La necessaria applicazione dei principi di *data protection* al diritto di accesso dei consiglieri *ex* art. 43, c. 2, TUEL*

Valentina De Nicola

Abstract

Il contributo intende analizzare la necessità di individuare alcuni limiti all'esercizio del diritto *sui generis* riconosciuto dall'art. 43, c. 2, TUEL ai consiglieri comunali e provinciali, connessi al rispetto del diritto alla riservatezza ed alla protezione dei dati personali, ripercorrendo il cammino della tematica così come analizzata dalla giurisprudenza di merito e di legittimità in Italia a partire dal 2018, ricostruendo il frammentario quadro della disciplina normativa di tale ampio istituto e definendone i limiti e le esclusioni attraverso un'applicazione ragionata dei principi di *data protection*. La tematica, infatti, è stata sino ad oggi affrontata in un'ottica miope, che non consente la completa attuazione dei principi introdotti dal Regolamento (UE) 2016/679, e che ha visto per molto tempo la risoluzione del problema della tutela del dato personale dei soggetti interessati relegata alla semplice tutela, *ex post* rispetto all'esercizio del diritto, della riservatezza personale, richiamando i consiglieri al dovere di segreto in merito alle informazioni ottenute.

This paper aims at analysing the need for limits to the sui generis right, granted by art. 43, para. 2, TUEL to municipal and provincial councillors, on the respect of right to privacy and data protection. This has been considered throughout its history as analysed by the proper law and with its lawfulness in Italy since 2018, gathering all the pieces of regulations and laws of this wide institution, defining its limitations and exclusions, through the appropriate application of the data protection principles. The shortsighted analysis of this topic so far has not allowed for the full implementation of the EU regulation 2016/679 principles and has limited the issue of the personal data protection to the sole protection, ex post to the execution of the law, of personal privacy, bounding councillors to the obligations of confidentiality and secrecy.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Sommario

Keywords

accesso amministrativo – consiglieri - protezione dei dati personali – trasparenza - bilanciamento.

1. Introduzione. L'esercizio del diritto di accesso del consigliere Comunale e l'atteggiamento miope nei confronti della *data protection*

Sebbene la materia della protezione dei dati personali abbia trovato recentemente una grande attenzione da parte di operatori ed interpreti in quasi tutti i settori potenziali di applicazione, un atteggiamento miope nei confronti della stessa si deve registrare, a ben due anni dalla piena applicazione della disciplina comunitaria, con riferimento all'esercizio del diritto di accesso riconosciuto specificamente al consigliere comunale e provinciale dall'art. 43, c. 2, TUEL. Tale diritto, previsto nel nostro ordinamento al fine di facilitare l' espletamento delle funzioni istituzionali riconosciute a tali soggetti qualificati, benché si scontri potenzialmente con la tutela del soggetto che, ai sensi della l. 241/1990, chiameremo "controinteressato", è da sempre definito come diritto ampio, privo di limiti prodromici al suo esercizio, soggetto ad un mero controllo successivo nell' ottica del dovere di segreto che si impone sui soggetti attivi di tale fattispecie. Storicamente il problema della tutela della riservatezza dei soggetti eventualmente coinvolti dall' esercizio di tale diritto, che ci si appresta qui ad analizzare,

è stato risolto in modo molto semplice e lineare dalla dottrina e dalla giurisprudenza interessate: la tutela del diritto alla riservatezza dei terzi eventualmente coinvolti dalla richiesta di accesso non può essere opposta come limite specifico al diritto *ex* art. 43, c. 2, TUEL, considerato che il consigliere è in ogni caso tenuto al vincolo del segreto[1].
In sostanza, la soluzione unitariamente prospettata con riferimento al problema della tutela della riservatezza nel caso di specie concerne una tutela riconosciuta solamente *ex post* rispetto all'esercizio di tale diritto *sui generis*: ci si occupa della riservatezza solo dopo che il consigliere abbia acquisito le informazioni richieste, ponendo l'attenzione sul come eventualmente egli utilizzi questi dati.
Si ritiene sia proprio questa prospettata soluzione, unita alla confusione dei confini tra riservatezza personale e tutela dei dati personali come oggi la conosciamo, ad aver determinato una sorta di blocco nel sistema di corretta applicazione delle norme, tale per cui per molto tempo la *data protection* non sembrava poter trovare spazio adeguato nell'espletamento di tale specifico diritto di accesso.
Considerato però che l'esercizio di tale diritto di accesso comporta delle innegabili ricadute sulla tutela dei dati personali e sulla riservatezza degli interessati dei quali sia fatta menzione nei documenti oggetto di accesso, che non possono essere analizzate e risolte sotto la sola lente dell'obbligo di segreto, oggi si impone ad interpreti ed operatori del diritto una necessaria riflessione in merito. È necessario adottare un atteggiamento di apertura, volto ad indagare quale sia il vero ruolo che l' ordinamento deve essere in grado di riconoscere al diritto alla tutela dei dati personali anche con riferimento a questa fattispecie, rilevato come il diritto alla *data protection* assurga a diritto di rango costituzionale, che per sua natura ha la capacità di porsi in confronto continuo con gli altri interessi costituzionalmente riconosciuti e garantiti[2], e che non può certamente essere eliso aprioristicamente dall' equazione.
La questione è oggi particolarmente pregnante, se si considera anche che le richieste di accesso dei consiglieri seguono il progressivo e radicale processo di digitalizzazione dell'organizzazione e dell'attività amministrativa: sono particolarmente diffuse, infatti, le richieste aventi ad oggetto la possibilità di accedere ai gestionali informatici degli Enti (le istanze più diffuse hanno ad oggetto l' accesso al protocollo informatico ed al programma di contabilità), i quali si compongono anche, senza ombra di dubbio, di dati personali secondo la definizione data dall' art. 4, n. 6, Reg. (UE) 2016/679 al concetto di "archivio"[3]. Risulta sempre più necessario, dunque, procedere ad un'ana-

[1] Si veda, sul punto, TAR Sardegna, sez. II, 20 maggio 2014, n. 360, ma anche la più recente Trib. Trani, sez. Lavoro, 9 gennaio 2020, che ricorda come «Il diritto di accesso del consigliere comunale non conosce né i vincoli, né le limitazioni previsti dall'ordinario accesso di cui alla legge n. 241 del 1990, ed in particolare quelli relativi alla riservatezza dei terzi. La legge non prende dunque in considerazione la posizione di coloro che potrebbero opporsi all'accesso (cui accorda come unica protezione l'obbligo del segreto a carico del consigliere comunale, con possibilità di far eventualmente valere nelle sedi competenti la violazione di tale obbligo) e pertanto non è configurabile in materia alcun contro interessato».

[2] Cfr. A. Soro, *Discorso del presidente, in apertura alla presentazione della Relazione Annuale del 2019*, in *garanteprivacy.it*, laddove il diritto alla protezione dei dati personali è stato definito come «un diritto inquieto, perché in costante evoluzione e mai tiranno, perché capace di porsi sempre in equilibrio con gli interessi giuridici che di volta in volta vengano in rilievo».

[3] Si veda art. 4, n. 6, Reg. (UE) 2016/679 che definisce l'archivio come «qualsiasi insieme strutturato

lisi che tenga conto anche di principi di *data protection*, al fine di poter individuare il necessario e continuo contemperamento tra esigenza di accesso ai documenti ufficiali della Pubblica Amministrazione, da un lato, e la necessità di tutelare i dati personali dei soggetti eventualmente interessati, dall'altro[4].

Non solo. È di fondamentale importanza valutare come i principi concernenti la tutela dei dati personali si relazionino con tale diritto *sui generis*, al fine di evidenziare se lo stesso possa effettivamente dirsi privo di limitazioni prodromiche con riferimento al suo esercizio, o se invece, più coerentemente, esso debba essere riportato all' interno dei binari di cui agli artt. 5, 24, 25 e 32 Reg. (UE) 2016/679.

Tali considerazioni, che non si riflettono in un mero tuziorismo giuridico, si impongono come irrinunciabili considerato che, per l'Ente richiesto, risulta estremamente problematico determinare i limiti eventuali da apporre all'esercizio di tale diritto, stante l'assenza, ad oggi, di linee guida specifiche per effettuare il bilanciamento degli interessi in gioco, rilevato inoltre l'elevato rischio di contenzioso che si prospetta in tali casi a carico delle stesse Amministrazioni (per iniziativa del consigliere, nel caso l'accesso sia negato e/o sia parzialmente consentito, oppure per iniziativa dei controinteressati, nel caso in cui l'accesso sia consentito in modo integrale, senza limitazioni dipendenti dalla protezione dei loro dati personali).

Nel presente lavoro si cercherà pertanto di esporre le ragioni che consentono di affermare la necessaria applicazione dei principi di *data protection* all'esercizio del diritto di accesso *ex* art. 43, c. 2, TUEL, onde ricavare un sistema di tutele integrato che operino non solo *ex post* ma anche *ex ante*, all'atto della richiesta da parte del consigliere, nel pieno rispetto dei principi espressi dal Reg. (UE) 2016/679.

2. Profili giuridici del diritto di accesso ex art. 43, c. 2, TUEL

Prima di procedere con l'analisi ragionata delle motivazioni che consentono di affermare la necessaria applicazione dei principi di *data protection* all'esercizio del diritto di accesso specificamente riconosciuto a favore di consiglieri comunali e provinciali, si ritiene necessario evidenziare qui di seguito i tratti somatici di questo istituto, utili per una più corretta analisi della fattispecie. Il diritto di accesso in commento concerne la previsione normativa di cui all'art. 43, c. 2, del d.lgs. 267/2000 (TUEL), per cui i consiglieri comunali e provinciali, sia di maggioranza che di minoranza, hanno diritto di ottenere dagli uffici del Comune, nonché dalle loro aziende ed enti dipendenti, «tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato»[5]. L' articolo in questione riprende le disposizioni normative in materia di

di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico».

[4] Tale richiamo alla necessità di bilanciamento risulta previsto inoltre *ex professo* dal Regolamento (UE) 2016/679 (di seguito anche "Reg. (UE) 2016/679"), al considerando 154 ed all'art. 86 di cui si dirà in seguito.

[5] Nello specifico, la norma rubricata «diritti dei consiglieri» prevede che «I consiglieri comunali e provinciali hanno diritto di ottenere dagli uffici, rispettivamente, del comune e della provincia,

accesso agli atti, per finalità istituzionali, già individuate espressamente dall' art. 31, c. 5, della legge n. 142/1990, che hanno storicamente delineato un diritto di accesso per i consiglieri, ampio, non sottoposto ad alcuna valutazione preventiva da parte dell' Amministrazione richiesta (che non può indagarne le motivazioni), i cui unici limiti si individuano nel richiamo al riserbo effettuato oggi dallo stesso art. 43 TUEL, e nel disposto giurisprudenziale per cui la richiesta di accesso debba essere tesa «a comportare il minor aggravio possibile per gli uffici comunali e che non debba sostanziarsi in richieste assolutamente generiche ovvero meramente emulative[6]».

Nello specifico, tale diritto *sui generis,* che trova le sue radici nelle prerogative costituzionalmente garantite agli artt. 3 e 97 Cost., risulta ad oggi privo di limitazioni, purché vi sia una stretta inerenza tra il documento e le informazioni che vi sono contenute rispetto allo svolgimento del mandato elettivo dei soggetti qualificati a favore dei quali il diritto è riconosciuto: la *ratio* dello stesso è da rinvenire nel principio democratico dell' autonomia locale e della rappresentanza esponenziale, sicché lo stesso è direttamente funzionale non tanto all' interesse del consigliere, ma alla cura dell' interesse pubblico connesso al mandato conferito, controllando il comportamento degli organi decisionali dell' Amministrazione[7].

Si tratta, all'evidenza, di un diritto dai confini più ampi del diritto di accesso riconosciuto al cittadino nei confronti del Comune di residenza (art. 10 TUEL) o, più in generale, nei confronti della Pubblica Amministrazione, disciplinato dalla legge n. 241 del 1990. La *ratio* di tale maggiore ampiezza si ricava nel particolare *munus* espletato dal consigliere comunale: un diritto di accesso dai confini così ampi viene riconosciuto per permettere al consigliere di valutare con piena cognizione di causa la correttezza e l' efficacia dell' operato dell' Amministrazione, onde poter esprimere un giudizio consapevole sulle questioni di competenza della P.A., «opportunamente considerando il ruolo di garanzia democratica e la funzione pubblicistica da questi esercitata, soprattutto se, come nel caso di specie, il consigliere comunale appartenga alla minoranza, istituzionalmente deputata allo svolgimento di compiti di controllo e verifica dell'operato della maggioranza[8]». Da ciò ne discende la definizione ampia dei limiti riconosciuti dall' ordinamento a tale diritto, tutti intrinsecamente legati alla funzione di garanzia svolta dal consigliere, tale per cui dovranno essere rispettate alcune forme e modalità di esercizio occorrendo valutare di volta in volta se «le istanze di

nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato. Essi sono tenuti al segreto nei casi specificamente determinati dalla legge».

