particolare** (ad es. basta una pec o un'email oppure una lettera racc. A/R). Tuttavia, è importante che la richiesta **permetta al titolare del trattamento l'identificazione** dell'interessato per procedere alla cancellazione dei dati che lo riguardano.
Di seguito, si può trovare, a mero titolo esemplificativo, un fac-simile per la richiesta di cancellazione.

Fac simile

Spett.le

CONSIGLIO REGIONALE DELLA CALABRIA

Via Cardinale Portanova

89128 Reggio Calabria

pec: consiglioregionale@pec.consrc.it o email: consiglioregionale@consrc.it

(in mancanza di un indirizzo email o pec del mittente, è possibile inviare una raccomanda cartacea A/R all'indirizzo di cui sopra)

Oggetto: Istanza per l'esercizio del diritto di cancellazione dei dati personali ai sensi dell'art. 17 del Regolamento (UE) 2016/679 (c.d. diritto all'oblio).

Il/La sottoscritto/a…… nato/a a……. il ……, con la presente inoltra formale richiesta di cancellazione, nei termini di legge, dei dati personali che riguardano lo/la scrivente, sussistendo uno dei motivi previsti dal paragrafo 1 dell'art. 17 del Regolamento (UE) 2016/679 *(specificare quale)*

……
……

oppure in caso richiesta da parte di un delegato:

Il/La sottoscritto/a……. nato/a a……. il……, **su delega del signor/della signora** ……..…… nato/a…… a ……. il……, con la presente inoltra formale richiesta di cancellazione, nei termini di legge, dei dati personali che riguardano il delegante,

sussistendo uno dei motivi previsti dal paragrafo 1 dell'art. 17 del Regolamento (UE) 2016/679 *(specificare quale)*

……
……

Nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, lo/la scrivente chiede, inoltre, che, in caso di accoglimento, il titolare destinatario della presente istanza attesti di aver informato gli altri titolari di trattamento della richiesta in questione, finalizzata, altresì, alla cancellazione di link, copie o riproduzioni dei suoi dati personali.

In caso contrario, lo/la scrivente chiede:

- di essere informato/a, ai sensi dell'art. 12, par. 4 del GDPR 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di svolgere le operazioni richieste e se tale termine potrà essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste;
- in particolare, di essere informato/a della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, par. 2, del GDPR 2016/679.

Si indica, qui di seguito, il recapito per la risposta:

Via ……

Comune…….. Provincia (…) CAP …..

Oppure

E-mail …… Pec: …….

Si allega, in ultimo, la seguente documentazione:

1) copia del documento di identità del/della richiedente (sottoscritto con firma autografa nel caso in cui l'istanza venga inoltrata tramite e-mail);
2) eventuale delega sottoscritta dal/dalla delegante;

(N.B. Nel caso di richiesta da parte di un soggetto delegato, è necessario allegare copia di un documento di riconoscimento del delegato, nonché copia di un documento di riconoscimento del delegante, ciascuna riportante la firma autografa della persona a cui si

riferisce, se l'istanza è inoltrata per e-mail. In caso di richiesta da parte di un genitore, è necessario allegare, inoltre, la Dichiarazione sostitutiva di certificazione attestante il grado di parentela (art. 47 D.P.R. 28 dicembre 2000, n. 445) senza autentica di sottoscrizione);

3) copia di altro documento occorrente.

Luogo e data _____

Firma del richiedente

_____[12]

Informativa sul trattamento dei dati personali rilasciata ai sensi dell'art. 13 GDPR 2016/679.

Informiamo che i dati personali da Lei forniti al Consiglio regionale della Calabria saranno trattati secondo quanto previsto dal "*Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento Generale sulla Protezione dei dati, di seguito GDPR)"*.

I dati personali a Lei riferiti verranno raccolti e trattati nel rispetto dei principi di correttezza, liceità e tutela della riservatezza, con modalità informatiche ed esclusivamente per finalità di trattamento dei dati personali dichiarati nella richiesta di che trattasi e comunicati agli uffici regionali o alle amministrazioni individuate come competenti a valutarla.

Il trattamento è finalizzato all'esercizio dei diritti previsti dall'art. 17 del GDPR. I dati acquisiti saranno utilizzati esclusivamente per la trattazione dell'istanza pervenuta o resi anonimi per finalità statistiche.

[12] Oltre alla firma autografa, è ammessa la firma digitale, ma in questo caso l'inoltro dovrà avvenire tramite posta elettronica (email o PEC)

Il conferimento dei Suoi dati ed il relativo trattamento sono obbligatori in relazione alle finalità sopra descritte; ne consegue che l'eventuale rifiuto a fornirli potrà determinare l'impossibilità del Titolare del trattamento ad erogare il servizio richiesto.

