European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 63-115
ISSN 2724-5969 – ISBN 979-12-218-0798-1 - DOI 10.53136/9791221807981 08

*La protezione dei dati personali nella pubblica amministrazione. L'esperienza italiana**

Sergio Niger
(Data Protection Officer at the University of Calabria, Professor of Security and Legal Issues of Computer Science at the Department of Mathematics and Informatics, University of Calabria)

ABSTRACT 25 May 2018, the Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) became fully operational. The GDPR obliges public administrations to adopt a series of appropriate technical and organizational measures to ensure that the processing of personal data takes place in compliance with the provisions of the GDPR. The most recent innovations introduced by the legislator in terms of transparency and publicity of administrative action, as well as the availability of documents, provide for various obligations for public entities to make the related information available. Mandatory disclosure must be balanced in compliance with the provisions of the GDPR.

1. *L'impatto del Regolamento UE 2016/679 sulle Amministrazioni Pubbliche*

Nel corso degli ultimi anni la pubblica amministrazione è stata investita da un poderoso processo di riforma, caratterizzato da rilevanti innovazioni normative che hanno imposto agli uffici pubblici una necessaria rivoluzione organizzativa e culturale, nonché un progressivo e faticoso adeguamento alle nuove prescrizioni.

Semplificazione amministrativa, trasparenza, prevenzione dei fenomeni di corruzione, processo di digitalizzazione, nuovo Codice dei contratti, queste sono solo alcune delle sfide con le quali gli uffici pubblici sono chiamati ogni giorno a confrontarsi.

Il processo di modernizzazione del settore pubblico in molti paesi "occidentali" è avvenuto in contemporanea con l'affermarsi delle nuove tecnologie ICT, che hanno generato importanti impatti sulla società, sulle relazioni tra individui e organizzazioni e all'interno delle stesse. In particolare, le ICT hanno contribuito a modificare in modo radicale l'accesso alle informazioni, così come i confini spazio-temporali tra individui e istituzioni pubbliche e private, modificando fabbisogni e abitudini dei cittadini. Nel soddisfare gli utenti, le ICT rispondono a tre importanti esigenze delle amministrazioni pubbliche nel processo di erogazione dei propri servizi: accessibilità, fruibilità, riduzione delle barriere spazio-temporali dei confini dell'amministrazione. Tutto ciò implica nuove modalità nella gestione delle nuove tecnologie e la tipologia di risposta deve essere univoca. È, pertanto, necessaria una forte riorganizzazione interna finalizzata all'eliminazione della frammentazione organizzativa e alla gestione condivisa ed integrata di informazioni relative ai servizi e alle richieste da parte degli utenti, i quali si aspettano risposte coerenti e in grado di soddisfare i propri bisogni.

Occorre, quindi, porsi nella logica del cambiamento sapendo che l'innovazione è cambiamento in pratica e che, pertanto, richiede una progettualità del percorso di trasformazione che non si esaurisce nella norma o nella decisione di innovare. A tal fine è necessario tener conto delle difficoltà, delle resistenze, con chiari progetti di gestione del cambiamento, con la definizione di precise responsabilità degli attori coinvolti, gli strumenti utilizzati, i percorsi da seguire in termini di competenze da sviluppare.

Le riforme amministrative degli ultimi anni hanno imposto alle amministrazioni pubbliche uno specifico dovere informativo, in quanto obbligano i soggetti pubblici a fornire informazioni su normative, attività e strutture amministrative, nonché sul funzionamento e l'erogazione dei servizi pubblici, a prescindere da un'esplicita richiesta proveniente dai cittadini.

Le più recenti novità introdotte dal legislatore in tema di trasparenza e pubblicità dell'azione amministrativa nonché di consultabilità degli atti prevedono in capo ai soggetti pubblici diversi obblighi di messa a disposizione delle relative informazioni.

* Article submitted to double-blind peer review.

Nel processo di trasformazione della pubblica amministrazione si inserisce (dal 25 maggio 2018) anche il Regolamento UE 2016/679 (*Regolamento Generale sulla protezione dei Dati*, d'ora in poi RGPD)[1], che nelle disposizioni che lo compongono riflette tutti i mutamenti avvenuti negli ultimi anni, dalla Direttiva 95/46/CE, in ambito tecnologico, economico, sociale, politico, antropologico. Con il RGPD l'Unione europea ha inteso rafforzare la tutela del diritto dei cittadini alla protezione dei dati personali, riflettendone la natura di diritto fondamentale dell'Unione stessa (art. 8 Carta dei diritti fondamentali dell'Unione e art. 16 del TFUE). Attraverso la previsione di un unico insieme di disposizioni direttamente applicabili negli ordinamenti giuridici degli Stati membri, l'U.E. vuole garantire la libera circolazione dei dati personali tra gli Stati membri e rafforzare la fiducia e la sicurezza dei consumatori, due elementi considerati indispensabili nell'ottica del nuovo mercato unico digitale[2].

Il RGPD segue l'impostazione della c.d. "direttiva madre" sulla protezione dei dati ma, facendo tesoro di vent'anni di legislazione dell'UE in materia e di giurisprudenza pertinente, chiarisce e modernizza le norme concernenti tale protezione e introduce alcuni elementi innovativi che rafforzano la tutela dei diritti delle persone e contemplano nuovi adempimenti, ma anche opportunità, per le amministrazioni pubbliche e per i soggetti privati, ossia: un quadro giuridico armonizzato che porta a un'applicazione uniforme delle norme a vantaggio del mercato unico digitale dell'Unione; parità di condizioni per tutte le imprese che operano sul mercato dell'Unione. Il RGPD impone alle imprese con sede al di fuori dell'UE di applicare le stesse norme vigenti per le imprese stabilite nell'UE quando trattano dati personali in relazione all'offerta di beni e servizi o al monitoraggio del comportamento dei cittadini nell'Unione. Le imprese che operano dall'esterno dell'UE e sono attive sul mercato unico devono, in determinate circostanze, nominare un rappresentante nell'UE al quale i cittadini e le autorità possano rivolgersi in aggiunta o in sostituzione dell'impresa con sede all'estero; i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita, che creano incentivi ad adottare sin dall'inizio soluzioni innovative in risposta ai problemi di protezione dei dati; diritti dei singoli rafforzati. Il regolamento introduce nuovi requisiti in materia di trasparenza e diritti rafforzati in materia di informazione, accesso e cancellazione; il silenzio o l'inattività non saranno più considerati valide espressioni di consenso, in quanto è richiesto un atto positivo inequivocabile per esprimerlo; è garantita la protezione dei minori online; maggiore controllo dei singoli sui propri dati personali (ad es. il diritto alla portabilità dei dati); maggiore protezione contro la violazione dei dati (c.d. *data breach*); il RGPD conferisce a tutte le autorità di protezione dei dati il potere di infliggere sanzioni pecuniarie ai titolari del trattamento e ai responsabili del trattamento; maggiore flessibilità per i titolari del trattamento e i responsabili del trattamento che trattano dati personali, grazie a disposizioni univoche in materia di responsabilità (principio di responsabilizzazione). Il regolamento si discosta da un sistema di notifica in favore del principio di responsabilizzazione, attuato tramite obblighi modulabili in funzione del rischio (per esempio l'obbligo di designare un responsabile della protezione dei dati o l'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati). Al fine di agevolare la valutazione del rischio prima di procedere al trattamento, è stato introdotto un nuovo strumento: la valutazione d'impatto sulla protezione dei dati. Quest'ultima, come

[1] L. Califano e C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2018; G. Comandè e G. Malgieri (a cura di), *Manuale per il trattamento dei dati personali: le opportunità e le sfide del nuovo Regolamento europeo sulla Privacy*, Roma, Il Sole 24 Ore, 2018; V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019; G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017; F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018; R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè, 2021; F. Pizzetti (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021.

[2] Cfr. Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018*, del 24 gennaio 2018.

vedremo in seguito, è richiesta ogniqualvolta il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche; maggiore chiarezza riguardo agli obblighi dei responsabili del trattamento e alla responsabilità dei titolari del trattamento quando selezionano un responsabile del trattamento; un sistema di *governance* moderno per garantire un'applicazione più coerente ed efficace delle norme. Il sistema prevede poteri armonizzati per le autorità di protezione dei dati, anche per quanto riguarda le sanzioni pecuniarie, e nuovi meccanismi di cooperazione in rete tra tali autorità; la protezione dei dati personali garantita dal regolamento segue i dati al di fuori dell'UE assicurando un livello elevato di protezione. In conformità con quanto prescritto dal RGPD, gli Stati membri devono adottare le misure necessarie per la rispettiva legislazione abrogando e modificando le norme esistenti, offrendo a questi la possibilità di precisare ulteriormente l'applicazione delle norme in materia di protezione dei dati in ambiti specifici, ossia: settore pubblico (art. 6, par. 2), rapporti di lavoro e sicurezza sociale (art. 88 e art. 9, par. 2, lett. *b*), medicina preventiva e medicina del lavoro, sanità pubblica (art. 9, par. 2, lett. *h* e *i*), fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici (art. 9, par. 2, lett. *j*), numero di identificazione nazionale (art. 87), accesso del pubblico ai documenti ufficiali (art. 86) e obblighi di segretezza (art. 90). Infine, per quanto concerne il trattamento di dati genetici, dati biometrici o dati relativi alla salute, il RGPD consente agli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni (art. 9, par. 4). "Le azioni degli Stati membri in questo contesto sono delimitate da due elementi:1. l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea ("Carta"), nel senso che qualsiasi legge nazionale volta a precisare le norme del regolamento deve soddisfare le condizioni previste dall'articolo 8 della Carta (e dal regolamento, che si fonda su detto articolo), e 2. l'articolo 16, paragrafo 2, del TFUE, in base al quale la legislazione nazionale non può interferire con la libera circolazione dei dati personali all'interno dell'Unione"[3].

[3] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Maggiore protezione, nuove opportunità*, 9.

Il RGPD impone alle amministrazioni pubbliche nuovi adempimenti, che non siano, però, solo di carattere formalistico e burocratico, secondo la c.d. "cultura del mero adempimento", ma richiedono alle stesse un ruolo proattivo e concreto ispirato al principio di *accountability* (che possiamo tradurre come "responsabilizzazione" o "responsabilità"). Muta, quindi, la filosofia di fondo nel trattamento dei dati personali, si passa cioè a un approccio fondato sull'*accountability*, tutto ciò comporta la modifica nella *governance*: le questioni relative al trattamento dei dati diventano questioni soprattutto di gestione del rischio. L'applicazione del RGPD interviene su più livelli: normativo, organizzativo, contrattuale, tecnologico, comunicativo. Interventi finalizzati a bilanciare la libera circolazione dei dati e i diritti fondamentali delle persone fisiche.

2. *Accountability (Responsabilizzazione / Responsabilità del Titolare) e principi applicabili di trattamento dei dati personali*

Il principio di *accountability* non rappresenta una novità assoluta nell'ambito del trattamento dei dati personali, essendo già stato oggetto di un interessante parere (n. 3/2010 sul principio di responsabilità, adottato il 13 luglio 2010) del Gruppo di lavoro Articolo 29 per la protezione dei dati. Nel succitato parere il Gruppo di lavoro ex art. 29 si soffermava sulla necessità che la protezione dei dati dovesse passare, quanto prima, "dalla teoria alla pratica". Pertanto, gli obblighi giuridici dovevano essere tradotti in misure concrete di protezione dei dati, per favorire la protezione dei dati nella pratica, il quadro giuridico dell'Unione europea doveva introdurre dei meccanismi aggiuntivi. Al riguardo, furono subito proposti nuovi istituti basati sulla responsabilità, come mezzo per incoraggiare i responsabili del trattamento ad attuare strumenti pratici e operativi per garantire una più efficace protezione dei dati: "Un principio di responsabilità vincolante imporrebbe esplicitamente ai responsabili del trattamento di attuare misure appropriate ed efficaci per dare applicazione ai principi e agli obblighi della direttiva, e per dimostrarne su richiesta l'osservanza. In pratica, ciò dovrebbe concretarsi in programmi improntati all'adattabilità mirati ad attuare i principi esistenti di protezione dei dati (talvolta denominati "programmi di conformità").

Quale complemento a tale principio, potrebbero essere istituiti obblighi aggiuntivi diretti ad attuare garanzie di protezione dei dati o ad assicurarne l'efficacia. Potrebbe trattarsi, per esempio, di una disposizione che obbliga a effettuare una valutazione d'impatto sulla privacy per le operazioni di trattamento di dati a più alto rischio"[4].

Con il progressivo effetto diluvio di dati, dovuto al continuo e inarrestabile aumento di quantità dei dati personali oggetto di trattamento mediante i più disparati dispositivi, sono aumentati drasticamente anche i rischi di abuso e di trattamento illecito degli stessi. Da qui la necessità che anche nel settore pubblico vengano attuati meccanismi reali ed efficaci per tutelare le informazioni personali. L'architettura giuridica dei meccanismi di responsabilità, delineata dal Gruppo ex Art. 29, sarebbe basata su due livelli: il primo livello sarebbe rappresentato da un obbligo vincolante per tutti i titolari del trattamento. Detto obbligo comprenderebbe due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove. "Il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure (norme di attuazione eccedenti il livello minimo)"[5].

Sotto il profilo terminologico, il termine inglese "accountability" (responsabilità) proviene dal mondo anglosassone, dove è di uso comune e dove il suo significato è ampiamente compreso e condiviso. "Ciononostante, risulta complesso definire che cosa esattamente significhi "accountability" in pratica. In generale, comunque, l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente. Nella maggior parte delle altre lingue europee, principalmente a causa delle differenze tra i sistemi giuridici, il termine "accountability" non è facilmente traducibile. Di conseguenza, il rischio di un'interpretazione variabile del termine, e quindi di una mancanza di armonizzazione, è sostanziale"[6].

Per addivenire a una proposta concreta, il Gruppo ex Art. 29 prevede che il principio generale di responsabilità avrebbe lo scopo di promuovere l'adozione di misure concrete e pratiche, in quanto trasformerebbe i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del titolare del trattamento, nel rispetto delle leggi e dei regolamenti applicabili. Il titolare del trattamento dovrebbe anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. Una disposizione generale di questo tipo si incentrerebbe su due elementi principali: 1) la necessità che il titolare del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati; 2) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile del trattamento deve fornire la prova di quanto esposto al punto 1.