6 Cfr. *ex multis* Cons. Stato, sez. IV 12 febbraio 2013, n. 846, Cons. Stato, sez. V, 29 agosto 2011, n. 4829 e recentemente TAR Campania, sez. VI, 7 novembre 2018, n. 6480. Si tenga anche conto del parere del 9 aprile 2014 fornito dalla Commissione per l'Accesso ai Documenti Amministrativi presso la Presidenza del Consiglio dei Ministri, laddove si prevede che il riconoscimento del diritto di accesso dei consiglieri di cui all'art. 43 TUEL «incontra il limite funzionale per cui tale strumento non dev'essere piegato a strategie ostruzionistiche o di paralisi dell'attività amministrativa, con istanze ripetute che, a causa del loro numero, possano tradursi in un aggravio se non nella paralisi del lavoro negli uffici ai quali sono rivolte».

7 Cfr. Cons. di Stato, sez. V, 2 gennaio 2019, n. 9 e TAR Emilia-Romagna, 20 gennaio 2020, n. 16.

8 Cfr. parere del 28 ottobre 2014 fornito dalla Commissione per l'Accesso ai Documenti Amministrativi presso la Presidenza del Consiglio dei Ministri.

accesso siano irragionevoli, sproporzionate e come tali se abbiano o meno aggravato gli uffici pregiudicandone la funzionalità[9]». Ed ancora, la *ratio* della norma determina conseguentemente l' impossibilità, per l' Amministrazione destinataria, di richiedere al consigliere l' adduzione di una prodromica specifica motivazione per l' accesso, considerato che essa appare «illegittima in quanto volta a costituire un ingiustificato limite all' accesso[10]».

Inoltre, per ciò che più qui interessa, si deve osservare come la risalente e consolidata giurisprudenza amministrativa di merito e di legittimità (*ante* Reg. (UE) 2016/679) si sia sempre espressa confermando come il diritto *ex* art. 43, c. 2, TUEL non incontri alcuna limitazione derivanti da esigenze di riservatezza o privacy dei terzi, in quanto il consigliere è vincolato all'osservanza del segreto[11]; secondo tale interpretazione giurisprudenziale, dunque, è proprio il richiamo al riserbo, operato dall'art. 43, c. 2, TUEL dove prevede che «essi sono tenuti al segreto nei casi specificamente determinati dalla legge» a ricondurre la fattispecie nell' alveo di applicazione della disciplina relativa alla riservatezza personale, evidenziandosi come tale diritto non operi come limite preventivo all' esercizio di accesso ma costituisca un interesse tutelato solamente a posteriori, a mezzo degli strumenti di salvaguardia già riconosciuti con altre specifiche norme dal nostro ordinamento.

L'interpretazione prevalente, prima della piena applicabilità nel nostro ordinamento del Reg. (UE) 2016/679 e della disciplina da esso conseguente in materia di protezione dei dati personali, era meramente incentrata sul concetto di privacy intesa come diritto alla riservatezza (il famoso "diritto ad essere lasciati soli") e faceva leva sull'assunto per cui «l'art. 43, comma 2, D.Lgs. 18 agosto 2000, n. 267, prevede infatti che i consiglieri comunali sono tenuti al segreto nel caso accedano ad atti che incidono sulla sfera giuridica e soggettiva di terzi[12]», essa risolvendosi così in un mero limite all' uso che il consigliere possa fare delle informazioni di cui è venuto a conoscenza, a seguito del positivo esperimento del diritto allo stesso riconosciuto.

Si anticipa in questa sede come, analizzato il diritto alla protezione dei dati personali e definito lo stesso come interesse costituzionalmente garantito, il richiamo al mero segreto non appare più una soluzione sufficiente tesa a garantire il rispetto di questo diritto dai tratti ben più ampi rispetto al diritto alla riservatezza personale, rendendosi necessarie le seguenti riflessioni.

---

9 *Ibid.*

10 *Ibid.* La Commissione specifica come «il consigliere comunale non deve motivare la propria richiesta di informazioni e documenti, perché, altrimenti, la P.A. si ergerebbe impropriamente ad arbitro delle forme di esercizio delle potestà pubblicistiche dell'organo deputato all'individuazione ed al perseguimento dei fini collettivi, con la conseguenza che gli uffici comunali non hanno il potere di sindacare il nesso intercorrente tra l'oggetto delle richieste di informazione e le modalità di esercizio della funzione esercitata dal consigliere comunale (in tal senso la Commissione si è già espressa, tra gli altri, con parere del 29 11 2011)».

11 Si vedano, sul punto Cons. Stato, sez. V 11 dicembre 2013, n. 5931, Cons. Stato, sez. V 17 settembre 2010, n. 6963 e Cons. Stato, sez. V 4 maggio 2004, n. 2716, nonché TAR Lazio, sez. I, n. 171/2013.

12 Cfr. Cons. Stato, sez. V 4 maggio 2004, n. 2716.

2.1. L'accesso ai sensi dell'art. 43, c. 2, TUEL come trattamento di dati personali

La domanda che necessita di trovare riscontro, oggi, concerne se e come il Reg. (UE) 2016/679 possa trovare corretta applicazione nella fattispecie di diritto di accesso sin qui descritta, e per rispondere si ritine necessario, in primo luogo, ridefinire i connotati del diritto di cui all'art. 43, c. 2, TUEL, analizzandolo sotto la lente di ingrandimento della definizione di trattamento di dati personali fornita dal legislatore europeo.
In particolare, l'art. 4 definisce il trattamento di dato personale come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come 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». Se si tiene presente che, non di rado, le informazioni e le notizie alle quali i consiglieri accedono possono contenere dati personali, riferiti dunque a persone fisiche secondo la definizione data anche qui dall'art. 4 Reg. (UE) 2016/679[13], attraverso la mera lettura della norma, appare chiaro come l'esercizio del diritto riconosciuto ai sensi dell'art. 43 TUEL determini sicuramente e nella maggior parte dei casi, il trattamento di dati personali appartenenti ai soggetti eventualmente coinvolti.
Più precisamente, laddove le notizie e le informazioni oggetto della richiesta di accesso contengano dati personali, l' espletamento del diritto con riscontro positivo da parte dell' Amministrazione richiesta individuerà un' operazione di comunicazione, contemplata specificamente nel nostro ordinamento all'interno dell'art. 2-*ter* d.lgs. 196/2003[14].
Ciò attrae inevitabilmente il diritto di cui all' art. 43, c. 2, TUEL nell'alveo applicativo della disciplina normativa di *data protection*, determinando la necessità, come già sopra anticipata, di superare e ampliare l'assunto che relega la riservatezza personale al mero dovere di segreto, al fine di applicare correttamente, anche a questo trattamento, tutti i principi che ispirano la tutela dei dati personali.

[13] Si veda, per la definizione di soggetto interessato e per la definizione di dato personale, l'art. 4, n. 1, Reg. (UE) 2016/679.

[14] Si veda, per la definizione di comunicazione l'art. 2-*ter* d.lgs. 196/2003, dove si prevede al c. 4 che «Si intende per: a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione».

3. Il ruolo del consigliere comunale (e provinciale) nell'organigramma *data protection*: il consigliere come autorizzato al trattamento dei dati

Al fine di meglio valutare la fattispecie, si ritiene inoltre necessario analizzare come possa configurarsi il ruolo del consigliere comunale nell'ambito dell'organigramma privacy di cui al combinato disposto degli artt. 4, 28 e 29 del Reg. (UE) 2016/679 nonché dall' art. 2-*quaterdecies* d.lgs. 196/2003.

In premessa, si ritiene opportuno definire, per brevi cenni, la titolarità del trattamento nell' Ente Pubblico ai sensi dell' art. 4, n. 7, Reg. (UE) 2016/679; in particolare, il titolare del trattamento si identifica come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali[15]». La lettura della norma consente di stabilire come, per l' Ente Pubblico, il titolare del trattamento debba essere individuato nell' autorità pubblica, e dunque nella persona giuridica in sé considerata[16]. Allo stesso modo si deve ricordare come, per le persone giuridiche – e dunque anche per gli Enti Pubblici[17] - il titolare del trattamento è individuato nell'Ente stesso, a prescindere dall'organo o dalle persone fisiche che ne esprimono la volontà: lo stesso Garante per la Protezione dei Dati Personali, con la circolare n. 291/S del 13 novembre 1997 doc. n. 39785, ha chiarito come «qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)» [18].

Effettuate tali prime deduzioni si intende escludere in prima battuta, in modo quasi del tutto automatico ed attraverso un'interpretazione puntuale dell'art. 28 Reg. (UE) 2016/679, che il consigliere possa definirsi quale responsabile del trattamento, posto che, nell'espletamento delle proprie funzioni, quale rappresentante degli organi di governo dell'Ente Pubblico Locale, come individuate dall'art. 36 e ss TUEL, tale soggetto non ricade nella definizione di cui all'art. 4, n. 8, Reg. (UE) 2016/679[19]. Il responsabile del trattamento, infatti, viene individuato dalla normativa europea come

---

15 Si veda su punto art. 4, n. 7, Reg. (UE) 2016/679.

16 Cfr. L. Cairo - G. Roberto, *commento all'art. 4 "Titolare del trattamento"* in *Leggi D'Italia* a sostegno della tesi appena richiamata.

17 Cfr. M. Di Pirro, *Compendio di Istituzioni di diritto privato (diritto civile)*, XXIII edizione, Napoli, Simone, 2019, 68. L'autore ci ricorda come l'Ente Pubblico è definito come persona giuridica pubblica, che persegue «interessi generali, propri dello Stato, e spesso godono di una posizione di supremazia nei confronti degli altri soggetti con cui vengono in rapporto (i c.d. enti pubblici)».

18 Si veda sul punto Autorità Garante per la protezione dei dati personali ("Garante Privacy"), in Circolare n. 291/S del 13 novembre 1997 recante direttive in materia di protezione dei dati personali. Rif. nota n. 14/97/MAN, doc. web. n. 39785.

19 La norma richiamata prevede infatti che il responsabile del trattamento sia definito come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

il soggetto, diverso ed estraneo rispetto al titolare del trattamento, chiamato a trattare dati per conto di quest'ultimo, secondo uno schema contrattuale che assume le forme del contratto di mandato ai sensi dell' art. 1703 c.c.: il consigliere deve considerarsi come parte dell' unitarietà della persona giuridica dell' Ente, e non dunque, come un soggetto esterno che agisca per conto dell' Amministrazione.
Come conseguenza diretta dell' affermata unitarietà della persona giuridica per l' Ente Pubblico Locale, si dovrà altrettanto escludere l' ipotesi che vede il consigliere comunale quale titolare autonomo del trattamento, ai sensi dell' art. 4 del Reg. (UE) 2016/679, determinando implicitamente l' individuazione dello stesso quale soggetto autorizzato al trattamento.
Il consigliere, dunque, sembra inserirsi nell'organigramma *data protection* quale soggetto autorizzato al trattamento dal titolare (il Comune o la Provincia), ai sensi del combinato disposto degli artt. 29[20] e 32[21] Reg. (UE) 2016/679 e 2–*quaterdecies,* c. 2, d.lgs. 196/2003[22], considerato che lo stesso opera sotto l' autorità diretta del titolare del trattamento.
Il ruolo dell'incaricato o autorizzato al trattamento sembrava, *prima facie*, scomparso e dalla normativa europea e dal Codice Privacy a seguito delle modifiche intervenute con il d.lgs. 101/2018 che hanno determinato l'abrogazione dell'art. 30 d.lgs. 196/2003[23], ma di fatto, il concetto di soggetto autorizzato al trattamento torna a più riprese anche all' interno del regolamento comunitario: basti ricordare che lo stesso art. 32 al c. 4 stabilisce che «Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri». Si può dunque affermare come sia stata eliminata la previsione normativa di una nomina obbligatoria ad autorizzato al trattamento, ma che tale "ruolo" rimanga ancora del tutto ben delineato sia nel Reg. (UE) 2016/679 che nel Codice Privacy come recentemente modificato[24]; di fatto, richiamato qui anche

[20] Si ricorda che l'art. 29 Reg. (UE) 2016/679 prevede infatti che «Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

[21] Il contenuto dell'art. 32 Reg. (UE) 2016/679 ci permette di rilevare come la definizione di un "organigramma *privacy*" si debba ricomprendere all'interno del comparto di misure organizzative di sicurezza che il titolare del trattamento è tenuto ad implementare.

[22] L'art. 2 – *quaterdecies* c. 2 d.lgs. 196/2003 stabilisce che «Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta».

[23] La norma in questione prevedeva che «Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima».