Il Titolare del trattamento dei dati personali è il Consiglio regionale della Calabria.

I dati di contatto del Responsabile della protezione dati (DPO) del Consiglio regionale della Calabria sono: email: rpd@consrc.it, pec: rpd@pec.consrc.it, indirizzo Via Cardinale Portanova snc, 89123 Reggio Calabria.

I dati saranno trattati esclusivamente da soggetti incaricati autorizzati ed istruiti in tal senso, adottando tutte quelle misure tecniche ed organizzative adeguate per tutelare i diritti, le libertà e i legittimi interessi che Le sono riconosciuti per legge in qualità di Interessato.

I dati personali indicati nel presente modulo saranno utilizzati esclusivamente per poter fornire riscontro all'istanza e saranno conservati per un tempo illimitato secondo l'attuale Piano di Conservazione dell'ente o come diversamente previsto nel caso di modifica dello stesso.

I dati personali non saranno in alcun modo oggetto di trasferimento in un Paese terzo extra europeo, né di comunicazione a terzi fuori dai casi previsti dalla normativa in vigore, né di processi decisionali automatizzati compresa la profilazione. Lei potrà esercitare il diritto di proporre reclamo all'Autorità di controllo competente (Garante per la protezione dei dati personali: garante@gpdp.it).

10. GLOSSARIO PRIVACY

Introduzione

Quando si parla del nuovo Regolamento UE 2016/679, (GDPR Privacy), si fa riferimento a tutta una serie di nuove definizioni, che in alcuni casi si vanno a sovrapporre a quelle già esistenti nel nostro ordinamento giuridico, in particolare dopo le modifiche e gli aggiornamenti apportati dal nuovo "Codice Privacy" (D.lgs. 196/2003) coordinato con il D.lgs. 101/2018 che integra la materia in questione recependo il GDPR UE 2016/679.

Come adeguarsi e come completare il processo di adattamento, secondo quanto previsto dall'attuale regolamento, resta il motivo fondante sul quale la PA italiana sta lavorando e formando il proprio personale.

Per iniziare è tuttavia necessario comprendere i concetti basilari, le definizioni essenziali che vanno a completare l'ambito della normativa in materia di Privacy, dopo l'entrata in vigore del GDPR 2016/679.

Di seguito, il glossario contenente le definizioni dei termini più rilevanti in materia di Privacy, con particolare riferimento a quanto enunciato negli articoli che costituiscono il GDPR 2016/679:

A	
Accountability (responsabilizzazione)	Principio di "responsabilizzazione" dei titolari e dei responsabili del trattamento dei dati a cui è richiesto di adottare tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è coerente con quanto previsto dal Regolamento UE 2016/679.
Anonimizzazione	È la trasformazione irreversibile dei dati personali che fa sì che le persone fisiche interessate non possano essere più identificate.
Archivio (Database)	Archivio elettronico che raccoglie un insieme di dati organizzati e memorizzati in forma strutturata e omogenea.

Atto amministrativo	Qualunque dichiarazione di volontà, di desiderio, di conoscenza, di giudizio compiuta da soggetti attivi della Pubblica Amministrazione nello svolgimento delle proprie funzioni.
Autorità di controllo	Autorità pubblica indipendente chiamata a controllare il rispetto delle norme vigenti sulla Privacy. È stata istituita in ciascun Paese dell'UE ai sensi dell'articolo 51 del Regolamento UE, 2016/679.
B	
Base giuridica del trattamento	È ciò che autorizza legalmente il trattamento dei dati. Il titolare del trattamento deve rispettare le condizioni previste dall'art. 6 del GDPR/2016 ed essere sempre in grado di dimostrare la correttezza della scelta effettuata. Deve essere indicata nell'informativa rivolta agli utenti.
Big Data	Insieme di dati presenti in database, che formano un patrimonio informativo così complesso e strutturato da richiedere l'utilizzo di nuovi strumenti e tecnologie per l'estrazione, la gestione e l'analisi dei dati stessi.
C	
Codice di condotta	È lo strumento che ha lo scopo di indicare le regole di protezione dei dati per i titolari e i responsabili del trattamento. Gli articoli 40 e seguenti del GDPR regolamentano le procedure di presentazione e approvazione dei Codici di condotta.
Codice privacy	Il "Codice in materia di protezione dei dati personali" del 30 giugno 2003 n. 196, detto anche "Testo unico sulla privacy", entrato in vigore il primo gennaio 2004, contiene le norme nazionali relative alla tutela dei dati personali. È stato integrato ed aggiornato dal D.lgs. del 10 agosto 2018, n. 101, che recepisce le modifiche introdotte con l'entrata in vigore, il 25 maggio 2018, del GDPR UE 2016/679.
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale manifesta l'assenso al trattamento dei dati personali.
Contitolare del trattamento	Si parla di contitolarità quando due o più titolari determinano congiuntamente "perché" e "come" debbano essere trattati i dati personali.
D	