Il principio generale di responsabilità sopra richiamato evita volutamente di precisare la tipologia di misura da attuare. Tutto ciò solleva due questioni di fondamentale importanza: 1) quali misure comuni soddisferebbero il principio di responsabilità? 2) Con quali modalità graduare e adattare le misure a circostanze specifiche? Al riguardo il Gruppo ex Art. 29 presenta un lungo elenco di misure comuni, che i titolari del trattamento dovrebbero adottare per ottemperare alla prima parte del principio di responsabilità. L'idoneità delle misure andrà valutata caso per caso per caso. Le misure specifiche da attuare dovranno essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare riferimento al rischio relativo al trattamento e alla tipologia di dati. Seguendo tale approccio, i titolari del trattamento devono essere in grado di adattare le misure alle specificità concrete delle loro situazioni particolari e delle operazioni di trattamento dei dati in questione.

Ciò vuol dire che non si deve partire

[4] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010 sul principio di responsabilità*, adottato il 13 luglio 2010, 3.

[5] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010*, 6.

[6] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Parere 3/2010*, 6.

semplicemente dal precetto normativo, ma dalla finalità cui tende la disposizione normativa, ossia la tutela del dato personale per poi individuare in concreto le misure da adottare in conformità con il RGPD. Si parte, quindi, dalla costruzione di un sistema di misure da parte del titolare del trattamento che deve essere in grado di garantire il rispetto dei diritti fondamentali dell'individuo alla protezione dei dati personali. Al riguardo, il RGPD non indica le misure da adottare, ma solo i principi da seguire per conseguire l'obiettivo fondamentale, ossia: la tutela dei dati personali.

Il RGPD è diventato pienamente operativo il 25 maggio 2018, ma le norme di adeguamento sono state emanate con il d.lgs. 10 agosto 2018, n. 101, con il decreto legge 8 ottobre 2021, n. 139 (convertito con modificazioni dalla legge 3 dicembre 2021, n. 205 e dal decreto legge 30 settembre 2021 n. 132 (convertito con modificazioni dalla legge 23 novembre 2021, n. 178) con i quali viene abrogato o modificato parte del precedente quadro normativo, il D.lgs, n.196/2003. Dal 2018 tutta la disciplina italiana dovrà essere interpretata alla luce del RGPD. Il regolamento europeo in materia di protezione dei dati personali diventa quindi la fonte del diritto per tutte le norme nazionali.

"Dal punto di vista della tecnica normativa si è novellato il Codice privacy previgente, pur nella consapevolezza che il Regolamento ha sostanzialmente modificato la prospettiva dell'approccio alla tutela della privacy, essendo informato ad una filosofia diversa rispetto a quella del vecchio Codice. Il nuovo approccio al rischio dettato dal legislatore europeo è, infatti, basato su numerosi istituti che si iscrivono in una prospettiva di carattere responsabilizzante, volta a trasformare la *compliance* privacy da adempimento normativo a sistema di gestione, che potremmo sintetizzare nel principio dell'a*ccountability* –ossia nella capacità di rendere conto– volto a valorizzare in capo ai *data controller* l'adozione di comportamenti proattivi, consistenti nell'obbligo per il titolare del trattamento non tanto di conformarsi passivamente a regole dettate dall'esterno, la cui osservanza formale potrebbe non rappresentare una garanzia effettiva, bensì di adottare le misure più efficaci per attuare i principi che presidiano alla protezione dei dati personali ed, all'occorrenza, dare conto ("rendicontare") delle misure giuridiche, organizzative e tecniche concretamente adottate. Pertanto, il Regolamento non effettua la scelta in molti casi specifici, ma la rimette al titolare del trattamento che è chiamato ad effettuare una valutazione, ad assumere una decisione e a provare di aver adottato misure proporzionate ed efficaci"[7].

Il Parlamento aveva raccomandato un'entrata in vigore soft della nuova disciplina, ma il d.lgs. n. 101/2018 non ha accolto tale raccomandazione. In sostanza con il d.lgs. 101/2018 si completa il percorso di armonizzazione che porta a un sistema normativo a due livelli in materia di trattamento dei dati personali. Il primo livello è quello europeo, ed è costituito dal RGPD. Quest'ultimo è la norma di fonte superiore, cui la disciplina nazionale deve allinearsi in base al principio della gerarchia delle fonti del diritto. Il secondo livello è rappresentato dal Codice per la protezione dei dati personali, emanato con il d.lgs. n. 196/2003 e modificato con il d.lgs. 101/2018. Il codice in materia di protezione dei dati personali raccoglie la normativa vigente in materia accumulatosi dal 1996 e la adegua alle disposizioni del RGDP.

Com'è noto, il RGPD è direttamente applicabile dal 25 maggio 2018. L'adeguamento dell'ordinamento italiano doveva essere coerente temporalmente con tale data. Al riguardo, la legge di delegazione europea ha stabilito, all'art. 13, comma 3, i seguenti criteri che devono ispirare il nostro legislatore:

"a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) modificare il codice di cui al d.lgs. 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati

[7] F. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, n. 22, 2018, 31.

personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse".

Oltre a ciò, fra i principi e criteri direttivi generali di cui all'art. 32 della legge 24 dicembre 2012, n. 23, sono indicati quelli del riassetto e della semplificazione normativi con l'indicazione esplicita delle norme abrogate.

Gran parte delle disposizioni del Codice è stata abrogata espressamente per essere risultate incompatibili con quelle contenute nel RGPD; norme che, a loro volta, sono per la maggior parte direttamente applicabili e costituiranno per il futuro il regime primario interno circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché circa la libera circolazione degli stessi dati. Altra e minore parte delle previsioni codicistiche nazionali è stata modificata in modo rilevante, in relazione a disposizioni del RGPD non direttamente applicabili, e che segnatamente lasciavano spazi all'intervento degli Stati membri, in particolare tramite il legislatore nazionale. In questo secondo caso, si è deciso di intervenire direttamente sul Codice introducendo nuove disposizioni o modificando quelle già presenti.

Codice e RGPD sono informati a due filosofie diverse. Il RGPD, come già rilevato, è basato sulla cosiddetta *accountability*, (responsabilità/responsabilizzazione). Questa consiste nell'obbligo per il titolare del trattamento di adottare misure appropriate ed efficaci per attuare i principi di protezione dei dati, nonché nella necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci.

Dunque il regolamento non effettua la scelta in molti casi specifici, ma la rimette al titolare del trattamento che è chiamato ad effettuare una valutazione, ad assumere una decisione e a provare di avere adottato misure proporzionate ed efficaci.

Il RGPD, facendo propria questa visione, pone, come anticipato, l'accento sulla responsabilizzazione dei titolari e dei responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione delle disposizioni regolamentari. Viene, quindi, affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati, ovviamente nel rispetto della normativa e dei criteri previsti dal RGPD.

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

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel RGPD rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (in particolare, considerando 75-77[8]); tali impatti dovranno essere analizzati

[8] Considerando (75) "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di

attraverso un apposito processo di valutazione (si vedano artt. 35-36), c.d. valutazione d'impatto, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (al riguardo, di particolare importanza sono le linee-guida in materia di valutazione di impatto sulla protezione dei dati adottate dal Gruppo "Articolo 29). All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare i rischi) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58, cioè dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Il principio di responsabilizzazione impone al titolare l'adozione del registro dei trattamenti (ai sensi dell'art. 30), di approntare misure di sicurezza che debbano "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza, poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del RGPD. La nuova normativa prevede la possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

In ogni caso, il Garante per la protezione dei dati personali potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti nel corso di questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del RGPD) potranno restare in vigore (in base all'art. 6, paragrafo 2, del RGPD) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi, ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto qualora ritengano probabile che da tale violazione possano derivare rischi per i diritti e le libertà degli interessati (considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice in materia di protezione dei dati personali. I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del RGPD. Al riguardo, di particolare rilievo sono le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo

persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati". Considerando (76) "La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato". Considerando (77) Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio".

"Articolo 29" (*Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679, adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 versione emendata e adottata il 6 febbraio 2018*). Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (art. 33, paragrafo 5).

Anche la designazione di un "Responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: *Data Protection Officer*) riflette l'approccio responsabilizzante che è proprio del RGPD (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35.

Il RGPD (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è appunto il principio detto di "responsabilizzazione" (o *accountability*), il quale richiede la messa in atto da parte del titolare di tutte le misure sopra citate; principio che viene poi esplicitato ulteriormente dall'art. 24, paragrafo 1, del RGPD, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento".

Alla luce anche del principio di *accountability*, ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, ossia: liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato; limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati; minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento; esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento; limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento; integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Una delle misure più importanti e concrete, nell'ambito del principio di responsabilizzazione, che il titolare del trattamento deve porre in essere riguarda la trasparenza delle attività di trattamento dati che pone in essere.

3. *Trasparenza nel trattamento dei dati personali da parte delle Amministrazioni Pubbliche*

Chi intende effettuare un trattamento di dati personali deve fornire all'interessato alcune informazioni, anche per metterlo nelle condizioni di esercitare i propri diritti, previsti agli artt. 15-22 del RGPD. Il principio di trasparenza[9], inteso come obbligo di rendere conoscibili le modalità con cui i dati sono raccolti, utilizzati e consultati grazie a comunicazioni e informazioni facilmente accessibili e comprensibili, utilizzando un linguaggio chiaro e semplice (considerando 39)[10], ha nel RGPD un ruolo fondamentale e

[9] M. Dell'Utri, *Il principio di trasparenza*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, 199; F. Pizzetti, *Trasparenza nel trattamento dati, che cambia col GDPR: l'alba di un nuovo valore sociale*, in *Agenda Digitale*, 2018 (*https://www.agendadigitale.eu/sicurezza/trasparenza-nel-trattamento-dati-che-cambia-col-gdpr-lalba-di-un-nuovo-valore-sociale/*).

[10] Considerando (39) "Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero es-

potenzialmente molto espansivo.

La trasparenza è un obbligo trasversale a norma del RGPD, che si esplica in tre elementi centrali: 1) la fornitura agli interessati d'informazioni relative al trattamento corretto; 2) le modalità con le quali il titolare del trattamento comunica con gli interessati riguardo ai diritti di cui godono ai sensi del regolamento; 3) le modalità con le quali il titolare del trattamento agevola agli interessati l'esercizio dei diritti di cui godono. Il Gruppo di lavoro Articolo 29 ha adottato, al riguardo, le Linee guida sulla trasparenza ai sensi del Regolamento 2016/679, adottate il 29 novembre 2017 ed emendate l'11 aprile 2018.

Dette linee guidano mirano, soprattutto, a consentire ai titolari del trattamento di comprendere, a un livello elevato, come il Gruppo interpreti gli effetti pratici degli obblighi di trasparenza e a indicare l'approccio che, secondo il Gruppo, i titolari del trattamento devono adottare per essere trasparenti, ricomprendendo al contempo correttezza e responsabilizzazione nelle loro misure di trasparenza.

La trasparenza è un aspetto che da tempo si è radicato nel diritto dell'Unione europea. È finalizzata infondere fiducia nei processi che riguardano i cittadini, permettendo loro di comprenderli e, se necessario, di opporvisi. Inoltre, è espressione del principio di correttezza in relazione al trattamento dei dati personali affermato all'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Ai sensi dell'art. 5, paragrafo 1, lettera a), del RGPD, oltre ai requisiti che il trattamento dei dati sia lecito e corretto, la trasparenza è ora inclusa in quanto elemento fondamentale di questi principi, questa, infatti, è intrinsecamente legata alla correttezza e al nuovo principio di responsabilizzazione ai sensi del RGPD. Il titolare del trattamento dev'essere sempre in grado di dimostrare che i dati personali sono trattati in modo trasparente nei confronti dell'interessato (art. 5, paragrafo 2, RGPD). A questo si aggiunge il fatto che il principio di responsabilizzazione impone la trasparenza delle operazioni di trattamento affinché il titolare del trattamento sia in grado di dimostrare il rispetto degli obblighi che il regolamento gli impone.

Secondo il considerando 171 del RGPD, laddove il trattamento fosse stato già in corso prima del 25 maggio 2018, il titolare del trattamento avrebbe dovuto garantirne la conformità agli obblighi di trasparenza alla data del 25 maggio 2018 (così come a tutti gli altri obblighi previsti dal regolamento). Ciò significa che prima del 25 maggio 2018 il titolare del trattamento avrebbe dovuto revisionare tutte le informazioni fornite agli interessati con riferimento al trattamento dei dati personali che li riguardano (ad esempio in dichiarazioni/informative sulla privacy, ecc.), al fine di garantire l'adempimento degli obblighi di trasparenza esaminati nelle citate linee guida.

Quando il titolare del trattamento la rispetta, la trasparenza consente agli interessati di imputare la responsabilità al titolare e al responsabile del trattamento e di esercitare il controllo sui dati personali che li riguardano, ad esempio dando o revocando il consenso informato e attivando i loro diritti di interessati.

Gli obblighi d'informazione sono specificamente indicati negli artt. 12-14 del RGPD. La qualità, l'accessibilità e la comprensibilità delle informazioni sono i requisiti fondamentali in grado di garantire la trasparenza del trattamento e fornire indicazioni concrete circa il principio di finalità alla base di ogni trattamento dati.

Gli obblighi di trasparenza imposti dal regolamento si applicano a prescindere dalla base giuridica del trattamento e per tutto il ciclo di vita dello stesso. Ciò risulta chiaro dall'art. 12, il quale stabilisce che la trasparenza si applica nelle seguenti fasi del ciclo di trattamento dei dati:

- prima o all'inizio del ciclo di trattamento dei dati, vale a dire quando i dati personali sono raccolti presso l'interessato od ottenuti in altro modo;
- nell'arco dell'intero ciclo di vita del trattamento, ovvero nella comunicazione con gli interessati sui loro diritti;

sere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento".