[24] Medesimi rilievi possono essere ricavati dalla lettura della Relazione illustrativa di accompagnamento al d.lgs. 101/2018, laddove, con riferimento all'art. 2-quaterdecies, si legge come «Tale disposizione permette di mantenere le funzioni e i compiti assegnati a figure interne all'organizzazione che, ai sensi del previgente codice in materia di protezione dei dati personali ma in contrasto con il regolamento, potevano essere definiti, a seconda dei casi, responsabili o incaricati».

il principio di *accountability*, si deve ritenere come il titolare, al fine anche di dimostrare correttamente il percorso di adeguamento alle disposizioni normative in materia di tutela dei dati personali, debba ben provvedere alla formalizzazione di una nomina scritta nei confronti dei soggetti autorizzati al trattamento – consiglieri comunali e provinciali compresi, anche con riferimento all'esercizio delle funzioni di cui all'art. 43, c. 2, TUEL - al fine di individuare le modalità corrette di trattamento del dato. Tale nomina scritta rappresenta, inoltre, una misura organizzativa atta ad istruire e formare in modo specifico i soggetti che provvedano, nell' ambito delle loro mansioni e delle loro funzioni, al trattamento di dati personali sotto l' autorità del titolare del trattamento. A ciò si deve aggiungere il provvedimento, tutt' ora richiamato dall' Autorità Amministrativa Indipendente, che con preciso riferimento alla Pubblica Amministrazione ha statuito come in assenza di una formale designazione come soggetto autorizzato al trattamento, i dipendenti delle pubbliche amministrazioni che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto alle amministrazioni stesse, con conseguenti rilevanti limiti per la comunicazione e l´utilizzazione dei dati e quindi per la liceità del trattamento. Tale designazione è, infatti, indispensabile, in quanto permette di considerare legittimo il flusso delle informazioni personali nell'ambito degli uffici e tra i dipendenti dell'amministrazione titolare del trattamento[25].

Tale principio, per l'estensione del ruolo di autorizzato al trattamento anche al consigliere comunale, dovrà appunto trovare applicazione anche nei confronti di tale soggetto: la nomina ad autorizzato al trattamento, in questo caso, avrà il fine di istruire correttamente il consigliere in merito al rispetto della normativa in materia di trattamento del dato personale, richiamandolo ai principi che ispirano la tutela dei dati personali in merito al trattamento di dati che venga compiuto nell'espletamento del *munus* di cui all' art. 43 TUEL, onde impartire indicazioni che siano tese ad evitare errori o trattamenti illegittimi delle informazioni. Il consigliere, così, dovrà essere destinatario delle stesse *policy* tese a disciplinare in modo organico tutti i processi che possono in qualche modo toccare la materia della tutela del dato personale e che vengono consegnate ai dipendenti dell'Ente: si pensi ad esempio, ai regolamenti che disciplinano l'uso della strumentazione informatica, o ancora, il codice di comportamento adottato dall'Amministrazione[26].

[25] Si veda a tal fine Garante Privacy, 23 maggio 2000, in Bollettino n. 13, pag. 21 [doc. web n.40229].

[26] Con specifico riferimento all'estensione del Codice di Comportamento della Pubblica Amministrazione ai consiglieri comunali, si vedano le Linee guida in materia di Codici di comportamento delle amministrazioni pubbliche ANAC, sottoposte a consultazione sino al 15.01.2020, che prevedono quanto segue: «Il d.P.R. 62/2013, all'art. 2, co. 3, stabilisce, infatti, che «le pubbliche amministrazioni estendono, per quanto compatibili, gli obblighi di condotta previsti dal presente codice a tutti i collaboratori o consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo, ai titolari di organi e di incarichi negli uffici di diretta collaborazione delle autorità politiche, nonché nei confronti dei collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione» […] "Con riferimento ai "titolari di organi", ad avviso dell'Autorità, il legislatore intende riferirsi ai titolari di organi di indirizzo amministrativo che non sono direttamente o indirettamente espressione di rappresentanza politica. Si tratta dei componenti degli organi, monocratici o collegiali, di enti pubblici, economici e non economici, anche nominati o designati da organi politici, che rivestono la carica pubblica al di fuori di ogni rapporto di lavoro. Considerato il rilevo di tali figure, potrebbe non essere opportuno escluderle da una qualunque forma di disciplina di doveri di comportamento con

Infine, preme in ogni caso ricordare come anche i consiglieri, come i dipendenti dell' Ente, sono sempre chiamati al rispetto della riservatezza degli interessati, come confermato anche a più riprese dal Garante per la Protezione dei Dati Personali, che ha rilevato come «i consiglieri comunali che abbiano avuto accesso ad atti dell' amministrazione comunale per ragioni connesse all' espletamento del loro mandato devono rispettare il diritto alla riservatezza degli interessati»[27].

3.1. Il consigliere come titolare del trattamento al momento della violazione privacy

Sempre sulla qualifica *data protection* dei consiglieri, è necessario compiere un' ulteriore riflessione con riferimento a cosa accada laddove tale soggetto violi la disciplina normativa in vigore. Seguendo le regole ordinarie di imputazione della responsabilità all'Ente per ciò che concerne gli illeciti compiuti dai suoi organi e dei suoi dipendenti, possiamo identificare nel consigliere autore di una violazione *data protection* un titolare autonomo del trattamento, con la conseguente applicazione della responsabilità (e dunque delle sanzioni) che si congiungono a tale figura, nel rispetto di quanto previsto dagli artt. 82 e ss Reg. (UE) 2016/679.
Si deve ricordare, infatti, come il rapporto organico, dal quale discende l'imputazione all' Ente Pubblico del fatto e delle sue conseguenze, opera solamente laddove il soggetto che agisce - sottoposto all' autorità dell' Amministrazione - lo fa nell'ambito circoscritto delle proprie funzioni e competenze; si assiste invece alla cesura del rapporto organico nel momento in cui il soggetto agisca perseguendo finalità sue proprie, in contrasto con i compiti istituzionali assegnati, a mezzo di una condotta che non si ispira certamente a principi costituzionali di liceità, di legalità e buon andamento della P.A. Questa attività non si imputa all'Ente, come allo stesso non si imputa la relativa responsabilità.
Estendendo analogicamente, infatti, i principi concernenti l'immedesimazione organica che discendono, per i dipendenti pubblici, dall'art. 28 Cost.[28], possiamo rilevare come l' attività del singolo amministratore, nell' esercizio dei compiti indicati all' art. 42 TUEL, possa essere imputata all' Ente solo laddove la stessa combaci con la volontà di quest' ultimo, rimanendo fermi i principi costituzionali che ispirano l' attività amministrativa: di conseguenza, la Pubblica Amministrazione può essere chiamata a rispondere degli eventuali danni arrecati a terzi solo qualora il proprio dipendente li abbia arrecati nell' esercizio di compiti istituzionali o di compiti legati da "occasionalità

conseguenti responsabilità. Per essi può essere adottata la soluzione di introdurre, nell'atto di incarico, clausole che estendono loro obblighi di condotta previsti dal codice nazionale con relative indicazioni in caso di violazioni. Resta ferma la possibilità che gli enti interessati per detti soggetti possono adottare codici etici dedicati».

[27] Cfr. A tal proposito Garante Privacy, in Relazione 2008 - 2 luglio 2009 Parte II - L'attività svolta dal Garante, p. 21 [doc. web n. 1637571].

[28] La norma prevede che «I funzionari e i dipendenti dello Stato e degli enti pubblici sono direttamente responsabili, secondo le leggi penali, civili e amministrative, degli atti compiuti in violazione di diritti. In tali casi la responsabilità civile si estende allo Stato e agli enti pubblici».

necessaria" con compiti di istituto[29].

Ne discende, dunque, che il consigliere che agisca in violazione dei principi racchiusi nel Reg. (UE) 2016/679, violando il diritto alla protezione dei dati personali dei soggetti eventualmente interessati dalle attività "ispettive", agirà quale titolare autonomo del trattamento; si assiste, qui, ad una sorta di estensione dei principi sanciti all' art. 28 dello stesso regolamento, laddove si prevede, con specifico riferimento al responsabile del trattamento, che «Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione».

La richiamata interpretazione è stata sostenuta dallo stesso Garante per la Protezione dei Dati Personali, che con l' ordinanza di ingiunzione del 4 aprile 2019 ha specificato come il consigliere comunale, che aveva ottenuto l' accesso ad alcuni documenti contenenti dati personali ai sensi dell' art. 43 TUEL, provvedendo poi a comunicarne il contenuto ad un soggetto terzo, dovesse qualificarsi «quale titolare del trattamento» ed allo stesso dovesse essere contestata «la violazione amministrativa prevista dall' art. 162, comma 2-bis, del Codice, che punisce la violazione delle disposizioni indicate nell' art. 167 e, in tal caso, la violazione dell' art. 19, comma 3, per aver effettuato un trattamento illecito di dati personali consistente, nello specifico, nella comunicazione di documentazione (D.I.A. n. 275/09 del 20 ottobre 2009) contenente dati personali del segnalante e acquisita in qualità di consigliere comunale, alla controparte giudiziale di tale segnalante in assenza dei presupposti normativi legittimanti»[30].

Il consigliere diviene dunque centro primario di imputazione della responsabilità nel momento in cui le informazioni ottenute a seguito dell' esercizio del proprio diritto di accesso siano utilizzate a mezzo di condotte che si distaccano dalle funzioni e dalle competenze riconosciute, con condotte che possano determinare la violazione del diritto alla riservatezza ed alla protezione dei dati personali eventualmente contenuti nei documenti e nelle informazioni ottenute da tale soggetto, con una tutela del dato personale che sembra operare, ancora una volta, a posteriori.

Sebbene l'individuazione del ruolo del consigliere nell'organigramma *data protection* sia di necessaria importanza per una disamina completa della fattispecie, si ritiene qui imprescindibile introdurre un tema di non secondaria importanza, relativo alla possibile applicazione dei principi che regolano la tutela dei dati personali all'atto dell'esercizio del diritto di accesso, in una prospettiva cautelativa *by design* e *by default*, come richiesto dall'art. 25 Reg. (UE) 2016/679, assodato che il diritto *ex* art. 43 TUEL si concretizza in un trattamento di dato personale.

[29] Cfr. A. M. Sandulli, *Manuale di diritto amministrativo*, Napoli, 1984, 1117, secondo il quale «non sono riferibili all'Amministrazione […] le azioni che non provengono da soggetti i quali possano essere considerati agenti di essa, […] gli atti personali degli agenti (lettere e negozi privati), […] gli atti viziati da incompetenza assoluta (straripamento di potere) e i comportamenti posti in essere volutamente (dolosamente) in violazione di norme proibitive (diversamente dall'opinione corrente nella dottrina francese, si ritiene che il fatto che costituisca reato doloso istituzionalmente non può essere ascritto all'Amministrazione)».

[30] A tal fine si veda Garante Privacy, ordinanza 4 aprile 2019, Registro dei provvedimenti n. 100 del 4 aprile 2019 [doc. web n. 9117119].

4. I profili di applicazione del Reg. (UE) 2016/679 all'esercizio dell'accesso ex art. 43, c. 2, TUEL

La ridefinizione del particolare diritto di accesso oggetto della presente trattazione come trattamento di dati personali introduce il tema della necessaria disamina relativa alle modalità di corretta applicazione delle norme e dei principi derivanti dal regolamento comunitario e dalla disciplina che da esso discende, in un' ottica volta non solo alla tutela (*ex post*) della riservatezza personale comunemente intesa, ma anche alla tutela *ex ante* dei dati personali riferiti allo stesso soggetto interessato.
Ciò implica un' inversione di prospettiva con riferimento alle valutazioni da compiersi nella fattispecie oggetto di analisi: il tema della protezione dei dati personali è ben più ampio rispetto a quello della riservatezza personale, tale per cui esso non può essere semplicemente escluso dall' equazione richiamando il consigliere al mero dovere di segreto imposto dall' art. 43, c. 2, TUEL. Il processo, concernente l' esercizio di tale specifico diritto di accesso, infatti, dovrà comprendere la compiuta attuazione di tutti i principi che il legislatore europeo prima, e quello nazionale poi, hanno individuato per provvedere alla necessaria tutela dei diritti personali coinvolti.
Si deve necessariamente ricordare in questa sede, infatti, come nella privacy si individui una famiglia di diritti inviolabili dell' uomo, che attengono a bisogni primari dell' essere umano; essa si è evoluta, a partire dal «diritto ad essere lasciati soli»[31] fondato ormai centotrent' anni fa, sino a poter essere definita come insieme di tutele a bisogni connaturati dell' essere umano, come complesso di tutele che vanno a proteggere lo stesso rispetto a delle infrazioni del sé nelle parti aggredibili da terzi. Ed è proprio a questa tutela prodromica e diffusa che tende il Reg. (UE) 2016/679, il quale guarda alla protezione delle persone fisiche attraverso la tutela dei loro dati personali, definendo la *data protection* come elemento integrante il diritto alla libera circolazione delle persone fisiche nell'UE.
La tutela dei dati personali pertanto deve essere considerata come elemento presupposto, strumentale alla tutela di altri diritti fondamentali ed inderogabili dell'essere umano, che deve trovare una necessaria costante applicazione, di talché tale tutela si estende, secondo quanto stabilito dalla normativa applicabile, a tutte le fattispecie che possono ricomprendere il trattamento di dati personali.
In particolare, l' identificazione di un' attività di trattamento di dati personali comporta la necessaria applicazione dei principi di cui al Reg. (UE) 2016/679, rientrando nell'ambito di applicazione materiale previsto dall'art. 2, par. 1, del regolamento stesso: ciò determina, come conseguenza diretta, una necessaria analisi concernente il corretto dispiegamento dei principi di cui agli artt. 5, 6, 24, 25 e 32 anche con riferimento all'esercizio del diritto di cui all'art. 43, c. 2, TUEL, individuando i soggetti attivi e le relative responsabilità connesse a tali adempimenti, e le modalità più coerenti per provvedere all' attuazione del generale obbligo di tutela dei dati personali.
Per ciò che concerne la fattispecie di trattamento oggetto della presente analisi, riprendendo quanto già espresso al paragrafo 3, dobbiamo necessariamente individuare