Data retention **(Periodo di conservazione dei dati)**	È il periodo oltre il quale i dati personali devono essere cancellati. È legato alle finalità specifiche per le quali sono stati raccolti. Difatti, il medesimo dato, se utilizzato per differenti finalità, potrebbe avere tempi di conservazione diversi.
Dati biometrici	Dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono, o confermano, l'identificazione univoca.
Dati genetici	Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute della stessa.
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile.
Dati personali particolari (ex sensibili)	Si tratta di dati "sensibili", cioè che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale oppure informazioni relative alla salute o alla vita sessuale.
Dati sanitari	Dati che rivelano lo stato di salute fisica o mentale di un individuo.
Dati relativi a condanne penali e reati	Dati che possono rivelare l'esistenza di provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o di indagato di un individuo. Il Regolamento UE 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali, ai reati e alle connesse misure di sicurezza.
Destinatario	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che riceve comunicazione di dati personali.
Diritto all'oblio	Consiste nel diritto di ogni persona di richiedere la cancellazione dei dati personali se ricorrono determinate fattispecie previste dall'art.17 del GDPR UE 2016/679.
Diritto alla deindicizzazione	Il diritto alla deindicizzazione non elimina definitivamente il dato, ma lo rende non direttamente accessibile tramite motori di ricerca esterni all'archivio in cui quel contenuto si trova.
Diritto alla portabilità	L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati che lo riguardano forniti al titolare e di trasmettere i propri dati da un titolare ad un altro titolare, senza impedimenti da parte di colui al quale sono stati forniti precedentemente.
Diritto alla rettifica	Il diritto di chiedere al titolare del trattamento dei dati la rettifica di dati personali inesatti.

Diritto di opposizione	Diritto di opporsi al trattamento dei propri dati personali. È possibile per motivi connessi alla situazione particolare dell'interessato (da specificare nella richiesta) oppure quando i dati sono trattati per finalità di marketing diretto (senza necessità di motivare l'opposizione).
G	
Garante Privacy	Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente, istituita dalla cosiddetta "Legge sulla privacy". È l'autorità di controllo designata ai fini dell'attuazione del Regolamento Generale sulla Protezione dei Dati Personali UE 2016/679 (art. 15).
Glossario	Il glossario è un piccolo dizionario di termini specialistici relativi ad una determinata materia ed ambito, in questo caso la privacy.
I	
Informativa	Nota con la quale la pubblica amministrazione informa i cittadini, i destinatari e tutti i potenziali interessati sulla modalità del trattamento dei dati e sull'applicazione di quanto previsto dalla normativa vigente in materia di privacy, sulle procedure attuate dall'ente titolare dei dati, sulla loro protezione e sicurezza e sulla finalità degli stessi. È resa ai sensi dell'art. 13 del Regolamento UE n. 679 del 27 aprile 2016, "General Data Protection Regulation" (G.D.P.R.).
Interessato	Si tratta della persona fisica alla quale si riferiscono i dati raccolti o in trattamento (articolo 4, paragrafo 1, punto 1 del Regolamento UE 2016/679).
Istanza di accesso	L'istanza di accesso è lo strumento tramite il quale l'interessato (la persona fisica cui i dati si riferiscono) può chiedere ed ottenere in forma intellegibile i dati in possesso del titolare.
L	
Limitazione di trattamento	Diritto dell'interessato a fari sì che i suoi dati siano utilizzati limitatamente a quanto necessario ai fini della loro conservazione (art. 18 del GDPR 2016/679).
M	