- in momenti specifici in cui il trattamento è in corso, ad esempio quando si verifica una violazione di dati oppure in caso di modifica rilevante del trattamento.

Il concetto di trasparenza non viene definito all'interno del regolamento. Il considerando 39 del RGPD, come già rilevato, ne illustra il significato e l'effetto nell'ambito del trattamento dei dati.

L'art. 12 del RGPD fissa le regole generali che si applicano alla fornitura delle informazioni agli interessati (ai sensi degli artt. 13 e 14 del RGPD), alla comunicazione con gli interessati riguardo all'esercizio dei loro diritti (ai sensi degli artt. 15-22 del RGPD) e alle comunicazioni relative alle violazioni di dati (art. 34 del RGPD). In particolare, l'articolo 12 impone che le informazioni o le comunicazioni in questione debbano rispettare i criteri seguenti: devono essere concise, trasparenti, intelligibili e facilmente accessibili; devono essere formulate con un linguaggio semplice e chiaro; il requisito di un linguaggio semplice e chiaro è di particolare importanza nel caso d'informazioni destinate ai minor; devono essere fornite per iscritto "o con altri mezzi, anche, se del caso, con mezzi elettronici"; se richiesto dall'interessato, possono essere fornite oralmente; devono essere in genere gratuite.

L'obbligo di fornire agli interessati le informazioni e le comunicazioni in forma "concisa e trasparente" implica che il titolare del trattamento presenti le informazioni/comunicazioni in maniera efficace e succinta al fine di evitare il c.d. "subissamento" informativo. Tali informazioni dovrebbero essere differenziate nettamente da altre che non riguardano la vita privata, quali clausole contrattuali o condizioni generali d'uso. Nell'ambiente online l'utilizzo di una dichiarazione/informativa sulla privacy stratificata può consentire all'interessato di consultarne immediatamente la specifica sezione desiderata, senza dover scorrere ampie porzioni di testo alla ricerca di un argomento in particolare.

L'obbligo di fornire informazioni "intelligibili" implica che queste debbano risultare comprensibili a un esponente medio del pubblico cui sono dirette. L'intelligibilità è strettamente connessa all'obbligo di utilizzare un linguaggio semplice e chiaro. Il titolare dei dati responsabilizzato saprà su che tipo di persone raccoglie informazioni e potrà utilizzare tali conoscenze per stabilire che cosa è probabile che il pubblico in questione comprenda.

Un aspetto fondamentale del principio della trasparenza messa in luce nelle linee guida risiede nel fatto che l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano Ciò costituisce un aspetto importante del principio di correttezza di cui all'articolo 5, paragrafo 1, del regolamento ed è altresì connesso al considerando 39, il quale stabilisce che "[è] opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali...".

L'elemento della "facile accessibilità" implica che l'interessato non sia costretto a cercare le informazioni, ma che anzi gli sia immediatamente chiaro dove e come queste siano accessibili.

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del RGPD) deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati (se raccolti direttamente presso l'interessato, art. 13 del RGPD).

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del RGPD), l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).

I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13, paragrafo 1, e 14, paragrafo 1, del RGPD e, in parte, sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD (Responsabile della protezione dei dati), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Se i dati non sono raccolti direttamente presso

l'interessato (art. 14 del RGPD), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

Il Regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Qualora il trattamento contemplasse processi decisionali automatizzati (anche la profilazione), l'informativa dovrebbe specificarlo e dovrebbe indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: art. 12, paragrafo 1, e considerando 58 del RGPD). Sono comunque ammessi "altri mezzi", quindi può essere fornita anche in forma orale, ma nel rispetto delle caratteristiche di cui sopra rappresentate (art. 12, paragrafo 1, RGPD).

Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone in futuro dovranno essere uniformate in tutta l'Ue attraverso l'intervento dalla Commissione europea.

In base al Regolamento, si deve porre particolare attenzione alla formulazione dell'informativa, che deve essere soprattutto comprensibile e trasparente per l'interessato, attraverso l'uso di un linguaggio chiaro e semplice. Per quanto riguarda i minori devono essere predisposte idonee informative (Considerando 58)[11].

La prospettiva da cui parte la nuova disciplina europea in materia di protezione dei dati personali è quella del "nuovo mondo digitale", le cui insidie sono rinvenibili non solo nel trattamento dei dati ma anche negli effetti da esso derivanti. In tal senso, si è spesso fatto ricorso proprio ai principi di trasparenza e lealtà del trattamento per chiedere che le informative fornite agli utenti consentissero di comprendere in modo adeguato non solo le modalità di trattamento, potevano verificarsi rispetto agli interessati e agli utenti[12].

4. *Il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri come base giuridica*

Dalla lettura del RGPD emerge chiaramente come, nel caso del titolare del trattamento sia un soggetto pubblico, presupposti e modalità del trattamento si differenzino da quelli che presiedono al trattamento operato da soggetti privati. Il primo elemento saliente concerne proprio la possibile base giuridica del trattamento. Nel caso delle amministrazioni pubbliche, infatti, questa può essere data non solo dal consenso o dall'esistenza di un obbligo legale, ma anche dalla necessità del trattamento per "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Al riguardo l'art 2-ter del Codice prevede che: la base giuridica prevista dall'art. 6, par. 3, lettera b), del regolamento è costituita da una norma di legge o di regolamento o da atti amministrativi generali. Fermo restando ogni altro obbligo previsto dal Regolamento e dal Codice, "il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi

[11] Considerando (58) "Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente".

[12] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016; C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018.

comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nonché da parte di una società a controllo pubblico statale o, limitatamente ai gestori di servizi pubblici, locale, di cui all' articolo 16 del testo unico in materia di società a partecipazione pubblica, di cui al decreto legislativo 19 agosto 2016, n. 175 , con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato, è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento"[13].

Se il trattamento per l'esecuzione di un interesse pubblico o per l'esercizio di pubblici poteri è un requisito alternativo all'obbligo legale, ciò significa che la valutazione della necessarietà può essere rimessa all'amministrazione procedente, alla quale la legge ha assegnato il potere di curare l'interesse pubblico in una data materia o per una determinata funzione.

L'interpretazione letterale non offre ragioni per ritenere superato quanto ritenuto prima delle modifiche introdotte al Codice, in merito alla possibilità di trattare dati personali "comuni" da parte di soggetti pubblici anche in assenza di una legge che lo preveda espressamente[14]. Al contrario, si può legittimamente ravvisare nello stesso art. 5 del RGPD la base giuridica "sufficiente per rientrare nel rispetto del principio di legalità dell'azione amministrativa e del fondamento legittimo previsto dalla legge richiesto per il trattamento dei dati personali dall'art. 8 della Carta dei diritti fondamentali UE, nel senso di consentire alla pubblica amministrazione di trattare dati semplici o ordinari, per i quali non c'è un esplicito divieto di trattamento, per finalità di interesse pubblico; e di ricondurre in tal caso nell'ambito e nei limiti del principio di proporzionalità dell'attività amministrativa le previsioni recate dall'art. 6 per il trattamento di dati ordinari o semplici"[15].

La comunicazione[16] fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del RGPD e di quelli relativi a condanne penali e reati di cui all'art. 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa "se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis" del Codice.

Al riguardo, il Garante per la protezione dei dati personali ha precisato che "Ai sensi della disciplina in materia, il trattamento di dati personali effettuato in ambito pubblico è lecito solo se tale trattamento è necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" oppure "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6, par. 1, lett. c) ed e)). Al riguardo, si evidenzia che la comunicazione di dati personali – ossia "il dare conoscenza dei dati personali a uno o più soggetti determinati

[13] Sul punto, F. Cardarelli, *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in G. Finocchiaro, R. D'Orazio, O. Pollicino e G. Resta (a cura di), *Codice della privacy e data protection*, Milano, Giuffrè 2021: "L'art. 6 del Regolamento elenca sei basi giuridiche (le quali rappresentano quindi i presupposti di legittimazione del trattamento) che rendono lecito e legittimo, fin dall'origine, il trattamento di dati "comuni". Tale disposizione, riprendendo quasi integralmente le previsioni dell'art. 7 della dir. 95/46/CE, àncora la liceità del trattamento alla sussistenza di presupposti che si fondano due requisiti generali alternativi (il consenso dell'interessato — par. 1, lett. a — oppure la necessità del trattamento — par. 1, lett. b-f). Tra queste ipotesi di trattamento necessario le lett. c) ed e) della disposizione contemplano "c) l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento", "e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

[14] F. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 4 ss.

[15] F. Francario, *Protezione dei dati personali e pubblica amministrazione*, in C. Pisani, G. Proia e A. Topo (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022.

[16] Per comunicazione si intende: "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" (Art. 2 – ter, comma 4 lett. a), D.lgs. n. 196/2003).

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'art. 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" – diversi da quelli previsti dagli artt. 9 e 10 del Regolamento (UE) 2016/679, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, è ammessa se prevista esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-ter del Codice). Con riguardo alle categorie particolari di dati personali, inclusi quelli relativi alla salute (in merito ai quali è previsto un generale divieto di trattamento, ad eccezione dei casi indicati all'art. 9, par. 2 del Regolamento e, comunque, un regime di maggiore garanzia rispetto alle altre tipologie di dati, in particolare, per effetto dell'art. 9, par. 4, nonché dell'art. 2-septies del Codice), il trattamento è consentito, quando "necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. g), del Regolamento). Il legislatore nazionale ha definito "rilevante" l'interesse pubblico per il trattamento "effettuato da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri" nelle materie indicate, seppur in modo non esaustivo, dall'art. 2-sexies del Codice, stabilendo che i relativi trattamenti "sono ammessi qualora siano previsti […] da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato". Il trattamento dei dati personali deve inoltre avvenire nel rispetto dei principi indicati nell'art. 5 del Regolamento, fra cui quelli di "liceità, correttezza e trasparenza" nonché di "minimizzazione dei dati", secondo i quali i dati personali devono essere – rispettivamente – "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" nonché "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5 par. 1, lett. a) e c)"[17].

La diffusione[18] e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente "se previste ai sensi del comma 1 o se necessarie ai sensi del comma 1-bis" del Codice. In tale ultimo caso, ne viene data notizia al Garante per la protezione dei dati personali almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

4.1. *Il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*

Come chiarito nei capitoli che precedono, quei dati che un tempo denominavamo dati sensibili, con l'entrata in vigore del RGPD hanno cambiato nome. Adesso sono denominati "dati particolari" e sono una tipologia della più ampia categoria dei dati personali. Secondo l'art. 9, par. 1, del RGPD, è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il trattamento di dati particolari da parte della PA, così come previsto dall'art. 9, par. 2, lett. g) GDPR, è ammesso solo se è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Il Legislatore nazionale, mediante il D.lgs. 101/2018, ha previsto all'art. 2-sexies, rubricato

[17] Garante per la protezione dei dati personali, 25 febbraio 2021, (doc. web n. 9565218).

[18] Per diffusione si intende: "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione" (Art. 2 – ter, comma 4 lett. b), D.lgs. n. 196/2003).

"Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante" che: "I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. 2. Fermo restando quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: accesso a documenti amministrativi e accesso civico; tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità; tenuta di registri pubblici relativi a beni immobili o mobili; tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli; cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato; elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari; Garante per la protezione dei dati personali esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche; svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo; attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale; attività di controllo e ispettive; concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni; conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali; rapporti tra i soggetti pubblici e gli enti del terzo settore; obiezione di coscienza; attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose; attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci; attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano; compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale; vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili; bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario; cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione,

l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati Garante per la protezione dei dati personali dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan); dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva". Occorre evidenziare che tale elenco deve intendersi come esemplificativo e non esaustivo e il riferimento alla base giuridica dell'interesse pubblico rilevante ha un forte ancoraggio al principio di legalità sostanziale. Pertanto, l'art. 2-sexies del Codice si sofferma diffusamente sul trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante.

5. *Il Responsabile della Protezione dei Dati nelle Amministrazioni Pubbliche*

Il RGPD fondato, come già più volte messo in luce, sul principio di accountability, delinea, in parte, un nuovo quadro giuridico e pone al centro di questo la figura del Responsabile della protezione dei dati (d'ora in poi, RPD). Questa figura non rappresenta una novità assoluta nel panorama europeo, dato che in molti Stati membri, pur non essendo prevista dalla direttiva 95/46/CE, la nomina del RPD è divenuta, nel corso degli anni, una prassi. Anche la Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, contempla all'art. 32 la designazione del RPD: "Gli Stati membri dispongono che il titolare del trattamento designi un responsabile della protezione dei dati. Gli Stati membri possono esentare le autorità giurisdizionali e le altre autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali da tale obbligo".

Il Gruppo Articolo 29 per la protezione dei dati personali ha più volte sottolineato, prima dell'adozione del RGPD, che la figura del RPD rappresenta un elemento chiave all'interno del nuovo sistema di governance dei dati e una figura fondamentale ai fini della "responsabilizzazione", e che tale nomina possa rendere più agevole l'applicazione della normativa: "oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente"[19].

Il RGPD (considerando 97) prevede che "per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali

[19] Gruppo di lavoro Articolo 29 per la protezione dei dati, *Linee guida sui responsabili della protezione dei dati, adottate il 13 dicembre 2016*, versione emendata e adottata in data 5 aprile 2017.

responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

Ai sensi dell'art. 37, par.1, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici: a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico; b) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; c) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, sono quindi obbligati a nominare un RPD. Al riguardo, l'art. 37, par. 1, lett. a), del RGPD prevede che i titolari e i responsabili del trattamento designino un RPD "quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali". L'atto di designazione è parte costitutiva dell'adempimento. Il RGPD non fornisce la definizione di "autorità pubblica" o "organismo pubblico" e, come chiarito anche nelle Linee guida adottate in materia dal Gruppo Art. 29 (Linee guida sui responsabili della protezione dei dati, adottate il 5 aprile 2017), ne rimette l'individuazione al diritto nazionale applicabile. Allo stato, in ambito pubblico, secondo le indicazioni fornite dal Garante per la protezione dei dati personali[20], devono ritenersi tenuti alla designazione di un RPD i soggetti che oggi ricadono nell'ambito di applicazione degli artt. 18 – 22[21] del Codice in materia di protezione dei dati personali, che stabiliscono le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio: le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.). Al riguardo, occorre richiamare la nozione di "organismo pubblico" come definita al par. 1.3 dell'Allegato alla Raccomandazione n. R (91) 10 del Comitato dei Ministri del Consiglio d'Europa, adottata il 9 settembre 1991: "l'espressione organismi pubblici indica qualsiasi amministrazione, istituzione, ente o altra entità che eserciti funzioni di servizio pubblico o di interesse pubblico tramite prerogative proprie dei pubblici poteri". Una definizione di "ente pubblico" e di "organismo di diritto pubblico" possiamo rinvenirla anche nell'art. 1, par. 1 e 2, della direttiva 2003/98/CE.