[31] S. D. Warren – L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 4-5, 15 December 1890, 193-220.

l'Amministrazione richiesta (o l'azienda o l'ente dipendente, a seconda del caso) come titolare del trattamento, soggetto che, all'atto della formazione del documento oggetto della richiesta del consigliere, individua finalità e mezzi del trattamento, e che di conseguenza è soggetto responsabile della corretta applicazione dei principi di *data protection*. Spetterà dunque all' Amministrazione adempiere agli obblighi derivanti dal Reg. (UE) 2016/679, anche all' atto della richiesta di accesso da parte del consigliere: e così dovrà essere garantito il rispetto dei principi di liceità, correttezza e trasparenza del trattamento, di limitazione delle finalità, di minimizzazione, esattezza, integrità e riservatezza dei dati, di limitazione della conservazione e del generale principio di *accountability* ai sensi dell'art. 5[32], nonché dei principi di *privacy by design* e *by default* ai sensi dell'art. 25[33], in aggiunta all'obbligo di individuare e porre in essere le misure tecniche ed organizzative adeguate a garantire la sicurezza del trattamento di cui all'art. 32 Reg. (UE) 2016/679[34].

[32] L'art. 5 Reg. (UE) 2016/679 prevede che «I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)».

[33] L'art. 25 Reg. (UE) 2016/679 prevede che «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo».

[34] L'art. 32 Reg. (UE) 2016/679 stabilisce che «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la

Ai fini di una compiuta analisi, si provvede nel prosieguo alla disamina di alcune casistiche specifiche, concernenti le richieste di consiglieri comunali di poter accedere, ai sensi dell'art. 43, c. 2, TUEL, al gestionale di protocollo informatico dell'Ente di appartenenza, nonché ad altre banche dati quali ad esempio il gestionale di contabilità, valutando le impostazioni giurisprudenziali che nel tempo si sono susseguite, al fine di evidenziare l' imprescindibile necessità di provvedere all' attuazione dei principi concernenti la tutela del dato personale anche in tale fattispecie.
L' analisi è volta ad indagare le ragioni che portano a definire la necessaria attuazione di una tutela *ex ante* rispetto all'uso eventuale che il consigliere intenda fare delle informazioni e dei dati personali eventualmente ottenuti, in comparazione rispetto al caso, successivamente valutato, dell'utilizzo illegittimo delle informazioni acquisite a seguito dell'esercizio del diritto di accesso.

5. Il caso concreto: la richiesta di accesso da remoto al protocollo informatico e ad altri gestionali comunali

La giurisprudenza amministrativa è stata recentemente chiamata ad interrogarsi sulla possibile estensione dell' alveo applicativo del diritto di cui all' art. 43, c. 2, TUEL, sino ad arrivare a ricomprendere anche il caso in cui il consigliere comunale richieda di poter accedere, da remoto, a mezzo della creazione di un collegamento VPN con creazione di *user* e *password*, ai sistemi gestionali dell' Ente, in particolar modo al protocollo informatico ed al gestionale di contabilità utilizzato dall' Amministrazione, al fine di valutare se tale diritto di accesso possa essere esercitato anche mediante l'utilizzo, da parte del consigliere, di tali strumenti.
Prima di analizzare compiutamente i passi che, timidamente, stanno permettendo un riavvicinamento alla materia della tutela dei dati personali, si ritiene opportuno procedere con una breve disamina concernente i precedenti giurisprudenziali che a più riprese si sono occupati della fattispecie in esame, utili per comprendere la portata del *vulnus* che si rischia di cagionare escludendo dal ragionamento tale diritto imprescindibile.

capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

5.1. Una breve disamina dei precedenti giurisprudenziali: la tutela dei dati personali come diritto "tradito"

Come sopra accennato, la giurisprudenza di merito e di legittimità in sede amministrativa è stata recentemente chiamata, a più riprese, a pronunciarsi sulla possibilità per il consigliere comunale, di avere accesso da remoto al gestionale di protocollo utilizzato dall' Ente, in applicazione dell' art. 43, c. 2, TUEL. Sul tema si è sviluppato sin da subito un orientamento prevalente, favorevole all' estensione dell' alveo applicativo del diritto di accesso in tal senso, al fine di permettere a tali soggetti qualificati l'espletamento di un accesso più efficace e meno dispendioso per gli uffici dell'Amministrazione.
Precisamente, prima il Consiglio di Stato con sentenza n. 3486/2018 e poi il TAR Salerno, con sentenza n. 545/2019, rilevavano come «ove il consigliere comunale fosse posto in condizione di individuare previamente gli atti il suo esame fosse utile all'esercizio delle sue prerogative, mediante la preventiva consultazione del protocollo informatico dell'Ente, tale modalità consentirebbe un accesso (ai singoli documenti) più efficace e meno dispendioso per l'ordinaria attività degli uffici; per converso, impedire o ostacolare il consigliere nell'individuazione di detti atti, ad esempio aggravando le modalità di consultazione delle fonti e di accesso alle stesse (protocollo dell'Ente), significherebbe impedire o frapporre ostacoli all'esercizio di un diritto»[35]. Sulla scorta di tale impostazione, il Giudice di prime cure, confermando l'orientamento già espresso dal Consiglio di Stato con sentenza appena sopra richiamata, evidenziava come dovesse essere riconosciuto al consigliere che lo richieda, un accesso in sola consultazione al protocollo informatico dell'Ente, con la consegna di credenziali (*username* e *password*) che permettano allo stesso un accesso (meramente valutativo e non esplorativo) anche da remoto.
Ancora, a conferma dell'orientamento appena esposto, si pronunciava il TAR Sardegna con sentenza n. 317/2019, evidenziando come l'accesso da remoto del consigliere comunale ai gestionali del Comune debba essere garantito in quanto strumento di valutazione preliminare, prodromico ad un più consapevole esercizio da parte di tale soggetto qualificato del diritto di accesso stesso, potendo in questo modo il consigliere selezionare in precedenza gli oggetti degli atti di cui chiedere l' esibizione[36].
Gli stessi rilievi venivano compiuti poi dal TAR Basilicata Potenza, che con sentenza n. 599/2019, pronunciandosi in merito ad una richiesta di accesso, da remoto, al pro-

[35] Si vedano sul punto le sentenze Cons. Stato, n. 3486/2018, TAR Campania Salerno, sez. II, 4 aprile 2019, n. 545.

[36] Cfr. sul punto, TAR Sardegna Cagliari, sez. I, 4 aprile 2019, n. 317. Precisamente, il Giudice di prime cure ha ritenuto che «In specie, la richiesta di accedere al protocollo informatico e ai programmi in uso presso il Comune, e quindi di avere il possesso delle chiavi di accesso telematico, rappresenta una condizione preliminare, ma nondimeno necessaria, per l'esercizio consapevole del diritto di accesso, in modo che questo si svolga non attraverso una apprensione generalizzata e indiscriminata degli atti dell'amministrazione comunale (che costituisce il timore manifestato anche in questa sede dal Comune intimato), ma mediante una selezione degli oggetti degli atti di cui si chiede l'esibizione. Peraltro, una delle modalità essenziali per poter operare in tal senso è rappresentata proprio dalla possibilità di accedere (non direttamente al contenuto della documentazione in arrivo o in uscita dall'amministrazione, ma) ai dati di sintesi ricavabili dalla consultazione telematica del protocollo (sia del protocollo generale dell'Ente, che dei registri di protocollo di settore, come quelli concernenti le determinazioni dei diversi responsabili dei servizi)».

tocollo informatico ed al gestionale informatico di contabilità dell' Ente convenuto, rilevava come si debba ritenere che il diritto di accesso dei consiglieri *ex* art. 43, c. 2, TUEL vada «oggi necessariamente correlato al progressivo e radicale processo di digitalizzazione dell'organizzazione e dell'attività amministrativa, risultante dal Codice dell'Amministrazione digitale»[37], con la conseguente applicazione di tale impianto normativo, che prevede per le Pubbliche Amministrazioni l' obbligo di garantire l' accessibilità e la fruibilità dei dati a mezzo delle tecnologie dell' informazione[38], concludendo come «l'Amministrazione comunale ha il dovere di dotarsi di una piattaforma integrata di gestione documentale, nell'ambito della quale è inserito anche il protocollo informatico. Corrispondentemente, il consigliere comunale ha il diritto di soddisfare le esigenze conoscitive connesse all'espletamento del suo mandato anche attraverso la modalità informatica, con accesso da remoto»[39].

Ne discende come gli orientamenti giurisprudenziali di merito e di legittimità analizzati siano concordi nel ritenere che il diritto di accesso dei consiglieri debba ritenersi esteso anche all'accesso al protocollo informatico ed agli altri gestionali informatici dell'Ente. La *ratio* del riconoscimento giurisprudenziale concernente le nuove modalità di esercizio del diritto di accesso, con l' assegnazione al soggetto richiedente di apposito *username* e *password* per utilizzare i gestionali informatici per le finalità specificate dall' art. 43, c. 2, TUEL, si individua dunque nella necessità di evitare un aggravio eccessivo per gli uffici comunali, che devono riscontrare alle richieste di accesso poste dai consiglieri comunali[40].

Gli stessi orientamenti affermano poi all' unisono come l' esercizio di tale specifica tipologia di accesso ai gestionali dell' Ente non possa essere però del tutto privo di limiti: in particolare, «al fine di evitare ogni accesso indiscriminato alla totalità dei documenti protocollati» i Giudici hanno ritenuto come «l'accesso da remoto vada consentito in relazione ai soli dati di sintesi ricavabili dalla consultazione telematica del protocollo, non potendo essere esteso al contenuto della documentazione, la cui acquisizione rimane

[37] Cfr. sul punto, TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599.

[38] Cfr. TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599, dove precisamente il giudice rilevava come «Deve ritenersi che il diritto di accesso dei consiglieri comunali *ex* art. 43 d.lgs. n. 267 del 2000 cit. del TUEL, cui è funzionalmente connessa la richiesta del ricorrente, va oggi necessariamente correlato al progressivo e radicale processo di digitalizzazione dell'organizzazione e dell'attività amministrativa, risultante dal Codice dell'Amministrazione digitale. Tale disciplina, per quanto di rilievo, impone allo Stato, alle regioni e alle autonomie locali di assicurare "la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale", "utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione" (cfr. art. 2, co. 1), precisando che "i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dei privati" (cfr. art. 50, co. 1)».

[39] Cfr. sul punto, TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599.

[40] Si veda sul punto TAR Campania Salerno sez. II, 4 aprile 2019, n. 545, che evidenzia come «ove il consigliere comunale fosse posto in condizione di individuare previamente gli atti il suo esame fosse utile all'esercizio delle sue prerogative, mediante la preventiva consultazione del protocollo informatico dell'Ente, tale modalità consentirebbe un accesso (ai singoli documenti) più efficace e meno dispendioso per l'ordinaria attività degli uffici; per converso, impedire o ostacolare il consigliere nell'individuazione di detti atti, ad esempio aggravando le modalità di consultazione delle fonti e di accesso alle stesse (protocollo dell'Ente), significherebbe impedire o frapporre ostacoli all'esercizio di un diritto».

soggetta alle ordinarie regole in materia di accesso (tra le quali la necessità di richiesta specifica)»[41].

Dunque, l'unica limitazione all'espletamento dell'accesso con riferimento ai gestionali dell'Ente, ed in particolare al protocollo informatico, concerne la sola possibilità di accesso in consultazione, al registro di protocollo.

Appare chiaro come il fattore relativo alla tutela dei dati personali eventualmente coinvolti da tali tipologie di accesso sia stato del tutto tralasciato dai Giudici che si sono pronunciati sul punto: le implicazioni *data protection* non sono in alcun modo state affrontate, non è stato valutato se l' accesso da remoto (nei vari casi di specie) possa dirsi o meno sicuro, non sono stati analizzati i principi di cui agli artt. 5, 24, 25 e 32 Reg. (UE) 2016/679, e di conseguenza non è stata in alcun modo considerata la necessità, per l' Amministrazione Comunale richiesta, di tutelare, anche nel momento dell' esercizio di tale diritto, i dati personali dei soggetti eventualmente coinvolti.