Minimizzazione	Il titolare del trattamento dei dati è tenuto a rilevare i dati strettamente necessari al raggiungimento delle finalità per le quali vengono raccolti. I dati, pertanto, devono essere adeguati, pertinenti ed esatti rispetto al fine che si intende perseguire, ed essi non possono essere raccolti in misura ulteriore a quella prescritta (art. 5 del GDPR 2016/679).
N	
Normativa	L'insieme delle norme che regolano una determinata materia o presiedono alla disciplina di un istituto, di un ordinamento giuridico.
O	
Organizzazione	Modalità di divisione e coordinamento del lavoro in una logica di sistema che definisce gli organi, gli aggregati di attività, i compiti, le relazioni fra organi, il grado di autonomia decisionale delle unità organizzative, la comunicazione e altri meccanismi di gestione e governo di una struttura.
P	
Persona fisica	Nell'ordinamento giuridico si definisce persona fisica ogni essere umano. È soggetto di diritto, ossia centro di imputazione di situazioni giuridiche.
Persona giuridica	La persona giuridica è un insieme di persone fisiche (enti, autorità ed organizzazioni in genere) che perseguono determinati obiettivi di interesse collettivo. Le persone giuridiche sono soggetto di diritto, vale a dire che la legge attribuisce loro la possibilità di agire nell'ordinamento giuridico per la realizzazione e la difesa dei propri interessi.
Privacy	Il termine inglese privacy fa riferimento all'insieme di informazioni personali che non vogliamo diventino di dominio pubblico senza il nostro consenso. La tutela della privacy ha acquistato un'importanza centrale con la diffusione delle tecnologie della comunicazione e con la nascita di banche dati in cui sono raccolte informazioni personali di tutti i tipi.
Privacy by default	Criterio che presuppone misure che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.
Privacy by design	Criterio che richiede che il titolare del trattamento dei dati personali adotti misure tecniche e organizzative idonee sin dal momento della progettazione del trattamento dei dati personali.

Procedimento	Successione di atti di più soggetti e di diversa natura che portano all'atto amministrativo vero e proprio.
Profilazione	Attività di raccolta ed elaborazione dei dati inerente gli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento.
Pseudonimizzazione	Trattamento dei dati personali che prevede l'oscuramento o la sostituzione parziale dei dati personali di un soggetto in modo da impedirne l'identificazione senza l'utilizzo di informazioni aggiuntive.
Pubblicazione	Modalità con cui si porta a conoscenza di tutti un atto o il suo contenuto. È realizzabile attraverso la stampa, l'affissione o la diffusione nel sito istituzionale di un ente.
R	
Rappresentante del titolare	È una persona fisica o giuridica, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto (articolo 27 del GDPR), chiamata a rappresentarli per adempiere agli obblighi previsti dal Regolamento UE 2016/679.
Registri delle attività di trattamento	Documento redatto dal titolare e dal responsabile in forma cartacea o elettronica, disciplinato dall'art. 30 del GDPR UE 2016/679, in cui sono indicate le caratteristiche, le modalità e le finalità dei trattamenti effettuati.
Regolamento privacy	"Regolamento Generale sulla Protezione dei Dati personali" del 2016, numero 679, del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR- General Data Protection Regulation).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Responsabile protezione dati (RPD)	"Data Protection Officer" (DPO): responsabile della protezione dei dati personali. Si tratta di una nuova figura che ha il compito di facilitare l'osservanza e l'attuazione del GDPR 2016/679 da parte del titolare/responsabile e la cui designazione è obbligatoria nelle specifiche ipotesi indicate dall'art. 37 del Regolamento UE 2016/679.
Revoca del consenso	Diritto dell'interessato a revocare il consenso prestato al trattamento dei propri dati personali. Si può attuare in qualsiasi momento e non pregiudica la liceità del trattamento basata sul consenso prima della revoca.
S	
Sanzione	La sanzione amministrativa è prevista dall'ordinamento giuridico italiano in caso di violazione di una norma. Nel caso specifico si fa riferimento alle violazioni previste dal Regolamento UE 2016/679.

T	
Titolare del trattamento	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.
Trasparenza	La trasparenza è intesa come accesso totale ai dati e dei documenti detenuti dalle pubbliche amministrazioni, attraverso gli strumenti della pubblicazione, dell'accesso agli atti e dell'accesso civico, al fine di favorire la partecipazione e il controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.
Trattamento	Operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali. Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
V	
Valutazione impatto del rischio **DPIA- Data privacy impact assestment**	Quando un determinato trattamento, tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità, può presentare un rischio elevato per i diritti e la libertà delle persone fisiche, il titolare, nei casi espressamente previsti dal GDPR UE 2016/679, deve effettuare una valutazione dei rischi connessi al trattamento di dati con l'obiettivo di identificare le misure più idonee per affrontarli.
Violazione di sicurezza (data breach)	Violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Riferimenti e note

Sito del Garante della Privacy

GARANTE PRIVACY

https://www.garanteprivacy.it/normativa-e-provvedimenti/gdpr-e-normativa-europea-e-internazionale