Il Garante raccomanda però che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), sarebbe auspicabile, ancorché non obbligatorio, che anche detti soggetti procedessero alla designazione di un RPD.

Qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti (in termini di criteri per la designazione, posizione e compiti) che valgono per i RPD designati in via obbligatoria.

Come già rilevato, nel RGPD non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo Art. 29, nelle predette Linee guida, precisa che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico. In questi casi la nomina di un RPD è obbligatoria. E, al riguardo, aggiunge che "lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di

[20] Garante per la protezione dei dati personali, Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29), www.garanteprivacy.it, docweb 7322110.

[21] Sul punto, P. Troiano, *Art. 18 – Regole applicabili a tutti i trattamenti effettuati da soggetti pubblici*, in C.M. Bianca e F.D. Busnelli (a cura di), *La protezione dei dati personali*, Padova, Cedam, 2007, 456-474.

disciplina professionale. In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD". Anche se nei casi sopra riportati non sussista l'obbligo di nominare un RPD, il Gruppo di lavoro consiglia che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD.

Con l'espressione "attività principali", sempre secondo il Gruppo Art. 29, possiamo intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento. Detta espressione ("attività principali") non va, ovviamente, interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisca una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento.

L'art. 37 del RGPD fa riferimento, per la nomina obbligatoria del RPD, al trattamento di dati personali su "larga scala". Nel regolamento non figura alcuna definizione di trattamento su "larga scala". Il considerando 91 fornisce, però, alcune indicazioni al riguardo: per trattamenti su "larga scala" si intendono quelli "che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". Pertanto, al fine di stabilire se un trattamento sia effettuato su larga scala è necessario tener conto: del numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; del volume dei dati e/o delle diverse tipologie di dati oggetto di trattamento; della durata, ovvero la persistenza, dell'attività di trattamento; della portata geografica dell'attività di trattamento.

Il RGPD non si sofferma neppure sul concetto di "monitoraggio regolare e sistematico", al riguardo giova riprendere quanto affermato, nelle predette Linee guida, dal Gruppo Art. 29: "Il considerando 24 menziona il monitoraggio del comportamento di detti interessati ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati. L'aggettivo regolare ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; ricorrente o ripetuto a intervalli costanti; che avviene in modo costante o a intervalli periodici. L'aggettivo sistematico ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolto nell'ambito di una strategia". Alcuni esempi di attività che possono comportare il "monitoraggio regolare e sistematico" di interessati possono essere: "curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.".

Per quanto riguarda la nomina di un RPD, l'art. 37 non distingue fra titolari del trattamento e responsabili del trattamento in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione. Tra

l'altro, qualora il titolare del trattamento sia tenuto, in base ai succitati criteri, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina, che però può costituire una buona prassi.

L'art. 37, par. 2, del RGPD, permette la designazione di un unico RPD per più organismi (es. gruppo imprenditoriale) a condizione che il responsabile sia "facilmente raggiungibile da ciascuno stabilimento". Ovviamente, il concetto di "raggiungibilità" è riferito ai compiti del RPD in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente, dato che uno dei compiti del RPD, ai sensi dell'art. 39, p. 1, lett. a), consiste "nell'informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento". Il RPD deve essere in grado di comunicare con gli interessati in modo efficiente. Al riguardo, appare opportuno ricordare quanto previsto dall'art. 12, par. 1, del RGPD "Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori". Il RPD deve essere anche in grado di comunicare e collaborare con le autorità di controllo interessate. L'art. 37, par. 3, consente la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenendo sempre presente la loro struttura organizzativa e la dimensione. Il titolare o il responsabile, poiché il RPD è chiamato a una molteplicità di funzioni, deve assicurarsi che un unico RPD, se necessario supportato da un gruppo di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

Il RPD è designato in funzione delle qualità professionali, "in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39" (art. 37, par. 5, RGPD). Al riguardo, il considerando 97 prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

Il livello di conoscenza specialistica richiesto, come fatto giustamente rilevare nelle Linee guida del Gruppo Art. 29, non trova una definizione tassativa. Pertanto, andrebbe proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. "Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi".

Il RGPD all'art. 37, par. 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un RPD. Al riguardo, sarebbe necessario prendere in considerazione la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD. Viene considerata utile anche la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento, nonché una conoscenza delle operazioni di trattamento svolte con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare. Negli ultimi tempi spesso ci si è chiesti quali certificazioni risultino idonee a legittimare il RPD nell'esercizio delle sue funzioni, ai sensi degli artt. 42 e 43 del RGPD. Il Garante per la protezione dei dati personali ha ritenuto opportuno precisare che "come accade nei settori delle cosiddette professioni non regolamentate, si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del RGPD) sono rilasciate anche all'esito della partecipazione ad attività formative e al controllo dell'apprendimento. Esse, pur rappresentando, al pari di altri titoli,

un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD".

Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

Il RPD deve essere in grado di assolvere i propri compiti, tenendo conto delle qualità personali e delle sue conoscenze, nonché della posizione dello stesso all'interno dell'amministrazione. Il RPD svolge un ruolo chiave, di assoluta centralità, nel promuovere la cultura della protezione dei dati all'interno dell'amministrazione, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

Il titolare del trattamento e il responsabile del trattamento devono assicurare che il RPD sia "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali". Il RPD va coinvolto, infatti, in ogni questione relativa alla protezione dei dati personali: "Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il RPD vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni. Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento. Ciò significa che occorrerà garantire, per esempio: che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello; la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea; che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il Gruppo di lavoro raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD; che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente".

L'art. 38, par. 2, del RGPD prevede che il titolare del trattamento o il responsabile del trattamento debbano adeguatamente sostenere il RPD "fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".

Il RPD deve poter operare con una certa autonomia all'interno dell'organizzazione del titolare o del responsabile, questi non deve, infatti, ricevere alcuna istruzione per quanto riguarda l'esecuzione dei compiti ad egli demandati. I RPD "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente" (Considerando 97). Nell'esecuzione dei compiti attribuitigli dall'art. 39, il RPD non deve ricevere istruzioni sull'approccio da seguire nel caso specifico, quali siano i risultati attesi, come eventualmente condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo, né ricevere istruzioni sull'interpretazione da fornire a una specifica questione in tema di protezione dati. I margini decisionali del RPD sono ben delineati nell'art. 39 del RGPD. Sul punto rilevano correttamente le Linee guida del Gruppo Art. 29 che "Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza. Se il titolare del trattamento o il responsabile del trattamento assumono decisioni incompatibili con il RGPD e le

indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'articolo 38, paragrafo 3, prevede che il RPD riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel quadro delle sue funzioni di informazione e consulenza a favore del titolare del trattamento o del responsabile del trattamento. Un altro esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico".

L'art. 38, par. 3, del RGPD mira a potenziare ulteriormente l'autonomia e l'indipendenza del RPD prevedendo che non debba essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. In base all'art. 38, par. 6, al RPD è consentito di "svolgere altri compiti e funzioni", ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che "tali compiti e funzioni non diano adito a un conflitto di interessi".

A seconda della natura dei trattamenti e delle attività e dimensioni della struttura del titolare o del responsabile, le eventuali ulteriori incombenze attribuite al RPD non dovrebbero pertanto sottrarre allo stesso il tempo necessario per adempiere alle relative responsabilità.

"In linea di principio, è quindi ragionevole che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al RPD ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle asl). In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, l'attribuzione delle funzioni di RPD al responsabile per la prevenzione della corruzione e per la trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti che il RGPD attribuisce al RPD" (Garante per la protezione dei dati personali, Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico, www.garanteprivacy.it, docweb 7322110).

Tra i diversi compiti affidati al RPD, l'art. 39, par. 1, lett. b), del RGPD riconosce al RPD il compito di sorvegliare l'osservanza del Regolamento. Il titolare del trattamento o il responsabile del trattamento, secondo il considerando 97, dovrebbe essere assistito dal RPD nel controllo del rispetto a livello interno del Regolamento.

In particolare, tra i compiti di controllo svolti dal RPD rientrano: la raccolta di informazioni per individuare i trattamenti svolti; l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Sul punto, le Linee guida del Gruppo Art. 29 fanno giustamente rilevare che "Il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza. Il RGPD chiarisce che spetta al titolare, e non al RPD, "mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento" (articolo 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD".

Il RPD svolge un ruolo non secondario nella gestione della valutazione di impatto di cui all'art. 35 del RGPD. Tuttavia, appare opportuno sottolineare che, ai sensi dell'art. 35, par. 1, spetta al titolare del trattamento, e non al RPD, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati[22]. Il RPD svolge, però, un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di detta valutazione. In applicazione del principio di data protection by design, l'art. 35, par. 2, prevede

[22] Sul punto si rinvia alle Linee-guida del Gruppo Art. 29 concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 – WP248adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 (http://ec.europa.eu/newsroom/article29/item-detailegge cfm?item_id=611236).

espressamente che il titolare si consulti con il RPD quando svolge una valutazione di impatto. L'art. 39, par. 1, lett. c), del RGPD affida al RPD il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35". Il Gruppo Art. 29 raccomanda che il titolare del trattamento si consulti con il RPD, fra l'altro, sulle seguenti tematiche: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate; se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD. Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

Il titolare del trattamento deve definire con chiarezza (per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa) i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della valutazione di impatto.

Il RPD deve cooperare con l'autorità di controllo e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione" (art. 39, par. 1, lett. d ed e). Detti compiti rientrano nel ruolo di "facilitatore" attribuito al RPD, questi funge anche da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti riconosciutele dall'art. 57 del RGPD e ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi previsti all'art. 58 del RGPD. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'art. 39, par. 1, prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

L'art. 30 del RGPD prevede che il titolare del trattamento o il responsabile del trattamento debbano tenere un registro delle attività di trattamento svolte sotto la propria responsabilità ovvero un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento. "Nella realtà, sono spesso i RPD a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE". Detto registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento. "In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'articolo 30 deve essere considerato anche uno strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione".

Come messo in luce da Antonello Soro[23], ex Presidente del Garante per la protezione dei dati personali, il protagonista della "rivoluzione" innescata dal RGPD è, accanto al titolare, proprio il RPD: figura da cui dipende la "scommessa" dell'*accountability*, la capacità cioè di fare della protezione dati non tanto un onere legale da assolvere quanto un elemento di vantaggio competitivo su cui puntare per reggere alle sfide di un mercato sempre più fondato sui dati, dei quali è quindi indispensabile assicurare protezione, qualità,

[23] Sul punto l'intervento di Antonello Soro, ex Presidente dell'Autorità Garante per la protezione dei dati personali, in occasione della piena applicazione del Regolamento (UE) 2016/679, 25 maggio 2018, Protezione dei dati: garanzia di libertà nella società digitale.

esattezza, sicurezza.

6. *Accesso a documenti amministrativi e protezione dei dati personali*

"La conoscenza ci dà potere", "sapere ci aiuta a decidere", "conoscere ci libera", è il 3 febbraio 2019 e la voce narrante dell'attore Tom Hanks declama le tre frasi chiave dello spot andato in onda durante la finale del campionato di football americano, uno spot commissionato dal Washington Post. "La democrazia muore nell'oscurità" è lo slogan finale, lo stesso che costituisce il motto del giornale che illuminò i Pentagon Papers sulla guerra in Vietnam e lo scandalo Watergate. Il terzo millennio ci ha portato anche in dote un'informazione self-made, tutta fondata sui social e sulle condivisioni, ingenerando il grande e pericoloso equivoco che non occorra autorevolezza per raccontare la realtà. Troppo spesso la quantità dell'informazione uccide la qualità e la breaking news a tutti i costi, tipiche dei siti web, appiattisce lo spessore dei fatti e nega loro complessità. I cittadini hanno bisogno di informazioni di qualità e di trasparenza al fine di attivare reali meccanismi di partecipazione democratica.

La trasparenza è uno dei miti assoluti dei nostri tempi, un tema articolato, complesso e scivoloso. In questa sezione, il tema sarà analizzato sotto il profilo più squisitamente giuridico della trasparenza dell'amministrazione pubblica, tralasciando gli aspetti filosofici e sociologici.

Gli strumenti di realizzazione del principio di trasparenza sono diversi. Alcuni di essi sono individuati nelle disposizioni della legge n. 241/1990, a questi si aggiungono le previsioni in materia di semplificazione del linguaggio dell'amministrazione, dirette a garantire maggiore visibilità dei contenuti dell'azione amministrativa.

Nell'ordinamento italiano, la trasparenza, e più in generale la disciplina del rapporto dialogico tra pubblica amministrazione e cittadino, è un istituto di recente introduzione, essendo stata prevista espressamente solo con la legge n. 241/1990.

Si tratta di un principio tutt'altro che statico: la trasparenza, infatti, costituisce uno dei gangli del diritto pubblico maggiormente soggetto all'evoluzione politica, sociale e tecnologica.

Il concetto di trasparenza nell'ordinamento giuridico italiano, nel corso degli anni, è stato legato al processo di semplificazione amministrativa, alla maggiore partecipazione dei cittadini ai processi decisionali, a una maggiore democratizzazione del rapporto tra cittadino e amministrazione per il miglioramento di quest'ultima, in particolare sotto i profili dell'efficienza e dell'imparzialità.