Ciò sebbene permanga il principio affermato dal Garante per la Protezione dei Dati Personali, alla cui stregua l' esistenza del segreto d' ufficio in capo al consigliere sulle informazioni conosciute attraverso l' esercizio delle prerogative di cui all' art. 43 TUEL non esime da responsabilità l' Ente che gli abbia comunicato i dati personali, fuori dei casi consentiti dalla legge (con le rilevanti sanzioni dell' art. 83, par. 5, Reg. (UE) 2016/679 e dell'art. 166, c. 2, d. lgs. 196/2003)[42].

Si ritiene che tale esclusione aprioristica non possa certo dipendere da ipotetici dubbi concernenti l'eventuale presenza, nei gestionali delle Amministrazioni, di dati personali definiti come da art. 4 Reg. (UE) 2016/679: tali strumenti contengono indiscutibilmente informazioni classificabili come dati personali, pertanto la miopia decisoria, che in questi frangenti non ha minimamente preso in considerazione il diritto imprescindibile alla tutela dei dati personali, dipende presumibilmente dall'interpretazione, sopra già discussa, del diritto alla privacy come mero diritto alla riservatezza personale, oggetto di una sola tutela a posteriori rispetto all'avvenuto accesso.

5.2. Valutazioni sui profili applicativi dei principi fondamentali del trattamento dei dati personali all'accesso *ex* art. 43 TUEL: artt. 5, 24, 25 e 32 del Reg. (UE) 2016/679

Ma se l'accesso *ex* art. 43, c. 2, TUEL comporta, di fatto, un' operazione di trattamento di dati personali, la quale si verifica a maggior ragione in presenza di un accesso ai gestionali informatici utilizzati dall' Amministrazione, ciò comporta come L'Ente richiesto non possa prescindere dall'applicazione corretta dei principi e delle tutele previste, anche nella fattispecie oggetto di esame.

In particolare, l' espletamento dell' accesso dovrà in ogni caso garantire il rispetto del principio di minimizzazione e di limitazione delle finalità del trattamento, individuato

[41] Cfr. sul punto, TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599.

[42] A tal fine si veda Garante Privacy, ord. 4 aprile 2019, Registro dei provvedimenti n. 100 del 4 aprile 2019 [doc. web n. 9117119].

dall' art. 5 Reg. (UE) 2016/679, che determina l' indispensabile limitazione dei dati trattati a quanto necessario per il raggiungimento delle finalità sottese al trattamento, imponendo di circoscrivere l'ambito delle operazioni ai soli dati personali appunto indispensabili per la realizzazione dello scopo perseguito, ricorrendo a dati anonimizzati o, se non sia possibile, quantomeno pseudonimizzati, al fine di ridurre il più possibile l'impatto del trattamento sulla sfera privata del singolo. L' affermazione è sicuramente forte, soprattutto se si pensa che il rispetto di un principio così delineato potrebbe di fatto inserire una sorta di obbligo di motivazione da addurre, da parte del consigliere, al momento della richiesta, ma la stessa si ritiene dovrà essere valutata al solo fine di tutelare correttamente le informazioni personali coinvolte, e non per l' eventuale disconoscimento del diritto di accesso. Tale canone è poi valorizzato con la previsione di principi quali la *privacy by design* e *by default* alle quali deve conformarsi il trattamento, per sua stessa configurazione.

La lettura integrale della fattispecie permette di ritenere che le opzioni di accesso del consigliere ai gestionali dell'Ente possano e debbano essere ben apprezzate anche per ciò che concerne i profili di sicurezza e tutela dei dati personali coinvolti nel trattamento, ai sensi degli artt. 5, par. 2, 24 e 32 Reg. (UE) 2016/679 e più in generale nel rispetto dell' intera normativa in materia di protezione dei dati personali, con la conseguenza che la scelta della modalità di accesso (da remoto, oppure a mezzo della previsione di una postazione specifica pressi gli uffici dell' Amministrazione) non possa essere rimessa alla semplice richiesta del consigliere.

Coerentemente rispetto ai principi *data protection*, infatti, sarà compito del titolare del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi del trattamento, individuare quali siano le modalità più corrette per l' espletamento di tale accesso, al fine di garantire la sicurezza delle informazioni personali coinvolte nel trattamento, prevedendo apposite misure di sicurezza tecniche ed organizzative, così come disposto dall' art. 32 del Reg. UE 2016/679.

In particolare, con riferimento all'accesso al sistema informatico dell'Ente, si deve rilevare quanto segue. Il trattamento di dati personali determina, sempre ed in modo intrinseco, un rischio congenito per i soggetti interessati da tale trattamento: laddove vi sia trattamento di dati personali, vi sarà sempre il rischio che questi possano essere violati ed il solo modo per mitigare del tutto tale rischio è quello di eliminare in modo completo i dati personali, e dunque interrompere il trattamento. Partendo da tale imprescindibile assunto, è innegabile che la possibilità di un accesso al sistema informatico dell' Ente, esercitato localmente o da remoto, così semplicemente inteso, senza alcun tipo di regolamentazione, e senza il necessario richiamo alla necessità, per l' Amministrazione, di dotarsi delle necessarie misure tecniche ed organizzative a tutela dei dati trattai, potrebbe essere foriero di rischi maggiori per gli stessi.

Resta ben inteso, quindi, che tale rischio dovrebbe essere correttamente valutato dal titolare del trattamento, il quale dovrebbe anche analizzare le possibili misure correttive da adottare al fine di ricondurre a sicurezza l'espletamento del diritto di accesso.

Dall'analisi appena compiuta risulta come sia necessaria una lettura del caso di specie orientata all'applicazione dei principi di *data protection*, elementi che non possono essere

tralasciati in quanto hanno ricadute innegabili sulle modalità corrette di esercizio del diritto di cui all' art. 43, c. 2, TUEL.

5.3. Il cambio di rotta nella giurisprudenza. La sentenza n. 253/2020 TAR Friuli-Venezia Giulia

Sebbene si debba ritenere che la richiesta di accesso agli atti, esercitata ai sensi dell'art. 43, c. 2, TUEL, possa estendersi sino alla possibilità, per il consigliere comunale, di accedere con proprie credenziali da remoto al registro di protocollo informatico dell' Ente, si deve evidenziare come a tale richiesta non corrisponda un diritto dello stesso consigliere di accesso da remoto: questa è, per l' appunto, una delle possibilità che possono essere previste per permettere il corretto espletamento del diritto soggettivo pubblico ivi in commento. Un primo input concernente la necessaria considerazione delle modalità specifiche di espressione di tale diritto lo ritroviamo nella Relazione della commissione per l' accesso ai documenti amministrativi sulla trasparenza dell' attività della pubblica amministrazione, per l' anno 2016, che, a sostegno della tesi poc' anzi esposta sottolineava come «non v'è d'altra parte dubbio che l'attività informativa debba essere ordinariamente svolta presso gli uffici dell'Amministrazione, come la norma stessa suggerisce, cosicché il consigliere non può vantare alcun "diritto" all'accesso al sistema informatico con connessione da remoto: né, secondo ragionevolezza il diritto del consigliere risulterebbe frustrato o compresso se esercitato in una postazione collocata presso gli uffici dell'Ente, il quale ha d'altra parte pieno titolo a garantire prioritariamente la sicurezza del sistema»[43]. Sono pertanto valutabili, dall'Ente, altre opzioni per permettere al consigliere comunale il corretto accesso al proprio sistema informatico: l'istanza di accesso da remoto del consigliere non determina, di contro, un immediato obbligo dell'Amministrazione ad adeguarsi a tale richiesta, ma si deve ritenere che, a seguito di specifica analisi del titolare del trattamento, il Comune possa prendere in considerazione altre possibilità, alternative a quella prospettata, che permettano, eventualmente, il corretto espletamento dell'accesso ai sensi dell'art. 43 TUEL senza determinare l'accesso da remoto al sistema informatico dell'Ente.

Tale rilievo è stato recentissimamente recepito anche a livello giurisprudenziale, con tre specifici interventi che hanno progressivamente dedotto come l' individuazione delle modalità di esercizio effettive di un tale diritto di accesso ad un gestionale dell' Ente non rientri nella disponibilità decisoria del consigliere stesso, quanto più dell' Amministrazione, unico soggetto titolato a compiere alcune valutazioni (anche riferite alla sicurezza dei dati e delle informazioni) che può stabilire come tale facoltà possa e debba essere esplicata.

La prima pronuncia, che ha evidenziato come la spinta verso la digitalizzazione dei servizi debba coinvolgere anche le modalità di esercizio del diritto di accesso di cui all' art. 43, c. 2, TUEL senza però che l' accesso ai gestionali informatici comporti «la elu-

[43] Cfr. sul punto, Relazione della commissione per l'accesso ai documenti amministrativi sulla trasparenza dell'attività della pubblica amministrazione – anno 2016, atti parlamentari, XVII legislatura, Doc. LXXVIII n. 5, p. 194.

sione dei principi di fondo che conformano l' esercizio del relativo diritto, nei termini stabiliti dagli artt. 22 e 24 della legge n. 241 del 1990[44]», è quella del TAR Molise, che con la sentenza n. 285/2019. Il Giudice amministrativo, pronunciandosi con riferimento ad una richiesta avente ad oggetto l'accesso da remoto con credenziali personali al programma di contabilità dell' Ente, affermava come «il rilascio delle credenziali di accesso all' area "Contabile e Patrimonio" del sistema Urbi Smart, nei termini richiesti dai ricorrenti, consentirebbe ai consiglieri regionali di accedere alla generalità indiscriminata dei documenti relativi alla contabilità dell' ente in mancanza di apposita istanza. Tale forma di accesso "diretto" si risolve in un monitoraggio assoluto e permanente sull' attività degli uffici, tale da violare la *ratio* dell'istituto, che, così declinato, eccede strutturalmente la sua funzione conoscitiva e di controllo in riferimento ad una determinata informazione e/o ad uno specifico atto dell' ente, siccome ritenuti strumentali al mandato politico, per appuntarsi, a monte, sull' esercizio della funzione propria dell' area "Contabile e Patrimonio" e sulla complessiva attività degli uffici, con finalità essenzialmente esplorative, che eccedono dal perimetro delle prerogative attribuite ai consiglieri regionali»[45].

Un primo passo verso la ridefinizione delle modalità effettive di esercizio di tale particolare diritto concerne la necessità di evitare un controllo esplorativo, posto in essere dal consigliere che acceda ai gestionali informatici dell' Ente.

Sulla scia di tale interpretazione, è stato lo stesso Consiglio di Stato, con sentenza n. 3345/2020, a compiere un ulteriore avanzamento nelle modalità di analisi della fattispecie, sottolineando, prima di tutto, come i giudizi aventi ad oggetto le richieste di accesso ai sistemi informatici dell' Amministrazione avanzate dai consiglieri concernono, solo in apparenza, giudizi «sull' accesso a atti o documenti», quanto piuttosto essi devono essere definiti come giudizi «sull' accessibilità indistinta al sistema informativo integrato, gestionale e direzionale, dell' amministrazione»[46].

Con un fondamentale distacco rispetto alla propria precedente interpretazione, già sopra richiamata, il Consiglio di Stato ha ben sottolineato come le richieste di accesso ai gestionali informatici degli Enti da parte dei consiglieri non possa tradursi automa-

[44] Cfr. sul punto, TAR Molise, sez. I, 3 settembre 2019, n. 285. Il Giudice di prime cure rilevava come «Vero è che l'accesso previsto dall'art. 43 del T.U.E.L. - pacificamente estensibile ai consiglieri regionali - deve essere letto ed applicato in conformità alla progressiva digitalizzazione che ha interessato negli ultimi anni l'attività degli uffici pubblici, ciò che rende sicuramente ammissibile l'accesso mediante l'utilizzo di sistemi informatici. È però parimenti vero che la concreta modalità dell'accesso con l'impiego di applicativi informatici non deve determinare la elusione dei principi di fondo che conformano l'esercizio del relativo diritto, nei termini stabiliti dagli artt. 22 e 24 della legge n. 241 del 1990».

[45] Cfr. sul punto, TAR Molise, sez. I, 3 settembre 2019, n. 285.