Il tema della trasparenza si lega a quello, come già rilevato, della semplificazione amministrativa, "La semplificazione dell'ordinamento è un compito che presenta gravissime difficoltà; ed è inutile cercare di superarle se non si hanno delle idee chiare. Insomma, bisogna sapersi orientare, anzi che procedere a tentoni"[24]. Oggi un dato certo è che per orientarsi nel semplificare occorre definire obiettivi, potenziali criticità, soggetti coinvolti, ricadute. Semplificare vuol dire attivare un processo di riforma della normativa esistente, ma anche di formazione di nuove regole, basato su dati empirici e sul coinvolgimento di tutti i soggetti interessati. "Le semplificazioni vanno anche programmate nel tempo, in modo da bilanciare adeguatamente gli sforzi in funzione di priorità condivise e raggiungibili"[25].

Con la legge 7 agosto 1990, n. 241, la semplificazione amministrativa assurge a principio generale dell'azione amministrativa, ma a quasi trent'anni dall'affermarsi di una specie di "dittatura culturale della semplificazione"[26], per usare le parole di Michele Ainis, i risultati appaiono deludenti[27]. In tale quadro, la trasparenza amministrativa diventa anch'essa un principio generale dell'attività e dell'organizzazione della

[24] F. Carnelutti, *Certezza, autonomia, libertà, diritto*, in *Il diritto dell'economia*, 1956, 1193.
[25] N. Rangone, *Semplificazione amministrativa*, in *Enciclopedia italiana Treccani*, IX Appendice, 2015, su *www.treccani.it/enciclopedia/semplificazione-amministrativa_%28Enciclopedia-Italiana%29/*
[26] M. Ainis, *La semplificazione complicante*, in *Federalismi.it*, 2014, 18, 2-9.
[27] Si vedano sul punto le conclusioni di un'indagine conoscitiva sulla semplificazione che descrivono un Paese «auto-avviluppato in una miriade di lacci e lacciuoli» (Commissione parlamentare per la semplificazione, Indagine conoscitiva sulla semplificazione legislativa ed amministrativa, nr. 32, 2014, 34, 38-39). Questa analisi, nel mettere in evidenza che la complicazione dell'ordinamento giuridico costituisce un frequente esito paradossale della semplificazione, ne fa anche emergere il carattere insostenibile in tempo di crisi. Viene poi evidenziato quanto sottolineato in dottrina e al centro del dibattito politico: una normativa inadeguata, sovrabbondante, poco comprensibile è terreno fertile per la diffusione della corruzione.

pubblica amministrazione, secondo il quale la PA è tenuta ad assicurare la visibilità, la conoscibilità e la comprensibilità della propria azione e dei propri assetti strutturali con i quali opera nel perseguire la cura in concreto dell'interesse pubblico. Principio fondamentale, questo, per l'attuazione del principio democratico nella PA, poiché coessenziale alla configurazione della democrazia come "regime del potere visibile"[28].

Il concetto di trasparenza si arricchisce di ulteriori contenuti e significati con il D.lgs. 27 ottobre 2009, n. 150 (*Ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*), che, all'art. 11, definisce la trasparenza come "accessibilità totale", da garantire essenzialmente attraverso la pubblicazione sui siti istituzionali di tutte le informazioni riguardanti ogni aspetto dell'organizzazione: "La trasparenza è intesa come accessibilità totale, anche attraverso lo strumento della pubblicazione sui siti istituzionali delle amministrazioni pubbliche, delle informazioni concernenti ogni aspetto dell'organizzazione, degli indicatori relativi agli andamenti gestionali e all'utilizzo delle risorse per il perseguimento delle funzioni istituzionali, dei risultati dell'attività di misurazione e valutazione svolta dagli organi competenti, allo scopo di favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità". Essa costituisce livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche ai sensi dell'art. 117, secondo comma, lettera m), della Costituzione[29].

Si costituisce in questo modo, in capo a ciascun cittadino, una posizione giuridica qualificata ad ottenere le informazioni pubbliche, che è chiaramente diretta a favorire quel controllo generalizzato sull'operato delle amministrazioni pubbliche, espressamente escluso dalla legge 241/1990 (art. 24, c.3). La trasparenza introdotta dal D.lgs. 150/2009 mira da un lato a garantire l'efficienza della pubblica amministrazione, tramite la trasparenza sulle performance dell'amministrazione e dei servizi pubblici, e, dall'altro, è finalizzata a prevenire la corruzione, mediante la trasparenza dei procedimenti e degli assetti organizzativi.

Ciò significa anche che i dati pubblicati "sono accessibili da parte di chiunque, che l'accessibilità non può essere limitata da aspetti tecnologici (*digital divide*), che l'accessibilità deve essere garantita come qualità delle informazioni secondo i principi di utilità, obiettività, integrità (nel senso di completezza) come individuati anche dal codice dell'amministrazione digitale: qualità dei dati in sé (esattezza, disponibilità, accessibilità e riservatezza); qualità dell'informazione aggregata (accessibilità,

[28] N. Bobbio, *La democrazia e il potere invisibile*, in *Rivista italiana di scienza politica*, vol. 10, 2, 1980, 181 ss.

[29] "La trasparenza totale persegue finalità nettamente diverse dall'accesso e connota un diverso modo di essere delle pubbliche amministrazioni che non può non spiegare effetti sugli assetti organizzativi specifici e sulle singole vicende dell'azione amministrativa. L'accessibilità totale è vista, in primo luogo, in funzione di servizio agli utenti e, ancora, sul versante della collettività, in funzione di controllo sociale diffuso sull'operato delle amministrazioni. A ben vedere, la trasparenza è posta in stretta correlazione con gli ambiti maggiormente significativi dell'attuale processo di riforma delle amministrazioni e, in un certo senso, può dirsi che la trasparenza costituisce il collante tra versante interno (organizzazione) e versante esterno (servizi al cittadino) della riforma. Sul piano macro, la trasparenza, come disciplinata dal legislatore del 2009, può dirsi finalizzata: a) all'efficienza, e quindi abbiamo le disposizioni sulla trasparenza della performance; b) alla prevenzione della corruzione e in generale di fenomeni di maladministration, cui si riporta in particolare la metodologia cd. della mappatura dei rischi nei procedimenti e negli assetti organizzativi; c) al miglioramento dei servizi pubblici, cui sono serventi sia la disciplina della performance organizzativa sia l'adozione di standard qualitativi e quantitativi nella logica del "miglioramento continuo" delle prestazioni; d) alla responsabilizzazione delle pubbliche amministrazioni, che ispira i sistemi di misurazione e valutazione. Se la trasparenza, nel contesto specifico della riforma complessiva delle amministrazioni delineata dal D.lgs. n. 150, ha queste finalità, ne discendono subito alcuni corollari che potremmo definire di sistema. Se è vero che. in presenza di una idonea base normativa, occorre tendenzialmente pubblicare tutto, è importante evitare quelle che sono state definite forme di opacità per confusione, in cui la massa di dati resi pubblici, in particolare sugli assetti organizzativi, rende impossibile l'identificazione dei dati rilevanti cioè dei dati che veramente interessano i cittadini come tali e come utenti dei servizi. L'identificazione dei dati rilevanti avviene essenzialmente attraverso i momenti di ascolto con i cittadini e le loro rappresentanze: questi momenti esprimono una "domanda di trasparenza" che va al di là della stessa "offerta di trasparenza" imposta dalla legge, perché seleziona tra i dati potenzialmente pubblici quelli di reale interesse e impone alle amministrazioni realmente aperte di concentrarsi su quelle informazioni che riguardano direttamente l'erogazione dei servizi anche al fine di assumere, nel momento della definizione degli obiettivi soprattutto di outcome. scelte coerenti con i bisogni della collettività" (F. Patroni Griffi, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *www.federalismi.it*, 2013).

elevata usabilità, interoperabilità, completezza delle informazioni, chiarezza di linguaggio, reperibilità, affidabilità, affidabilità, semplicità di consultazione, qualità, omogeneità, conformità ai documenti originali"[30].

Il D.lgs. 150/2009 prevede anche di dare pubblicità a ogni aspetto organizzativo. Nella nozione di organizzazione rientrerebbero sia l'elemento oggettivo (le funzioni di attività predeterminate in vista della cura di finalità di interesse generale, funzioni scopo), le competenze, i caratteri degli organi, le discipline sul funzionamento degli organi, le tipologie dei procedimenti, sia l'elemento soggettivo (il titolare dell'organo, il responsabile del procedimento, il personale addetto, le informazioni personali rilevanti).

Nonostante la piena operatività del RGPD e le conseguenti modifiche apportate dal legislatore al Codice in materia di protezione dei dati personali, la disciplina dell'accesso ai documenti amministrativi, disciplinato dalla legge 7 agosto 1990, n. 241[31], è rimasto inalterato. All'art. 59 del Codice è sempre presente una clausola di salvezza in base alla quale restano ferme le disposizioni della legge n. 241/1990, dei successivi regolamenti di attuazione e delle altre leggi regolanti il diritto di accesso: "Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso". Sempre l'art. 59 del Codice precisa che i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal d.lgs. 14 marzo 2013, n. 33.

L'articolo successivo evidenzia che "Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale".

La legge n. 241 del 1990, come già rilevato, per prima ha riconosciuto il diritto di accesso agli atti della pubblica amministrazione. Occorre che tale diritto sia assicurato a chiunque vi abbia interesse, il legislatore non ha tuttavia contemplato un'azione popolare volta a consentire un controllo generalizzato sull'attività amministrativa. E infatti, la norma correla espressamente l'interesse all'ostensione alla tutela di situazioni giuridicamente rilevanti: l'art. 22, comma 1, lett. b) della legge n. 241 del 1990, infatti, definisce "interessati" all'accesso non già tutti i soggetti indiscriminatamente, ma esclusivamente i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso[32].

La legge ha avuto il merito di aprire le porte ai cittadini nei confronti di un sistema che, fino a quel momento, aveva visto affermarsi la superiorità della pubblica amministrazione sugli stessi e che si esplicava nell'assoluta riservatezza dei procedimenti amministrativi. Questo sistema è stato scardinato dalla citata legge, voluta non solo per avvicinare il modus operandi della pubblica amministrazione a quello delle altre legislazioni europee, ma anche per renderlo più affine al dettato costituzionale che, all'art. 97, individua nel buon andamento e nell'imparzialità i principi cardine cui la pubblica amministrazione italiana dovrebbe uniformarsi.

Anche se questa legge è stata fondamentale per avviare quello che è stato in un certo senso un cambiamento dei paradigmi del rapporto tra pubblica amministrazione e cittadini, occorre, però, rimarcare che si parla pur sempre di accesso documentale, ciò significa che non è un accesso consentito a tutti e in qualsiasi momento, ma solo a determinate

[30] F. Merloni e B. Ponti, *Gli strumenti della trasparenza*, in F. Merloni, L. Vandelli (a cura di), *La corruzione amministrativa*, Firenze, Passigli Editori, 2010, 410-411.

[31] In questa sede, appare pleonastico soffermarsi sull'annosa questione del rapporto tra accesso ai documenti amministrativi e tutela della riservatezza, tema rispetto al quale, da tempo, sono stati spesi fiumi d'inchiostro.

[32] Cons. Stato, sez. V, 21 agosto 2017, n. 4043.

condizioni: ovvero ci deve essere un interesse diretto, concreto e attuale che faccia riferimento ad una situazione giuridica tutelata dall'ordinamento e collegata ai documenti per i quali si richiede l'accesso, come recita lo stesso art. 22, comma 1. Proseguendo nella sommaria analisi della legge n. 241/90, non si può non segnalare quello che è il vero fulcro dell'accesso agli atti documentale, cioè la possibilità di prendere visione degli stessi. Difatti, grazie all'art. 22, comma 2, è possibile prendere visione degli atti ed estrarne copia, cosa impensabile fino a qualche anno fa e segno inequivocabile che i rapporti di forza tra cittadini e pubblica amministrazione stavano inevitabilmente cambiando.

Se da un lato ci sono aspetti positivi, dall'altro bisogna sottolineare che non è una legge libera tutti: infatti, sono ancora presenti segni tangibili di quella diffidenza che ha caratterizzato, e che caratterizza tutt'ora, il rapporto tra pubblica amministrazione e cittadini.

L'art. 24, comma 1, regola proprio i casi di esclusione all'accesso, come: i documenti coperti dal segreto di Stato, i procedimenti tributari, gli atti normativi ed amministrativi generali; casi che per nostra sfortuna non sono pochi. Tra l'altro il dettato dell'art. 24, comma 6, della citata legge, prevede come il governo possa ulteriormente rafforzare i limiti all'accesso nel caso in cui i documenti amministrativi dovessero riguardare argomenti sensibili quali: la sicurezza nazionale e la difesa nazionale; l'eventuale danno ai processi di formazione e attuazione della politica monetaria; il potenziale danno alla vita privata di persone fisiche, persone giuridiche, enti. L'ultimo comma dell'art. 24 sembra quasi contemplare un piccolo risarcimento: infatti, il legislatore ha concesso l'accesso ai documenti amministrativi in caso di difesa dei propri interessi giuridici e, se dovessero esserci in ballo dati sensibili e giudiziari, il suddetto accesso è consentito nei limiti strettamente previsti.

7. *Accesso civico "semplice", accesso "generalizzato" e protezione dei dati personali*

La democrazia è idealmente il governo del potere visibile, cioè del governo i cui atti si svolgono in pubblico, sotto il controllo della pubblica opinione. Le istituzioni di un paese libero non possono durare a lungo, scrisse nel secolo scorso Maurice Joly nel suo *Dialogo agli inferi* tra Machiavelli e Montesquieu[33], se non agiscono *au grand jour* (alla luce del sole).

Tema ricorrente della dottrina dello Stato assoluto è quello degli *arcana imperii*. Uno dei più noti scrittori machiavellici, Gabriel Naudé, ha sentenziato: "Non vi è nessun principe così debole e privo di senno da essere scriteriato al punto da rimettere al giudizio del pubblico ciò che a mala pena rimane segreto se confidato all'orecchio di un ministro o di un favorito"[34]. Il potere autocratico si sottrae al controllo del pubblico in due modi: occultandosi, cioè prendendo le proprie decisioni nel «consiglio segreto», e occultando, cioè attraverso l'esercizio della simulazione o della menzogna considerata come lecito strumento di governo.

"Il segreto sta nel nucleo più interno del potere". Norberto Bobbio usava spesso citare questo passo di *Massa e potere* di Elias Canetti per sottolineare come, per secoli, il segreto sia stato considerato da uomini di Stato e teorici della politica uno strumento essenziale all'esercizio del potere.

A questa teoria (e pratica) degli *arcana imperii* i sostenitori della democrazia hanno contrapposto l'idea di un potere "in pubblico", in cui, kantianamente, si faccia un «uso pubblico della ragione», cioè si discuta in modo informato e competente sui problemi della comunità per giungere a decisioni consapevoli e condivise e per esercitare un efficace controllo sui governanti.

Peraltro un simile obiettivo non è stato raggiunto a giudizio di Bobbio, che nel saggio *II futuro della democrazia* indica nell'eliminazione del potere invisibile una delle sei grandi promesse non mantenute dall'ideologia democratica[35].

Colin Crouch[36], sociologo e politologo britannico, è noto per aver coniato il termine post-democrazia. Ossia una condizione in cui la pratica democratica perde di consistenza, garantendo solo libertà svuotate di contenuto. La politica smarrisce il contatto con i cittadini.

"Chi guardi il generale processo di riforme, che hanno interessato l'amministrazione

[33] M. Joly, *Dialogo agli inferi tra Machiavelli e Montesquieu*, Genova, ECIG, 1995.
[34] In N. Bobbio, *La democrazia e il potere invisibile*, 191.
[35] N. Bobbio, *Il futuro della democrazia*, Torino, Einaudi, 1984.
[36] C. Crouch, *Postdemocrazia*, Roma-Bari, Laterza, 2000.

pubblica quanto meno a partire dagli anni '90, noterà l'emersione progressiva nel mondo del diritto di quello che potremmo definire un valore dell'ordinamento che a poco a poco acquisterà contorni sempre più netti e pervasivi della tradizionale sfera di "riservatezza" delle pubbliche amministrazioni, nell'ottica di un dialogo tra amministrazione e amministrato che favorisca la trasformazione del suddito in cittadino (l'immagine è mutuata dal prezioso saggio di W. Ulmann, su *Individuo e società nel Medioevo*, edito da Laterza nel 1983).

Da allora la trasparenza assumerà sempre più le sembianze di un valore immanente all'ordinamento, un valore di tipo finalistico, perché espressione di democrazia politica e amministrativa; ma anche un valore strumentale, e quindi formale, attraverso il quale assicurare la conoscenza dei processi decisionali, delle organizzazioni, dei procedimenti, delle prestazioni e dei servizi al pubblico.

Volendo schematizzare il percorso normativo registratosi, è consentito tener conto di tre tappe evolutive:

a. quella inaugurata con l'approvazione della legge n. 241 del 1990;

b. quella che ha inizio con l'affermazione, ad opera del D.lgs. n. 150 del 2009, del principio di accessibilità totale;

c. quella, infine, che prende avvio con il D.lgs.14 marzo 2013, n. 33, recante "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione" e adottata in attuazione della delega contenuta nella legge 6 novembre 2012, n. 190 (legge c.d. anticorruzione)"[37], che si arricchisce di un più articolato e complesso strumento di accesso introdotto con il D.lgs. n. 97/2016: l'accesso c.d. generalizzato.

Con la legge n. 190/2012 la trasparenza diventa uno dei principali strumenti di contrasto e prevenzione della corruzione, alla luce del D.lgs. n. 33/2013, che mira a rendere accessibili non solo le azioni cristalizzate negli atti, ma anche le condizioni personali del soggetto che le pone in essere.

Dopo l'introduzione dell'informatica nell'attività amministrativa e il ripensamento sul ruolo del settore pubblico, l'originario concetto di trasparenza (circoscritto al diritto di accesso agli atti e ai documenti per coloro che avessero specifico e concreto interesse) ha iniziato a dimostrarsi insufficiente. La digitalizzazione della PA conferisce nuovi significati al concetto di trasparenza (si pensi agli artt. 2, 12 e 50 del CAD).

Il tema dell'amministrazione aperta, e dei suoi principi, si lega strettamente ad una riflessione sull'amministrazione elettronica, specie se letta da un'angolazione attenta ai diritti del cittadino. Il Codice dell'amministrazione digitale, che disciplinando la presenza nel web delle pubbliche amministrazioni ha posto le premesse per la successiva maturazione di un nuovo modello di trasparenza attraverso la diffusione di informazioni tramite siti istituzionali, sul quale ultimo il legislatore ha puntato con forza a partire dalle riforme del 2009 per arrivare al decreto legislativo n. 33 del 2013, riformato nel corso del 2016.

Di questo stretto collegamento tiene conto il legislatore: così, recentemente, di amministrazione "digitale ed aperta" si occupa la legge c.d. Madia n. 124/2015, art. 1, lett. n), che collega i due concetti quasi come endiadi: la riorganizzazione delle amministrazioni sul versante dell'informatizzazione è finalizzata "alla realizzazione di un'amministrazione digitale e aperta", oltre che di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

Parlare di "openness" significa, in questo scenario, segnare la "mutazione genetica" che ha interessato la trasparenza, come principio e negli strumenti chiamata a realizzarlo: nel corso degli ultimi anni si è assistito ad un forte cambiamento di prospettiva, con la perdita di centralità del diritto di accesso in favore della trasparenza assicurata dalla pubblicazione nei siti istituzionali e quindi della disponibilità (on line) di informazioni: né il percorso di evoluzione sembra arrestato, posto che il legislatore ha nel 2016 introdotto una disciplina ispirata al modello del Freedom of Information Act. Uno sviluppo che ci consegna un quadro composito di strumenti della trasparenza, sempre meno collegabile a meccanismi di garanzia del singolo interessato, ma sempre più declinata in termini di autonomo diritto alla conoscibilità.

Tutto deve essere accessibile, tutto deve essere visibile. La trasparenza viene istituzionalizzata, questa si condensa nell'imperativo di svelare ciò che è nascosto e non stupisce il fatto che sia assurta a

[37] F. Patroni Griffi, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *Federalismi.it*, 2013.

condizione della democrazia. Nel mondo anglosassone il cardine della democrazia è l'*accountability*, "il dovere di rendere conto". Ma se il controllo diffuso, pubblico, è il fermento del dissenso, equiparare "pubblico" a "democratico", in una visione manichea e ingenua, può portare a storture inquietanti. "Muoversi nel diafano palazzo di cristallo non è poi così semplice. Si rischia di urtare contro le pareti invisibili, la trasparenza inganna. Il sogno diventa un incubo". Anche coloro che credono fideisticamente nell'altissimo cielo della trasparenza, come ricorda Vladimir Nabokov in "Cose trasparenti"[38] , prima o poi saranno costretti ad ammettere che questa non è che un abbaglio e vano sarebbe rincorrere l'ideale della trasparenza assoluta[39] .

Anche la trasparenza e la luce devono essere sottoposte alla nostra capacità critica, come scriveva Hegel, "nell'assoluta chiarezza non ci si vede né più né meno che nell'assoluta oscurità". Questa affermazione, oggi, si rivela in tutta la sua attualità. "Oggi, infatti, viviamo in un mondo ad altissima visibilità in cui però molto resta celato agli occhi della coscienza. La grande quantità di immagini e di dati a nostra disposizione ci permettono di vedere posti remoti e di accedere a informazioni che fino a tempi recenti erano privilegio di pochi. Ciò non implica, però, necessariamente un miglioramento della nostra capacità di analisi e conoscenza. Ci sentiamo spesso accecati; vediamo ma non sempre capiamo. Ci illudiamo che la rapidità della comunicazione ci mostri immediatamente il reale, ma dimentichiamo che vecchi e nuovi media continuano a selezionare, scegliere, mediare. Inoltre, le nostre vite sono continuamente sotto i riflettori, e come attori su un palcoscenico siamo in mostra senza vedere il pubblico, abbagliati da troppa luce. La trasparenza, certo, è necessaria al governo democratico, da sempre legittimato proprio dalla possibilità per i cittadini di vedere all'opera i propri rappresentanti sul palcoscenico della politica… Perché rinnovare la società democratica vuol dire riaprire canali di dialogo fra rappresentanti e rappresentati ma soprattutto fra cittadini; rinnovare lo scambio fra persone differenti e mondi tra loro lontani. Tra cultura umanistica e scientifica, tra centro e periferia, tra alto e basso, per superare la logica di contrapposizione che riduce la politica ad un campo di battaglia in cui si affrontano nemici. Per quanto faticoso tutto ciò possa apparire, questo è il terreno su cui si gioca la sopravvivenza della democrazia" [40].

Come già rilevato, con il d.lgs.14 marzo 2013 n. 33, intitolato "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" il legislatore – in attuazione della delega contenuta nella legge 6 novembre 2012, n. 190, recante: "Disposizioni per la prevenzione e la repressione della corruzione e dell´illegalità nella pubblica amministrazione" (art. 1, commi 35 e 36) – ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzione di dati, informazioni, atti e documenti sui siti web istituzionali dei soggetti obbligati. A tal fine, nel capo I dedicato ai "principi generali", la trasparenza è definita come "come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche" (art. 1, comma 1).

Nel medesimo capo I è precisato che "oggetto del decreto" è quello di disciplinare "la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione". Si sottolinea, in proposito, che lo stesso legislatore, ai soli fini del campo di applicazione del decreto, definisce la pubblicazione come la diffusione "in conformità alle specifiche e alle regole tecniche di cui all'allegato A, nei siti

[38] V. Nabokov, *Cose trasparenti*, Milano, Adelphi, 1995.

[39] G. Greenwald, *No place to hide. Sotto controllo, Edward Snowden e la sorveglianza di massa*, Milano, Rizzoli, 2014.

[40] G. Zagrebelsky, *Luci, oscurità e nuovi poteri nella società della vetrina*, in *La Repubblica*, 20 marzo 2019, 33.

istituzionali delle pubbliche amministrazioni dei documenti, delle informazioni e dei dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, cui corrisponde il diritto di chiunque di accedere ai siti direttamente ed immediatamente, senza autenticazione ed identificazione. (art. 2, comma 2). Da ciò si evince che tutte le volte in cui nel d.lgs. n. 33/2013 è utilizzata la locuzione "pubblicazione obbligatoria ai sensi della normativa vigente", il riferimento è limitato agli "obblighi di pubblicazione concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" contenuti oltre che nel d.lgs. n. 33/2013 anche in altre disposizioni normative aventi analoga finalità di trasparenza, con esclusione degli obblighi di pubblicazione aventi finalità diverse.

La tipologia dei predetti obblighi di pubblicazione per finalità di trasparenza concernenti l´organizzazione e l´attività delle pubbliche amministrazioni è schematicamente riassunta nell´allegato A al d.lgs. n. 33/2013 che individua la "struttura delle informazioni sui siti istituzionali"(1) e che precisa come la sezione dei siti istituzionali denominata "Amministrazione trasparente" deve essere organizzata in sotto-sezioni all´interno delle quali devono essere inseriti i documenti, le informazioni e i dati previsti dal decreto.

Devono, pertanto, ritenersi estranei all'oggetto del d.lgs. n. 33/2013 tutti gli obblighi di pubblicazione previsti da altre disposizioni per finalità diverse da quelle di trasparenza, quali gli obblighi di pubblicazione a fini di pubblicità legale, pubblicità integrativa dell'efficacia, pubblicità dichiarativa o notizia. Si pensi, ad esempio – tra i diversi casi indicati – alle pubblicazioni matrimoniali, la cui affissione alla porta della casa comunale (e oggi sui siti web istituzionali dei comuni) è prevista per otto giorni (cfr. art. 55 del d.P.R. n. 396 del 3/11/2000). La pubblicazione dei dati personali dei nubendi assolve a una funzione che evidentemente esula dalle finalità di trasparenza previste dal d.lgs. n. 33/2013 e che è pienamente assolta con la semplice pubblicazione per la durata temporale prevista. Infatti, sarebbe irragionevole applicare a essi il regime di conoscibilità previsto dalla normativa sulla trasparenza (limiti temporali di permanenza sul web, indicizzazione, accesso civico, riutilizzo etc.). Pertanto, tutte le ipotesi di pubblicità non riconducibili a finalità di trasparenza, qualora comportino una diffusione di dati personali, sono escluse dall'oggetto del d.lgs. n. 33/2013 e dall´ambito di applicazione delle relative previsioni fra cui, in particolare, quelle relative all´accesso civico (art. 5), all´indicizzazione (art. 4 e 9), al riutilizzo (art. 7), alla durata dell´obbligo di pubblicazione (art. 8) e alla trasposizione dei dati in archivio (art. 9).

Il Garante per la protezione dei dati personali, al fine di garantire i diritti e le libertà fondamentali (con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali) e contribuire a declinare in modo equilibrato il rapporto tra esigenze di trasparenza dell'amministrazione e garanzie poste a tutela dei diritti, il 15 maggio 2014 ha, a proposito, adottato delle linee guida, alla ricerca di un corretto bilanciamento, di un ragionevole equilibrio, tra attuazione del principio di trasparenza e tutela dei dati personali.

Infatti, i principi e la disciplina di protezione dei dati personali (come peraltro previsto anche dagli artt. 1, comma 2, e 4 del d.lgs. n. 33/2013; v. altresì art. 8, comma 3) devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.

La "diffusione" di dati personali – ossia "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione" (art. 4, comma 1, lett. m) – da parte dei "soggetti pubblici" è ammessa unicamente quando la stessa è prevista da una specifica norma di legge o di regolamento. Pertanto, in relazione all'operazione di diffusione, occorre che le pubbliche amministrazioni, prima di mettere a disposizione sui propri siti web istituzionali informazioni, atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, verifichino che la normativa in materia di trasparenza preveda tale obbligo. Qualora l'amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell´atto o del documento nel proprio sito web istituzionale è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l´oscuramento di determinate informazioni. I soggetti pubblici, infatti, in conformità ai principi di protezione

dei dati, sono tenuti a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l´interessato solo in caso di necessità (cd. "principio di minimizzazione o necessità"). Pertanto, anche in presenza degli obblighi di pubblicazione di atti o documenti contenuti nel d.lgs. n. 33/2013, i soggetti chiamati a darvi attuazione non possono comunque rendere intelligibili i dati personali non pertinenti o, se particolari o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione. È, quindi, consentita la diffusione online dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti. È, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" e "la vita sessuale" (art. 4, comma 6, del d.lgs. n. 33/2013).