[46] Cfr. Cons. Stato, sez. V, 26 maggio 2020, n. 3345; nella sentenza è stato ben rilevato come «L'oggetto della contestazione in giudizio, infatti, è non un diniego all'accesso ad un singolo documento amministrativo (ovvero a più, determinati, provvedimenti amministrativi), come è nelle controversie in siffatta materia (art. 116 Cod. proc. amm.); ma è, in termini sostanziali, il diniego di un'innovazione organizzativa radicale, che prescinde da singoli atti o documenti, e che consiste nella disponibilità da parte del consigliere regionale delle credenziali di accesso alla documentazione digitale o digitalizzata di tutta l'attività amministrativa regionale: tale da metterlo in condizione di avere immediato ingresso, a discrezione e senza una ragione particolare, a qualsivoglia – anche se allo stato indeterminato e indeterminabile - passato, presente o futuro atto o documento amministrativo contemplato dal sistema in discorso».

ticamente nel riconoscimento di tale modalità di accesso, in quanto la stessa è tale da determinare, per tali soggetti qualificati, la possibilità di acquisire «un patrimonio conoscitivo che potenzialmente è pari alla latitudine dell' intera amministrazione regionale», anche per finalità meramente esplorative, eccedenti rispetto ai confini imposti dalla *ratio* della norma a tale particolare diritto[47]. Le ragioni di tale evoluzione interpretativa vanno individuate nel passaggio successivo della sentenza, che rappresenta, per l' organo giudicante, una prima presa di coscienza avente a riguardo la necessità di provvedere, all' atto dell' esercizio del diritto di accesso dei consiglieri, ad un equo bilanciamento con tutti gli opposti e meritevoli interessi eventualmente coinvolti da tale operazione, con richiamo espresso al «rispetto della vita privata», previo il riconoscimento dell' impossibilità di presumere sempre e comunque che tali esigenze di bilanciamento siano compatibili con «l' indiscriminata accessibilità qui in questione»[48].

E così, il Giudice definiva «ragionevole, adeguato e corrispondente al generale principio di proporzionalità che per ciascuna delle varie tipologie di accesso previste dall' ordinamento [..] siano stabiliti presupposti e modalità specifiche, poiché diversi sono gli interessi di volta in volta in contrapposizione e diversa è la ragione dell' accesso», rilevando come per il diritto *sui generis* in esame «non concretizza una prerogativa personale ma uno strumento per l' esercizio delle funzioni consiliari, di sindacato politico o legislative» individuando dunque il limite intrinseco al diritto di accesso del consigliere proprio nella menzionata utilità di tale strumento.

Sulla scorta di tali orientamenti, un ulteriore fondamentale passo volto al riconoscimento della necessità di ricomprendere, nell' esercizio del diritto *ex* art. 43, c. 2, TUEL, le tutele richieste dalla normativa in materia di protezione del dato personale, è stato compiuto dal TAR Friuli-Venezia Giulia, che con sentenza n. 253/2020, ha ricondotto la fattispecie ad una lettura integrale, orientata anche alla protezione delle informazioni che possono potenzialmente essere acquisite dal consigliere.

La questione sottoposta all'attenzione del Giudice di prime cure concerneva la richiesta, avanzata da un consigliere comunale alla propria Amministrazione, di poter accedere da remoto, con creazione di *username* e *password*, al protocollo informatico ed al programma di contabilità: la richiesta era stata declinata dall' Ente, il cui sistema informatico è gestito dalla Regione, sulla base dell' assenza di disponibilità economica per poter provvedere all' apertura di una VPN specifica per il richiedente, al quale era

[47] Cfr. Cons. Stato, sez. V, 26 maggio 2020, n. 3345, dove il Giudice rileva come «qui non è in contesa la facoltà di accesso del consigliere regionale ad atti dell'amministrazione regionale – facoltà ampiamente evidenziata dalla giurisprudenza amministrativa (sin da Cons. Stato, V, 17 settembre 2010, n. 6963; V, 5 settembre 2014, n. 4525) – ma l'ingresso senza più forma, riscontro e vaglio in una strumentazione digitale che continuativamente permetta l'accesso a tutti – nei sensi detti - gli atti dell'amministrazione regionale».

[48] Cfr. Cons. Stato, sez. V, 26 maggio 2020, n. 3345; nella sentenza si legge che «[…] va comunque ricordato che le regole legali dell'accesso espressamente o implicitamente commisurano una ragionevole proporzione e un equilibrio tra gli opposti e meritevoli interessi coinvolti dall'accesso a documenti amministrativi. La definizione di tali regole corrisponde alla natura fondamentale di interessi che possono esservi antagonisti, come quello al rispetto della vita privata (cfr. Corte cost., 21 febbraio 2019, n. 20) […] o comunque al rispetto dell'immanente principio di buon andamento della pubblica amministrazione (art. 97 Cost.) che eleva a principio costituzionale la congruenza, l'adeguatezza e l'efficacia dell'azione amministrativa: ciò che, per la realtà delle cose, non è dato presumere sempre e comunque compatibile con l'indiscriminata accessibilità qui in questione».

stato però proposto di provvedere all' accesso ai gestionali indicati a mezzo di una postazione a ciò specificamente adibita presso la sede dell' Amministrazione. Il ricorso presentato dal consigliere è stato respinto in quanto privo di pregio, laddove il Giudice ha dichiarato come «nella fattispecie in esame non viene assolutamente in rilievo il diritto del ricorrente medesimo di ottenere dagli Uffici del Comune, quale consigliere comunale, "tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato" ai sensi dell'art. 43, c. 2, del d.lgs. n. 267 del 2000 […], ma unicamente la pretesa dell'interessato, non assistita da alcun corrispondente obbligo di legge gravante sull'ente civico, di esercitare il diritto in questione nella modalità a lui più gradita e della cui effettiva e stretta funzionalità alle esigenze proprie di mandato il Collegio dubita fortemente, dato che, come si avrà modo di evidenziare in seguito viene in rilievo l' indistinta accessibilità all' intero sistema informatico dell'Amministrazione comunale, che nulla ha a che vedere con l'obbligo di cui all'art. 2, comma 1, del d.lgs. 7 marzo 2005, n. 82, gravante sulle PP.AA., di assicurare "la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale"»[49].

L'organo giudicante ha rilevato chiaramente come alla richiesta di accesso da remoto al sistema informatico dell'Ente non consegua alcun obbligo *ex lege* gravante in tal senso sullo stesso, considerato che le valutazioni concernenti le modalità più corrette al fine di permettere l'esplicazione del diritto di cui all'art. 43, c. 2, TUEL sono, in questo caso, rimesse al solo Comune, che, «a prioritaria tutela del pubblico interesse cui devono essere preordinati tutti gli atti e le iniziative assunte» non può in alcun modo prescindere dall' analisi della «fattibilità pratica dell' attivazione della postazione di accesso da remoto» e della sussistenza di eventuali non trascurabili «problematiche di carattere economico tecnico, di tutela della sicurezza del sistema informatico in uso e di trattamento dei dati personali contenuti e/o comunque veicolati dal sistema stesso»[50].

Così il Giudice di merito sottolineava come le modalità di corretto esercizio del diritto di accesso da parte del consigliere comunale possano essere individuate dalla sola Amministrazione richiesta, rilevato inoltre che «questo giudice non può in alcun modo invadere spazi intangibili di discrezionalità, né, tanto meno, sostituirsi all'Amministrazione in valutazioni di carattere organizzativo/funzionale che solo ad essa competono e che – si ribadisce – fuoriescono dal perimetro proprio della speciale forma di accesso spettante ai consiglieri comunali *ex* art. 43 d.lgs. 267/2000»[51]. Il TAR Friuli-Venezia Giulia, infine, rilevava, con specifico riferimento alla tutela dei dati personali che possono ben essere contenuti all'interno della documentazione che quotidianamente transita attraverso il programma di protocollo informatico, come «molti atti che vengono "veicolati" attraverso il protocollo comunale, anche se resi disponibili in forma di mera sintesi, possono rendere immediatamente consultabili "dati", anche personalissimi, che non possono considerarsi in alcun modo attratti nella sfera di necessaria conoscenza e/o conoscibilità che deve essere assicurata ai consiglieri comunali, sì da rendere, conseguentemente, ingiustificato il "trattamento" che in tal modo verrebbe effettuato [ ]

[49] Cfr. Sul punto, TAR Friuli-Venezia Giulia, sez. I, 9 luglio 2020, n. 253.

[50] *Ibid.*

[51] *Ibid.*

peraltro in assenza delle necessarie garanzie, essendo palese che il "segreto" cui sono tenuti i consiglieri comunali ai sensi dell' art. 43, comma 2, ult. periodo, d.lgs. cit. nulla ha a che vedere con le garanzie che devono, per l' appunto, presidiare il trattamento dei dati personali»; ne consegue come non si possa ritenere che la conoscenza di tali informazioni ricada nelle esigenze di mandato che rappresentano, come già detto, il limite intrinseco all' esercizio del diritto di accesso in commento[52].

L'organo giudicante ha evidenziato chiaramente come nell' identificazione delle modalità per rendere effettivo l' accesso, spetti al solo Comune compiere alcune prodromiche valutazioni, che dovranno comprendere inevitabilmente anche l' individuazione delle misure tecniche ed organizzative volte alla tutela dei dati personali coinvolti, stante l' impossibilità di ricondurre le garanzie richieste dal Reg. (UE) 2016/679 al semplice dovere di segreto.

Con ciò, vengono confermati i ruoli *data protection* come descritti nel paragrafo 3, tale per cui il Comune, in qualità di titolare del trattamento e dunque soggetto chiamato al rispetto del principio di *accountability*, alla richiesta del consigliere che voglia accedere, ai sensi dell'art. 43, c. 2, TUEL ai sistemi informatici dell' Ente, avrà il compito di mettere in atto misure tecniche e organizzative adeguate, per «garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento»[53] ciò sempre «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche»[54].

Il consigliere comunale, autorizzato al trattamento, dovrà dunque attenersi alle indicazioni fornite dall' Ente per l' esercizio del proprio diritto sui generis, rilevata la necessità per tale soggetto, seppur qualificato, di attenersi alle istruzioni ricevute dal titolare del trattamento ai sensi del combinato disposto degli artt. 29 e 32 Reg. (UE) 2016/679 e dell'art. 2-*quaterdecies* d.lgs. 196/2003[55].

---

[52] *Ibid.* Di particolare interesse è poi il decalogo effettuato dal Giudice di prime cure, con riferimento alla tipologia di atti, e dunque di dati personali, che possono quotidianamente transitare all'interno del protocollo informatico dell'Ente, che si riporta qui di seguito: «Ritenuto, invero, in via meramente esemplificativa e non esaustiva, di richiamare l'attenzione su tutti gli atti riferibili ai compiti svolti dal Comune per servizi di competenza statale (si pensi ad es. alle comunicazioni riguardanti annotazioni sugli atti di anagrafe), sulle richieste e/o comunicazioni riguardanti la cessione del quinto dello stipendio, sugli atti provenienti da altre PP.AA. relativi a indagini in corso, sulle istanze e/o gli atti relativi alla fruizione degli istituti previsti e disciplinati dalla legge 5 febbraio 1992, n. 104 (Legge quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate) e/o dal decreto legislativo 26 marzo 2001, n. 151 (Testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità, a norma dell'articolo 15 della legge 8 marzo 2000, n. 53), sugli atti relativi ai TSO, sugli interventi assistenziali su disposizione del Tribunale per i minorenni, etc. etc.); Ritenuto *ictu oculi* evidente che trattasi di atti, come potrebbero esserlo, ad esempio, anche quelli afferenti a procedure di gara in corso dei quali è preclusa la diffusione allo scopo di evitare fenomeni distorsivi della concorrenza [n.d.r. il riferimento è all'art. 53, comma 2, lett. a) e b), e comma 3, del d.lgs. n. 50/2016], che non sono nemmeno latamente riconducibili alle esigenze di mandato, le quali trovano la propria ragione d'essere e, al contempo, il proprio limite nelle attribuzioni (tassative) del Consiglio comunale (cfr. art. 42 d.lgs. n. 267/2000) e nel correlato e complementare diritto d'iniziativa e/o di presentare interrogazioni o mozioni che la legge riconosce ad ogni consigliere comunale (cfr. art. 43, comma 1)».

[53] *Ex* art. 5, par. 2, Reg. (UE) 2016/679.

[54] *Ex* art. 32 Reg. (UE) 2016/679.

[55] Ad integrazione di quanto evidenziato, si ricordi anche che nella sentenza TAR Friuli-Venezia

5.4. Il caso specifico: l'utilizzo illegittimo delle informazioni acquisite a seguito dell'esercizio del diritto di accesso

Prima di procedere con le valutazioni conclusive, è sembrato opportuno concentrare la nostra attenzione anche alla seconda fattispecie eventuale, ovverosia quella concernente l' eventuale utilizzo illegittimo che il consigliere possa fare delle informazioni ricevute a seguito dell'esercizio del diritto di cui all'art. 43, c. 2, TUEL.
In merito, come già ampiamente dedotto, gli orientamenti del Garante per la Protezione dei Dati Personali sono stati uniformi nell' affermare come «il trattamento dei dati contenuti negli atti dell´amministrazione comunale, connesso all´espletamento del loro mandato, può essere effettuato dai consiglieri comunali che abbiano esercitato il diritto di accesso a tali atti, nel rispetto del diritto alla riservatezza degli interessati»[56], individuando con ciò la tutela a posteriori riconosciuta alla sfera personale dei soggetti interessati, connessa al richiamo al segreto effettuato dallo stesso art. 43, c. 2, TUEL.
E così, partendo da un principio ormai cogente nel nostro ordinamento, tale per cui «la comunicazione e la diffusione dei dati personali da parte di privati e di enti pubblici economici può prescindere dal preventivo consenso dell' interessato nel caso in cui il trattamento sia effettuato in adempimento di un obbligo previsto dalla legge, da un regolamento o da una norma comunitaria»[57], il consigliere non potrà utilizzare i dati entrati in suo possesso per finalità estranee all' effettivo esercizio delle funzioni consiliari individuate all' art. 42 TUEL, tali da ledere la riservatezza degli interessati coinvolti[58].
Tale è stato appunto l' orientamento interpretativo prevalente, che ha essenzialmente

Giulia, sez. I, 9 luglio 2020, n. 253 il Giudice ha rilevato come «è pacifico e innegabile che l'esercizio del diritto in questione non risulta, allo stato, in alcun modo compromesso o limitato, dato che il Comune ha, comunque, assicurato all'odierno ricorrente che "ove richiesto, potrà essere messa a Sua disposizione presso gli uffici dell'Ente una postazione pc alla quale potrà accedere tramite utilizzo di apposite credenziali per la consultazione telematica delle notizie necessarie in ragione dell'esercizio delle sue funzioni" (così l'atto impugnato - all. 2 fascicolo ricorrente), al punto da appalesare finanche l'inammissibilità per carenza di interesse della richiesta qui dal medesimo avanzata».

[56] Cfr. Garante Privacy, Registro dei provvedimenti del 28 febbraio 2008 [doc. web n. 1501081].

[57] Cfr. Garante Privacy, 29 maggio 1998, in *Bollettino* n. 4, pag. 9 [doc. web n. 42144].

[58] Cfr. Garante Privacy, Registro dei provvedimenti del 28 febbraio 2008 [doc. web n. 1501081]. Sul punto «Una segnalazione inviata da un Comune lamentava l'avvenuta pubblicazione, su sito web non direttamente riconducibile al comune medesimo, di dati personali concernenti contributi erogati dall'Amministrazione per l'acquisto di libri di testo per l'anno scolastico 2005/2006, e, in particolare, l'ammontare del contributo nonché, in taluni casi, le coordinate del relativo conto corrente bancario. Le risultanze istruttorie hanno evidenziato che la lista dei destinatari dei contributi era stata divulgata via Internet dal capogruppo consiliare di minoranza (cui una copia era stata precedentemente consegnata in ragione di asserite motivazioni concernenti l'esercizio del proprio mandato politico) e che tale divulgazione consentiva l'immediata accessibilità a chiunque alle citate informazioni tramite mera ricerca nominativa dei beneficiari, anche con l'ausilio di eventuali motori di ricerca. In proposito, si è rilevato che i consiglieri comunali che abbiano avuto accesso ad atti dell'amministrazione comunale per ragioni connesse all'espletamento del loro mandato devono rispettare il diritto alla riservatezza degli interessati. Poiché il trattamento dei menzionati dati è risultato, allo stato degli atti, in violazione dei princìpi di liceità, finalità e pertinenza e non eccedenza (art. 11, comma 1, lett. a), b) e d), del Codice), è stato disposto il blocco del relativo trattamento nelle more della definizione di ulteriori accertamenti da parte dell'Autorità» come dedotto dalla stessa Autorità Garante nella Relazione 2008 - 2 luglio 2009 Parte II - L'attività svolta dal Garante, 3. Il Garante e le pubbliche amministrazioni, [doc. web n. 1637571].

rilevato come il diritto di accesso del consigliere non incontri il limite della riservatezza, la quale opera indistintamente da tale diritto *sui generis*, a posteriori, con riferimento alle azioni eventualmente compiute dal soggetto qualificato[59].
Laddove le informazioni acquisite vengano utilizzate in violazione di tale diritto, il consigliere ne risponderà in qualità di titolare del trattamento, stante quanto già esplicitato al paragrafo 3.1., ricadendo sullo stesso tutte le responsabilità derivanti da tale qualificazione soggettiva e dalla relativa violazione.
Ne discende la definizione di una responsabilità che non tiene conto dell' atto di accesso, ma solamente delle condotte ad esso successive, con la configurazione di una tutela a metà, privata della corretta applicazione dei principi posti a fondamento della tutela del dato personale: è qui necessario provvedere ad una ricostruzione del sistema di tutele, al fine di procedere al menzionato bilanciamento tra i due interessi costituzionalmente garantiti, affinché la protezione dei dati personali cominci ad operare all' atto del primo trattamento, rappresentato appunto dall' accesso.

6. Riflessioni conclusive: sulla necessità di un bilanciamento tra i due interessi costituzionalmente garantiti, anche alla luce dell' art. 86 Reg. (UE) 2016/679

Una preliminare riflessione conclusiva, avente ad oggetto la necessità di introdurre il concetto di bilanciamento tra interessi costituzionalmente garantiti anche nella fattispecie oggetto della presente trattazione, discende come conseguenza diretta dall'analisi del diritto di accesso *ex* art. 43, c. 2, TUEL da un lato e del diritto alla tutela dei dati personali dall'altro, i quali si qualificano entrambi, senza ombra di dubbio, come diritti di rango costituzionale.
In particolare, già al paragrafo 2 del presente lavoro si è avuto modo di evidenziare come il diritto di accesso riconosciuto dal nostro ordinamento ai consiglieri comunali e provinciali affondi le sue radici negli artt. 3 e 97 Cost. come espressione del principio democratico di autonomia locale e della rappresentanza esponenziale, qualificando dunque lo stesso quale interesse costituzionalmente garantito.
La stessa tutela di rango costituzionale viene riconosciuta anche al diritto alla riservatezza personale, oggi meglio e più ampiamente declinato, anche a seguito dell' entrata in vigore del Reg. (UE) 2016/679, nel diritto alla tutela del trattamento dei dati personali. Tale diritto è stato storicamente inteso e definito come un diritto fondamentale, un diritto della personalità, che non trova un riconoscimento esplicito nel sistema normativo ma che può essere ricavato per via interpretativa dal combinato disposto degli articoli 2, 13, 15 e 21 della Costituzione[60].

[59] Si veda, ad integrazione delle sentenze già ivi richiamate, anche Cons. Stato, sez. V, 2 marzo 2018 n. 1298.

[60] L'art. 2 e l'art. 13 Cost. nello specifico, laddove il primo rappresenta il riconoscimento di tutti i diritti inviolabili dell'uomo e il secondo è madre di tutte le libertà riconosciute dal nostro ordinamento, costituiscono l'alveo all'interno del quale la Corte Costituzionale, sin dal 1973, ha visto svilupparsi e crescere il seme della tutela della riservatezza personale, sino al riconoscimento definitivo ottenuto a mezzo della formulazione dell'art. 117 Cost. Si ricordi sul punto quanto affermato nella celebre sentenza

Come già ampiamente definito al paragrafo 4 del presente lavoro, la privacy oggi individua una famiglia di diritti inviolabili dell'uomo, che attengono a bisogni primari dell' essere umano, evolutasi a partire dal «diritto ad essere lasciati soli», per arrivare a definire un insieme di tutele integrato a bisogni connaturati dell' essere umano, costituzionalmente garantiti.

I connotati di rilievo costituzionale riconosciuti ad ambedue gli interessi impongono la necessità, laddove questi entrino in conflitto, di provvedere ad un loro bilanciamento, a mezzo di un confronto continuo tra gli stessi, volto a determinare un punto di equilibrio nella fattispecie concreta, realizzando il minor sacrificio possibile del diritto pregiudicato.

A differenza però di tutte le altre casistiche nelle quali si può produrre un conflitto tra tutela del dato personale e tutela di un altro interesse costituzionale[61], la fattispecie concernente il diritto di accesso ex art. 43, c. 2, TUEL non ha trovato, sino ad oggi, nel nostro ordinamento, alcun richiamo specifico alla necessità di provvedere a tale bilanciamento; nessuna menzione al bilanciamento è fatta dal TUEL, e così nessuna menzione viene compiuta dallo stesso d.lgs. 196/2003 a seguito della sua riformulazione del 2018.

La fattispecie, dunque, sembra in un qualche modo essere stata dimenticata, come suggerito anche nei precedenti paragrafi, a causa della confusione dei confini tra tutela del dato personale e riservatezza personale, ma la stessa merita qui di essere analizzata in tal senso.

In particolare, si richiama in questa sede l' art. 86 Reg. (UE) 2016/679, che recita «I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l' autorità pubblica o l' organismo pubblico sono soggetti, al fine di conciliare l' accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento»[62]. Il richiamato

Corte Cost., 5 aprile 1973, n. 38, ove la Consulta ha avuto modo di evidenziare come «Non contrastano con le norme costituzionali ed anzi mirano a tutelare e a realizzare i fini dell'art. 2 affermati anche negli artt. 3, secondo comma, e 13, primo comma, che riconoscono e garantiscono i diritti inviolabili dell'uomo, fra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza**,** intimità e reputazione, sanciti espressamente negli artt. 8 e 10 della Convenzione europea sui diritti dell'uomo, gli artt. 10 del codice civile».

[61] Si pensi semplicemente al conflitto tra tutela del dato personale e trasparenza amministrativa.

[62] La norma è espressione dei principi definiti dal considerando (154) che prevede come «Il presente regolamento ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali. L'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali e possono quindi prevedere la necessaria conciliazione con il diritto alla protezione dei dati personali, in conformità del presente regolamento. Il riferimento alle autorità pubbliche e agli organismi pubblici dovrebbe comprendere, in tale contesto, tutte le autorità o altri organismi cui si applica il diritto degli Stati membri sull'accesso del pubblico ai documenti. La direttiva 2003/98/CE del Parlamento europeo e del Consiglio (14) non pregiudica in alcun modo il livello di tutela delle persone

concetto di bilanciamento, dunque, permea il Reg. (UE) 2016/679, in quanto fonte sovraordinata per i principi di diritto comunitario, determina una necessaria interazione del contemperamento in tutte le ipotesi di accesso ai documenti ufficiali in possesso dell' autorità pubblica, e così anche al caso *sui generis* previsto dall'art. 43, c. 2, TUEL.
Risulta allo stesso modo incompleta la disciplina delineata dal legislatore nazionale nella nuova formulazione dell'art. 59 d.lgs. 196/2003, rubricato "Accesso a documenti amministrativi e accesso civico", che dimentica di tenere in debito conto le ulteriori ipotesi speciali di accesso ai documenti amministrativi quale quello in commento, occupandosi solamente dell' accesso documentale, civico e civico generalizzato; nonostante ciò, rilevata la forza normativamente riconosciuta al regolamento comunitario quale fonte normativa sovraordinata, non possiamo che concludere come il diritto *ex* art. 43, c. 2, TUEL dovrà sempre trovare un corretto bilanciamento con gli altri interessi costituzionali in gioco, primo tra tutti il diritto alla protezione dei dati personali, anche in assenza di una specifica disposizione normativa che indichi tale necessità di contemperamento.
L'applicazione trasversale della normativa transnazionale in materia di *data protection* erode così la forza sinora incontrastata del diritto di accesso dei consiglieri, richiamando gli operatori e gli interpreti al necessario contemperamento continuo tra interessi, e tratteggiando così alcuni innegabili limiti per l' esercizio di tale facoltà.
Come si avrà modo di meglio evidenziare qui di seguito, gli strumenti di tale fondamentale bilanciamento dovranno essere rilevati nei principi fondamentali di cui agli artt. 5, 24, 25 e 32 Reg. (UE) 2016/679: in particolare, l'attitudine al bilanciamento che caratterizza il diritto alla tutela dei dati personali deriva, come conseguenza diretta, dall' applicazione dei principi di necessità e proporzionalità[63], nonché dei principi cardine, regolatori della materia.

fisiche con riguardo al trattamento dei dati personali ai sensi delle disposizioni di diritto dell'Unione e degli Stati membri e non modifica, in particolare, gli obblighi e i diritti previsti dal presente regolamento. Nello specifico, tale direttiva non dovrebbe applicarsi ai documenti il cui accesso è escluso o limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali, e a parti di documenti accessibili in virtù di tali regimi che contengono dati personali il cui riutilizzo è stato previsto per legge come incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali».

[63] Si deve ricordare in tale sede il richiamo effettuato dal considerando 4 del Reg. (UE) 2016/679, che prevede come «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità». La Corte Costituzionale, inoltre, con la sentenza 21 febbraio 2020, n. 20, ricorda come «la Corte di giustizia dell'Unione europea ha ripetutamente affermato 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 (sentenze 20 maggio 2003, nelle cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk e altri, e 9 novembre 2010, nelle cause riunite C-92/09 e 93/09, Volker und Markus Schecke e Eifert)».