In particolare, con riferimento ai dati idonei a rivelare lo stato di salute degli interessati, è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Il procedimento di selezione dei dati personali che possono essere resi conoscibili online deve essere, inoltre, particolarmente accurato nei casi in cui tali informazioni siano idonee a rivelare l´origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l´adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale ("dati particolari"), oppure nel caso di dati idonei a rivelare provvedimenti di cui all´articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, nonché la qualità di imputato o di indagato ("dati giudiziari").

I dati particolari e giudiziari, infatti, sono protetti da un quadro di garanzie particolarmente stringente che prevede la possibilità per i soggetti pubblici di diffondere tali informazioni solo nel caso in cui sia previsto da una espressa disposizione di legge e di trattarle solo nel caso in cui siano in concreto "indispensabili" per il perseguimento di una finalità di rilevante interesse pubblico come quella di trasparenza; ossia quando la stessa non può essere conseguita, caso per caso, mediante l´utilizzo di dati anonimi o di dati personali di natura diversa. Pertanto, come rappresentato dal Garante per la protezione dei dati personali nel parere del 7 febbraio 2013 (doc. web 2243168), gli enti pubblici sono tenuti a porre in essere la massima attenzione nella selezione dei dati personali da utilizzare, sin dalla fase di redazione degli atti e documenti soggetti a pubblicazione, in particolare quando vengano in considerazione dati sensibili. In proposito, può risultare utile non riportare queste informazioni nel testo dei provvedimenti pubblicati online (ad esempio nell´oggetto, nel contenuto, etc.), menzionandole solo negli atti a disposizione degli uffici (richiamati quale presupposto del provvedimento e consultabili solo da interessati e controinteressati), oppure indicare delicate situazioni di disagio personale solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici (cfr. par. 2 del parere citato).

Una volta effettuata la preventiva valutazione circa i presupposti e l´indispensabilità della pubblicazione di dati sensibili e giudiziari, devono essere adottate idonee misure e accorgimenti tecnici volti ad evitare "la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo" (cfr. art. 7, del d.lgs.n. 33/2013, nonché le precisazioni fornite dal Garante nel parere sopra richiamato).

L´art. 6 del d.lgs. n. 33/2013 prevede che "Le pubbliche amministrazioni garantiscono la qualità delle informazioni riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti dalla legge, assicurandone l´integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l´omogeneità, la facile accessibilità, nonché la conformità ai

documenti originali in possesso dell´amministrazione, l´indicazione della loro provenienza e la riutilizzabilità secondo quanto previsto dall´art. 7"[41] e che "l´esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l´omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti".

Tale previsione deve essere interpretata anche alla luce dei principi in materia di protezione dei dati personali, per cui le pubbliche amministrazioni sono, altresì, tenute a mettere a disposizione soltanto dati personali esatti, aggiornati e contestualizzati. Le pubbliche amministrazioni titolari del trattamento devono, quindi, non solo controllare l´attualità delle informazioni pubblicate, ma anche modificarle o aggiornarle opportunamente, quando sia necessario all´esito di tale controllo e ogni volta che l´interessato ne richieda l´aggiornamento, la rettificazione oppure, quando vi abbia interesse, l´integrazione. Ormai siamo entrati in una seconda fase. Occorre passare dall'elemento puramente quantitativo a quello qualitativo. L'accumulo di informazioni non produce di per sé verità e trasparenza e non genera di per sé nuova conoscenza. Più informazioni non eliminano la fondamentale opacità del tutto, anzi rischiano di accrescerla. L'iperinformazione spesso non getta alcuna luce nelle tenebre. Esiste, infatti, la c.d. opacità per confusione. È il tema del *civic engagement*: provare a coinvolgere i cittadini per risolvere problemi comuni. Nell'adempimento degli obblighi di pubblicazione deve essere garantita la qualità dei dati, assicurandone il costante e tempestivo aggiornamento, la "comprensibilità", la "completezza", "l'integrità" e "l'omogeneità", nonché la conformità agli originali in possesso del soggetto obbligato alla pubblicazione, l'indicazione della provenienza e deve essere eliminato ogni ostacolo e difficoltà all'accessibilità e alla consultazione. È espressamente previsto, inoltre, che l'esigenza di garantire la qualità dei dati non possa giustificare l'omissione o il ritardo nell'adempimento degli obblighi di pubblicazione.

La necessità di assicurare una qualità adeguata dei dati pubblicati è funzionale all'effettività del controllo diffuso della cittadinanza che le norme in esame mirano a garantire e la relativa disciplina si completa con i rimedi previsti a fronte dell'inerzia del soggetto pubblico, ma anche dall'ulteriore obbligo delle amministrazioni pubbliche di garantire la qualità delle informazioni pubblicate.

È dunque necessario garantire l'adeguata qualità delle informazioni mediante la semplicità nella accessibilità e nella consultazione dei dati, la comprensibilità delle informazioni e il loro diligente e tempestivo aggiornamento; standards che i nuovi strumenti tecnologici possono concorrere ad assicurare. La trasparenza vede infatti come necessario corollario la "comprensione" dei dati, superando le barriere che su un piano organizzativo limitano l'individuazione delle informazioni utili al controllo democratico.

La problematica della qualità delle informazioni è in grado di influire in modo significativo sulle modalità di azione e di relazione delle amministrazioni pubbliche, ma è anche una sfida difficilmente eludibile, se è vero che l'esigenza di disporre di informazioni caratterizzate da uno specifico regime di qualità attesa, è sempre più sentita a livello di organizzazioni complesse. In via generale, possiamo definire la qualità dei dati come "l'insieme delle caratteristiche di un'entità, idonee a soddisfare le esigenze esplicite ed implicite, e questa risulta centrale per garantire l'efficienza delle condotte degli operatori, per ridurre i costi ed aumentare la soddisfazione degli utenti clienti, per consentire la comunicazione tra strutture diverse, per permettere l'assunzione di decisioni corrette"[42].

L´art. 7 del d.lgs. n. 33/2013 prevede che "I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, resi disponibili anche a seguito dell´accesso civico di cui all´articolo 5, sono pubblicati in formato di tipo aperto ai sensi dell´articolo 68 del Codice dell'am-

[41] E. Carloni, *La qualità delle informazioni pubbliche. L'esperienza italiana nella prospettiva comparata*, in *Rivista trimestrale di diritto pubblico*., 2009, 155; F. Di Mascio, *Open data e trasparenza in Italia: quantità senza qualità*, in A. Natalini e G. Vesperini (a cura di), *Il Big Bang della trasparenza*, Napoli, Editoriale Scientifica, 2015, 275.

[42] E. Carloni, *La qualità delle informazioni pubbliche. L'esperienza italiana nella prospettiva comparata*, in *Riv. trim. dir. pub.*, 155. Sulla qualità delle informazioni pubbliche, cfr. anche F. Di Mascio, *Open data e trasparenza in Italia: quantità senza qualità*, 275.

ministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e sono riutilizzabili ai sensi del decreto legislativo 24 gennaio 2006, n. 36, del decreto legislativo 7 marzo 2005, n. 82, e del decreto legislativo 30 giugno 2003, n. 196, senza ulteriori restrizioni diverse dall´obbligo di citare la fonte e di rispettarne l´integrità". Detta disposizione persegue, peraltro, lo scopo di non obbligare gli utenti a dotarsi di programmi proprietari o a pagamento per la fruizione – e, quindi, per la visualizzazione – dei file contenenti i dati oggetto di pubblicazione obbligatoria. Infatti, il "formato di tipo aperto" è "un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi" (art. 68, comma 3, lett. a, del d.lgs.7 marzo 2005, n. 82, Codice dell'amministrazione digitale-CAD). Con riferimento ai dati personali, si rappresenta, quindi, che l´obbligo di pubblicazione in "formato di tipo aperto" non comporta che tali dati, pubblicati sui siti web istituzionali in ottemperanza agli obblighi di trasparenza, siano anche "dati di tipo aperto" nei termini definiti dal CAD. Appare opportuno, infatti, tenere distinto il concetto di "formato di tipo aperto" avente il significato sopra descritto, da quello di "dato di tipo aperto" che attiene, invece, più propriamente alla disponibilità unita alla riutilizzabilità del dato da parte di chiunque, anche per finalità commerciali e in formato disaggregato (art. 52, comma 2, e art. 68, comma 3, lett. b, del CAD).

Gli artt. 7 e 7-*bis* del d.lgs. n. 33/2013 stabiliscono che il riutilizzo dei dati personali pubblicati è soggetto alle condizioni e ai limiti previsti dalla disciplina sulla protezione dei dati personali e dalle specifiche disposizioni del d.lgs. 24 gennaio 2006 n. 36 di recepimento della direttiva 2003/98/CE sul riutilizzo dell'informazione del settore pubblico. Tale direttiva è stata oggetto di revisione (v. direttiva 2013/37/UE entrata in vigore dopo l'approvazione del decreto legislativo sulla trasparenza). Con la modifica della predetta direttiva, l'Unione europea conferma il principio, da ritenersi ormai consolidato in ambito europeo, in base al quale il riutilizzo di tali documenti non deve pregiudicare il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali fissato dalle disposizioni di diritto europeo e nazionale in materia. In particolare, le nuove disposizioni della direttiva introducono specifiche eccezioni al riutilizzo fondate sui principi di protezione dei dati, prevedendo che una serie di documenti del settore pubblico contenenti tale tipologia di informazioni siano sottratti al riuso anche qualora siano liberamente accessibili online. Ciò significa che il principio generale del libero riutilizzo di documenti contenenti dati pubblici, stabilito dalla disciplina nazionale ed europea, riguarda essenzialmente documenti che non contengono dati personali oppure riguarda dati personali opportunamente aggregati e resi anonimi. In altri termini, il semplice fatto che informazioni personali siano rese pubblicamente conoscibili online per finalità di trasparenza non comporta che le stesse siano liberamente riutilizzabili da chiunque e per qualsiasi scopo, bensì impone al soggetto chiamato a dare attuazione agli obblighi di pubblicazione sul proprio sito web istituzionale di determinare – qualora intenda rendere i dati riutilizzabili – se, per quali finalità e secondo quali limiti e condizioni eventuali utilizzi ulteriori dei dati personali resi pubblici possano ritenersi leciti alla luce del "principio di finalità" e degli altri principi di matrice europea in materia di protezione dei dati personali.

Al fine di evitare di perdere il controllo sui dati personali pubblicati online in attuazione degli obblighi di trasparenza e di ridurre i rischi di loro usi indebiti, è quindi in primo luogo opportuno che le pubbliche amministrazioni e gli altri soggetti chiamati a dare attuazione agli obblighi di pubblicazione di cui al d.lgs. n. 33/2013 inseriscano nella sezione denominata "Amministrazione trasparente" dei propri siti web istituzionali un Alert generale con cui si informi il pubblico che i dati personali pubblicati sono "riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva comunitaria 2003/98/CE e d.lgs.36/2006 di recepimento della stessa), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali".

A tal proposito, giova ricordare che una volta effettuata la pubblicazione online dei dati personali prevista dalla normativa in materia di trasparenza, il soggetto pubblico può rendere riutilizzabili tali dati o accogliere eventuali richieste di riutilizzo degli stessi da parte di terzi, solamente dopo avere effettuato una rigorosa valutazione d´impatto in materia

di protezione dei dati, al fine di ridurre il rischio di perdere il controllo sulle medesime informazioni o di dover far fronte a richieste di risarcimento del danno da parte degli interessati.

L'art. 7-*bis* del d.lgs. n. 33/2013 prevede che: "Gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari, di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali. La pubblicazione nei siti istituzionali, in attuazione del presente decreto, di dati relativi a titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali. Le pubbliche amministrazioni possono disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non hanno l'obbligo di pubblicare ai sensi del presente decreto o sulla base di specifica previsione di legge o regolamento, nel rispetto dei limiti indicati dall'articolo 5-*bis*, procedendo alla indicazione in forma anonima dei dati personali eventualmente presenti. Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione. Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione sono rese accessibili dall'amministrazione di appartenenza. Non sono invece ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione dal lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il predetto dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di cui all'articolo 4, comma 1, lettera d), del decreto legislativo 30 giugno 2003, n. 196. Restano fermi i limiti all'accesso e alla diffusione delle informazioni di cui all'articolo 24, commi 1 e 6, della legge 7 agosto 1990, n. 241, e successive modifiche, di tutti i dati di cui all'articolo 9 del decreto legislativo 6 settembre 1989, n. 322, di quelli previsti dalla normativa europea in materia di tutela del segreto statistico e di quelli che siano espressamente qualificati come riservati dalla normativa nazionale ed europea in materia statistica, nonché quelli relativi alla diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale".

Un'altra questione di non secondaria importanza riguarda la decorrenza e la durata dell'obbligo di pubblicazione, al riguardo l'art. 8 del d.lgs. 33/2013 dispone che: "I documenti contenenti atti oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione. I documenti contenenti altre informazioni e dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati e mantenuti aggiornati ai sensi delle disposizioni del presente decreto. I dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali e quanto previsto dagli articoli 14, comma 2, e 15, comma 4. Decorsi detti termini, i relativi dati e documenti sono accessibili ai sensi dell'articolo 5. L'Autorità nazionale anticorruzione, sulla base di una valutazione del rischio corruttivo, delle esigenze di semplificazione e delle richieste di accesso, determina, anche su proposta del Garante per la protezione dei dati personali, i casi in cui la durata della pubblicazione del dato e del documento può essere inferiore a 5 anni.