6.1. Conclusioni. Gli strumenti del bilanciamento: l'applicazione dei principi di *data protection* al diritto di accesso *ex* art. 43, c. 2, TUEL

L'attrazione del diritto di accesso dei consiglieri all'interno dell'orbita del Reg. (UE) 2016/679 comporta la necessaria applicazione di tutti i principi fondamentali, posti alla base delle tutele riconosciute ai dati personali, sin dal primo momento di attuazione di tale trattamento.

In tal senso l'applicazione concreta dei principi di *data protection* anche alla fattispecie qui analizzata si configura come *conditio sine qua non* per la realizzazione dell'equilibrio tra i due interessi.

E così, l' Ente destinatario delle richieste, titolare del trattamento, dovrà assicurare anche all' atto dell' esercizio del diritto di accesso del consigliere che i fondamentali principi di cui all' art. 5 Reg. (UE) 2016/679 siano rispettati. In particolare, l' Amministrazione dovrà compiere alcune valutazioni preliminari al riconoscimento del diritto di accesso, volte ad indagare la corrispondenza tra i dati richiesti e le finalità di esercizio di tale facoltà da parte del consigliere: di conseguenza, un primo limite intrinseco all' esercizio di tale diritto *sui generis* si ricava dall'applicazione necessaria dei principi di minimizzazione e limitazione delle finalità, primi strumenti di bilanciamento che ci ricordano come i dati personali debbano essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati con modalità che non siano incompatibili con tali finalità, e debbano essere mantenuti adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, legandosi tale principio a quello, ugualmente fondamentale, di *privacy by design e by default*, con la conseguenza che il titolare del trattamento sarà chiamato ad usare tanti e quali dati quanti ne siano necessari per le finalità che sono state individuate nelle linee direttrici dei principi di trattamento.

Non corrisponde così al vero l' affermazione per la quale il diritto all' informazione qui in commento è privo di limitazioni con riferimento al suo esercizio, considerato che le richieste dovranno essere vagliate alla luce dell' art. 5 Reg. (UE) 2016/679; tale rilievo era già stato compiuto dallo stesso Garante per la Protezione dei Dati Personali nel 2009, laddove con una specifica nota aveva rilevato come «spetta all´amministrazione destinataria della richiesta accertare il fondamento della pretesa all´informazione *ratione officii* del consigliere comunale, con valutazione eventualmente sindacabile dal giudice amministrativo»[64].

L' accessibilità alle informazioni contenenti dati personali, siano essi definiti quali dati personali comuni, relativi a categorie particolari di dati oppure concernenti reati e condanne penali[65], dovrà superare il vaglio dei principi di finalità e minimizzazione, e le

[64] Cfr. Garante Privacy, in Relazione 2008 - 2 luglio 2009 Parte II - L'attività svolta dal Garante, 3. Il Garante e le pubbliche amministrazioni, [doc. web n. 1637571], laddove l'Autorità ricordava anche come «resta ferma la necessità che i dati personali così acquisiti dagli aventi diritto siano utilizzati effettivamente per le sole finalità realmente pertinenti al mandato, rispettando il dovere di segreto nei casi specificamente determinati dalla legge, nonché i divieti di divulgazione dei dati personali».

[65] L'applicazione di tali principi non dipende, infatti, dalla tipologia di dati personali coinvolti nelle richieste del consigliere: essi si applicano anche con riguardo ad informazioni che contengano solo dati personali comuni, implicando la necessaria riconduzione delle richieste alle "esclusive" finalità di

stesse dovranno essere così inerenti le funzioni collegate al *munus* di questi soggetti qualificati. Ne discende un' implicita necessità per l' Amministrazione di verificare l'oggetto della richiesta, circoscrivendo l'ambito delle operazioni ai soli dati personali appunto indispensabili per la realizzazione dello scopo perseguito dal consigliere richiedente.

Non solo. L'applicazione dei principi di cui all' art. 25 Reg. (UE) 2016/679 conferma ancora una volta come le tutele volte alla protezione dei dati personali debbano essere individuate ed implementate «sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento», e dunque all' atto stesso dell' esercizio del diritto di accesso, al fine di «garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento».

In questo modo, si ridurrà anche la possibilità che a seguito del conseguimento delle informazioni, il consigliere possa porre in essere condotte in grado di violare i diritti riconosciuti e garantiti dal Reg. (UE) 2016/679 e dal d.lgs. 196/2003: egli avrà infatti diritto di accedere, in ragione della propria funzione istituzionale, a tanti e quali dati personali siano effettivamente necessari allo svolgimento del mandato elettivo, e gli stessi potranno così essere successivamente utilizzati in funzione del *munus* qui richiamato[66].

Ulteriori riflessioni si rendono opportune con riferimento all'applicazione delle disposizioni di cui agli artt. 24 e 32 Reg. (UE) 2016/679 come diretta conseguenza del principio di *accountability*, al fine di riprendere ed approfondire qui i rilievi prima facie esposti dalla sentenza TAR Friuli-Venezia Giulia n. 235/2020 sopra esposta per esteso. In particolare, spettando al solo Ente destinatario della richiesta l' individuazione delle modalità più corrette per permettere al consigliere di esercitare il diritto di cui all'art. 43, c. 2, TUEL, le valutazioni rimesse al titolare del trattamento dovranno necessariamente tenere conto dei profili di sicurezza e tutela dei dati personali coinvolti nel trattamento, ai sensi dell'art. 32 Reg. (UE) 2016/679 e più in generale nel rispetto dell'intera

rilevante interesse pubblico «direttamente connesse all'espletamento di un mandato elettivo», con la conseguente estensione delle riflessioni effettuate dal Garante con provvedimento Garante Privacy, Registro dei provvedimenti n. 369 del 25 luglio 2013 [doc. web n. 2536172], pronunciandosi in merito alla richiesta di ostensione di una cartella clinica e di certificazioni sanitarie, contenenti categorie particolari di dati, da parte di un consigliere regionale.

[66] Gli stessi rilievi si possono compiere anche sulla base di precedenti giurisprudenziali, come ad esempio le annotazioni del Garante per la Protezione dei Dati Personali, che nella Relazione 2007 - Garanzie e sicurezza nel trattamento dei dati: l'attività dell'Autorità - 16 luglio 2008 rilevava come «Sono stati forniti chiarimenti a un comune sulla condotta tenuta da un consigliere comunale il quale, dopo aver esercitato l'accesso ai dati contenuti nell'anagrafe della popolazione residente, ottenendo l'elenco di cittadini minorenni ricompresi in una determinata fascia di età, aveva successivamente trasmesso tale elenco a una società sportiva. Quest'ultima aveva utilizzato i dati personali in questione inviando ai minori una comunicazione promozionale in ordine all'attività esercitata e pubblicizzando, altresì, la proposta di adesione alla medesima tramite la richiesta di pagamento di una quota associativa. L'Ufficio ha rilevato che, in linea generale, il comune aveva agito correttamente nei confronti della richiesta di accesso formulata dal consigliere comunale ai sensi dell'art. 43 del d.lgs. n. 267/2000, in quanto all'ampia e qualificata pretesa non sono opponibili profili di riservatezza, a condizione che i documenti e le informazioni richiesti siano pertinenti all'esercizio del mandato. Non è apparsa invece conforme al quadro normativo di riferimento la trasmissione ad un soggetto privato dei dati anagrafici legittimamente ottenuti, in quanto tale comunicazione non risultava direttamente funzionale alla cura di un interesse connesso al mandato conferito al consigliere comunale (Nota 28 novembre 2007)».

normativa in materia di riservatezza dei dati personali.
Di conseguenza, sarà compito del titolare del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi del trattamento, individuare quali siano le modalità più corrette per l' espletamento di tale accesso, al fine di garantire la sicurezza delle informazioni personali coinvolte nel trattamento. Tali valutazioni saranno richieste in modo particolarmente pregnante ogniqualvolta il consigliere chieda di poter accedere da remoto ai gestionali informatici dell'Ente; l'identificazione delle misure sia tecniche (come ad esempio i sistemi volti ad assicurare su base permanente la sicurezza e la resilienza dei servizi di trattamento e il ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico *ex* art. 32, par. 1, lett. *b)* e *c)*) che organizzative è rimessa completamente al titolare del trattamento, il quale dovrà caso per caso valutare quali misure possano essere maggiormente adeguate, in rapporto ai rischi nello specifico evidenziati per i diritti e le libertà dei soggetti interessati, derivanti dal trattamento delle loro informazioni personali. Ne consegue che, con riferimento alle richieste di accesso al protocollo informatico, ad esempio, laddove l'Ente ritenga di non possedere una struttura informatica adeguatamente protetta, tale da poter permettere l'esplicazione di un accesso da remoto (e da pc personale) in totale sicurezza, con evidenti rischi per la sicurezza dei dati personali eventualmente coinvolti, sarà ben possibile per lo stesso provvedere all' individuazione di modalità di accesso alternative: ad esempio, la messa a disposizione di una postazione del Comune, attrezzata *ad hoc* per permettere l'accesso nominativo, in sola consultazione al solo registro di protocollo, come prospettato dallo stesso TAR Friuli-Venezia Giulia.
In tale contesto merita una menzione la necessaria valutazione, al fine di individuare le misure tecniche ed organizzative da adottare, dell'elemento richiamato nell'art. 32 Reg. (UE) 2016/679 concernente i "costi di attuazione". Specificamente, in un'ottica di interpretazione congiunta delle diverse normative che disciplinano, nel nostro ordinamento, l'accesso in via digitale ai dati della Pubblica Amministrazione, la presente analisi non può prescindere dalla valutazione delle disposizioni contenute nel CAD (Codice dell' Amministrazione Digitale, d.lgs. 82/2005). Tale testo impone a tutte le Pubbliche Amministrazioni di assicurare «la disponibilità, la gestione, l' accesso, la trasmissione, la conservazione e la fruibilità dell' informazione in modalità digitale», «utilizzando con le modalità più appropriate le tecnologie dell' informazione e della comunicazione»[67]; con riferimento a tale indicazione, l'attenzione deve essere rivolta in modo particolare alla previsione di cui all'art. 50, c. 1, dello stesso CAD, che impone che «i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l' uso delle tecnologie dell' informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall' ordinamento, da parte delle altre pubbliche amministrazioni e dei privati». Tale previsione normativa determina, inoltre, il fondamento giuridico dell' esercizio dell'accesso, ai sensi dell'art. 43, c. 2, TUEL, con possibilità di ingresso nel sistema informatico dell' Ente (ed in particolare al registro del protocollo informatico) come già visto.
La fruibilità dei dati della Pubblica Amministrazione in forma digitale è normativa-

[67] Si veda l'art. 2 c. 1, CAD d.lgs. 82/2005.

mente prevista, ma si deve ritenere come la valutazione concernente l' implementazione dei sistemi con i quali tale accessibilità deve essere garantita debba essere rimessa ad un' opportuna analisi dell' Ente nel caso di specie: tale orientamento corrisponde anche con quello recentemente espresso dal TAR Campania Salerno nella già menzionata sentenza n. 545/2019. Il Giudice di prime cure ha affermato infatti come «la complessiva disciplina risultante dal richiamato CAD impone che la fruibilità dei dati e delle informazioni in modalità digitale debba essere garantita con modalità adeguate (in finalità informativa) ed appropriate (alla tecnologia disponibile), sicché grava sull' amministrazione l' approntamento e la valorizzazione di idonee risorse tecnologiche che, senza aggravio eccessivo sulle risorse pubbliche, appaiano in grado di soddisfare, in una logica di bilanciamento, le esigenze rappresentate dalla trasparenza amministrativa»[68]. Pertanto, le valutazioni condotte dal titolare del trattamento, e dunque dall' Amministrazione interpellata, dovranno determinare un' analisi globale della situazione, monitorando sia gli aspetti di accessibilità previsti dal CAD sia le esigenze di tutela dei sistemi ed in ultima istanza (non per importanza) le necessità di protezione dei dati personali coinvolti nel trattamento, tenendo conto anche delle imprescindibili condizioni economiche dell'Ente.

Tutto ciò dedotto, nell' auspicio che il Garante per la Protezione dei Dati Personali possa pronunciarsi chiaramente in merito alla necessità di un bilanciamento tra gli interessi in gioco nella fattispecie qui analizzata, non si può che concludere affermando l'indispensabile applicazione dei principi concernenti la *data protection* anche al diritto di accesso *ex* art. 43, c. 2, TUEL, con una rimodulazione dei confini di tale diritto *sui generis*, volti ad un corretto bilanciamento con la protezione dei dati personali, al fine di definire un sistema integrato di tutele che possa operare non soltanto *ex post*, ma sin dal primo momento di tale trattamento.

[68] Cfr. TAR Campania Salerno, sez. II, 4 aprile 2019, n. 545.