Sono, però, previsti espressamente alcune deroghe alla durata temporale quinquennale: a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della

produzione degli effetti; b) per alcuni dati e informazioni riguardanti i "titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale" (art. 14, comma 2) e i "titolari di incarichi dirigenziali e di collaborazione o consulenza" che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell´incarico (art. 15, comma 4); c) nel caso in cui siano previsti "diversi termini" dalla normativa in materia di trattamento dei dati personali. In merito, si evidenzia come il Codice – che non prevede termini espliciti (come già evidenziato dal Garante nel parere del 7 febbraio 2013), – richiede espressamente che i dati personali devono essere "conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati" e che l´interessato ha diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati. Tali principi erano già declinati nella direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali le quali, in quanto tali, non possono essere derogate dalla disciplina nazionale in virtù del primato del diritto europeo. Da tale principio, inoltre, discende l´obbligo di interpretare il diritto nazionale in maniera conforme al diritto europeo e, nello specifico, alle disposizioni direttamente applicabili che impongono il rispetto dei principi di pertinenza, necessità e proporzionalità, in base alle quali la pubblicazione di dati personali è consentita soltanto quando è al contempo necessaria e appropriata rispetto all´obiettivo perseguito e, in particolare, quando l´obiettivo perseguito non può essere realizzato in modo ugualmente efficace con modalità meno pregiudizievoli per la riservatezza degli interessati".[43] Per tale motivo, il Garante ritiene che laddove atti, documenti e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, anche prima del termine di cinque anni, quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti stessi hanno prodotto i loro effetti.

Secondo l´art. 9 del d.lgs. n. 33/2013 le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente". "Si evidenzia che l´obbligo di indicizzazione nei motori generalisti durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati ai sensi delle disposizioni in materia di trasparenza da collocarsi nella "sezione "Amministrazione trasparente", con esclusione di altri dati che si ha l´obbligo di pubblicare per altre finalità di pubblicità diverse da quelle di "trasparenza"… Sono, fra l´altro, espressamente sottratti all´indicizzazione i dati sensibili e i dati giudiziari (art. 4, comma 1, d.lgs. n. 33/2013). Pertanto, i soggetti destinatari degli obblighi di pubblicazione previsti dal d.lgs. n. 33/2013 devono provvedere alla relativa deindicizzazione tramite – ad esempio – l´inserimento di *metatag noindex* e *noarchive* nelle intestazioni delle pagine web o alla codifica di regole di esclusione all´interno di uno specifico file di testo (il file robots.txt) posto sul server che ospita il sito web configurato in accordo al *Robot Exclusion Protocol* (avendo presente, comunque, come tali accorgimenti non sono immediatamente efficaci rispetto a contenuti già indicizzati da parte dei motori di ricerca Internet, la cui rimozione potrà avvenire secondo le modalità da ciascuno di questi previste)"[44].

La disciplina in materia di trasparenza prevede di rendere visibile al pubblico, rispetto a taluni soggetti, informazioni personali concernenti il percorso di studi e le esperienze professionali rilevanti, nella forma del curriculum redatto in conformità al vigente modello europeo (art. 10, comma 8, lett. d, d.lgs. n. 33/2013). Le ipotesi contemplate riguardano, ad esempio, i curricula professionali dei titolari di incarichi di indirizzo politico (art. 14), dei titolari di incarichi amministrativi di vertice, dirigenziali

[43] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, 15 maggio 2014, doc. web 3134436.

[44] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, 15 maggio 2014, doc. web 3134436.

e di collaborazione o consulenza (art. 15, comma 1, lett. b), nonché delle posizioni dirigenziali attribuite a persone – anche esterne alle pubbliche amministrazioni – individuate discrezionalmente dall´organo di indirizzo politico senza procedure pubbliche di selezione, di cui all´articolo 1, commi 39 e 40, della legge 6 novembre 2012, n. 190 (art. 15, comma 5), dei componenti degli organismi indipendenti di valutazione (art. 10, comma 8, lett. c), nonché dei dirigenti in ambito sanitario come individuati dall´art. 41, commi 2 e 3.

Il riferimento del legislatore all´obbligo di pubblicazione del curriculum non può però comportare la diffusione di tutti i contenuti astrattamente previsti dal modello europeo (rispondendo taluni di essi alle diverse esigenze di favorire l´incontro tra domanda e offerta di lavoro in vista della valutazione di candidati oppure, nel corso del rapporto di lavoro, per l´assegnazione dell´interessato a nuovi incarichi o per selezioni concernenti la progressione di carriera), ma solo di quelli pertinenti rispetto alle finalità di trasparenza perseguite. Prima di pubblicare sul sito istituzionale i curricula, il titolare del trattamento dovrà pertanto operare un'attenta selezione dei dati in essi contenuti. Sarebbe auspicabile che le amministrazioni predisponessero modelli omogenei, impartendo opportune istruzioni agli interessati (che, in concreto, possono essere chiamati a predisporre il proprio curriculum in vista della sua pubblicazione per le menzionate finalità di trasparenza). In tale prospettiva, sono pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative (ad esempio, gli incarichi ricoperti), nonché ulteriori informazioni di carattere professionale (si pensi alle conoscenze linguistiche oppure alle competenze nell'uso delle tecnologie, come pure alla partecipazione a convegni e seminari oppure alla redazione di pubblicazioni da parte dell'interessato). Non devono formare invece oggetto di pubblicazione dati eccedenti, quali ad esempio i recapiti personali oppure il codice fiscale degli interessati, ciò anche al fine di ridurre il rischio di c.d. furti di identità. Deve inoltre essere garantita agli interessati la possibilità di aggiornare periodicamente il proprio curriculum.

L´art. 14 del d.lgs. n 33/2013 dispone la pubblicazione delle "dichiarazioni di cui all'articolo 2, della legge 5 luglio 1982, n. 441, nonché le attestazioni e dichiarazioni di cui agli articoli 3 e 4 della medesima legge, come modificata dal presente decreto, limitatamente al soggetto, al coniuge non separato e ai parenti entro il secondo grado, ove gli stessi vi consentano". Con riferimento all'obbligo di pubblicazione della dichiarazione dei redditi, la predetta disposizione deve essere coordinata con le altre disposizioni dello stesso d.lgs. n. 33/2013 (art. 4, comma 4), con i principi di pertinenza e non eccedenza del RGPD, nonché con le previsioni a tutela dei dati particolari. Pertanto, ai fini dell´adempimento del previsto obbligo di pubblicazione, risulta sufficiente pubblicare copia della dichiarazione dei redditi – dei componenti degli organi di indirizzo politico e, laddove vi acconsentano, del coniuge non separato e dei parenti entro il secondo grado – previo però oscuramento, a cura dell´interessato o del soggetto tenuto alla pubblicazione qualora il primo non vi abbia provveduto, delle informazioni eccedenti e non pertinenti rispetto alla ricostruzione della situazione patrimoniale degli interessati (quali, ad esempio, lo stato civile, il codice fiscale, la sottoscrizione, etc.), nonché di quelle dalle quali si possano desumere indirettamente dati di tipo sensibile, come, fra l´altro, le indicazioni relative a: familiari a carico tra i quali possono essere indicati figli disabili; spese mediche e di assistenza per portatori di handicap o per determinate patologie; erogazioni liberali in denaro a favore dei movimenti e partiti politici; erogazioni liberali in denaro a favore delle organizzazioni non lucrative di utilità sociale, delle iniziative umanitarie, religiose, o laiche, gestite da fondazioni, associazioni, comitati ed enti individuati con decreto del Presidente del Consiglio dei ministri nei paesi non appartenenti all´OCSE; contributi associativi versati dai soci alle società di mutuo soccorso che operano esclusivamente nei settori di cui all´art. 1 della legge 15 aprile 1886, n. 3818, al fine di assicurare ai soci medesimi un sussidio nei casi di malattia, di impotenza al lavoro o di vecchiaia, oppure, in caso di decesso, un aiuto alle loro famiglie; spese sostenute per i servizi di interpretariato dai soggetti riconosciuti sordomuti ai sensi della legge 26 maggio 1970, n. 381; erogazioni liberali in denaro a favore delle istituzioni religiose; scelta per la destinazione dell´otto per mille; scelta per la destinazione del cinque

per mille.

Giova ricordare che non possono essere pubblicati i dati personali del coniuge non separato e dei parenti entro il secondo grado che non abbiano prestato il consenso alla pubblicazione delle attestazioni e delle dichiarazioni di cui all´art. 14, comma 1, lett. f), del d.lgs. n. 33/2013.

La disciplina in materia di trasparenza prevede che informazioni concernenti l'entità di corrispettivi e compensi percepiti da alcune tipologie di soggetti formino oggetto di pubblicazione secondo le modalità previste dal d.lgs. n. 33/2013. Tra questi ultimi sono annoverati, ad esempio, i titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza (cfr. artt. 15 e 41, commi 2 e 3), nonché i dipendenti pubblici cui siano stati conferiti o autorizzati incarichi (art. 18). Pertanto, ai fini dell'adempimento degli obblighi di pubblicazione, risulta proporzionato indicare il compenso complessivo percepito dai singoli soggetti interessati, determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione. Non appare, invece, giustificato riprodurre sul web la versione integrale di documenti contabili, i dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore come pure l'indicazione di altri dati eccedenti riferiti a percettori di somme (quali, ad esempio, i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti). Non risulta inoltre giustificata la pubblicazione di informazioni relative alle dichiarazioni dei redditi dei dipendenti e dei loro familiari, ipotesi questa che la legge impone esclusivamente nei confronti dei componenti degli organi di indirizzo politico (art. 14, del d.lgs. n. 33/2013).

L´art. 23 del d.lgs. n. 33/2013 prevede la pubblicazione obbligatoria di elenchi dei provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti, tra i quali vanno menzionati i provvedimenti finali dei procedimenti relativi alla scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta ai sensi del codice dei contratti pubblici, relativi a lavori, servizi e forniture, di cui al decreto legislativo 18 aprile 2016, n. 50, fermo restando quanto previsto dall'articolo 9-bis e gli accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche, ai sensi degli articoli 11 e 15 della legge 7 agosto 1990, n. 241.

L´art. 26, comma 2, del d.lgs. n. 33/2013 si occupa dell'obbligo di pubblicazione degli atti di concessione "delle sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese, e comunque di vantaggi economici di qualunque genere a persone ed enti pubblici e privati ai sensi del citato articolo 12 della legge n. 241 del 1990, di importo superiore a mille euro". Il comma 3 del medesimo articolo aggiunge che tale pubblicazione "costituisce condizione legale di efficacia dei provvedimenti che dispongano concessioni e attribuzioni di importo complessivo superiore a mille euro nel corso dell'anno solare al medesimo beneficiario". In merito alle predette pubblicazioni è prevista l´indicazione delle seguenti informazioni: a) il nome dell´impresa o dell´ente e i rispettivi dati fiscali o il nome di altro soggetto beneficiario; b) l´importo del vantaggio economico corrisposto; c) la norma o il titolo a base dell´attribuzione; d) l´ufficio e il funzionario o dirigente responsabile del relativo procedimento amministrativo; e) la modalità seguita per l´individuazione del beneficiario; f) il link al progetto selezionato e al curriculum del soggetto incaricato (art. 27, comma 1). In tale quadro, lo stesso d.lgs. n. 33/2013 individua una serie di limiti all'obbligo di pubblicazione di atti di concessione di benefici economici comunque denominati. Non possono, infatti, essere pubblicati i dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici, nonché gli elenchi dei relativi destinatari: a) di importo complessivo inferiore a mille euro nel corso dell´anno solare a favore del medesimo beneficiario; b) di importo superiore a mille euro nel corso dell´anno solare a favore del medesimo beneficiario "qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute" (art. 26, comma 4, d.lgs. n. 33/2013; nonché artt. 22, comma 8, e 68, comma 3, del Codice); c) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario "qualora da tali dati sia possibile ricavare informazioni relative […] alla situazione di disagio economico-sociale degli interessati" (art. 26, comma 4, d.lgs. n. 33/2013).

Si ribadisce, con specifico riferimento alle informazioni idonee a rivelare lo stato di

salute, che è vietata la diffusione di qualsiasi dato o informazione da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. Si pensi, ad esempio, all'indicazione della disposizione sulla base della quale ha avuto luogo l´erogazione del beneficio economico se da essa è possibile ricavare informazioni sullo stato di salute di una persona o dei titoli dell´erogazione dei benefici (es. attribuzione di borse di studio a "soggetto portatore di handicap", o riconoscimento di buono sociale a favore di "anziano non autosufficiente" o con l´indicazione, insieme al dato anagrafico, delle specifiche patologie sofferte dal beneficiario); delle modalità e dei criteri di attribuzione del beneficio economico (es. punteggi attribuiti con l´indicazione degli "indici di autosufficienza nelle attività della vita quotidiana" ; della destinazione dei contributi erogati (es. contributo per "ricovero in struttura sanitaria" o per "assistenza sanitaria").

È, inoltre, vietato riportare dati o informazioni da cui si può desumere la condizione di indigenza o di disagio sociale in cui versano gli interessati (art. 26, comma 4, del d.lgs. n. 33/2013).

Si tratta di un divieto funzionale alla tutela della dignità, dei diritti e delle libertà fondamentali dell'interessato, al fine di evitare che soggetti che si trovano in condizioni disagiate – economiche o sociali – soffrano l'imbarazzo della diffusione di tali informazioni, o possano essere sottoposti a conseguenze indesiderate, a causa della conoscenza da parte di terzi della particolare situazione personale. Si pensi, fra l'altro alle fasce deboli della popolazione (persone inserite in programmi di recupero e di reinserimento sociale, anziani, minori di età, etc.). Alla luce delle considerazioni sopra espresse, spetta agli enti destinatari degli obblighi di pubblicazione online contenuti nel d.lgs. n. 33/2013, in quanto titolari del trattamento, valutare, caso per caso, quando le informazioni contenute nei provvedimenti rivelino l'esistenza di una situazione di disagio economico o sociale in cui versa il destinatario del beneficio e non procedere, di conseguenza, alla pubblicazione dei dati identificativi del beneficiario o delle altre informazioni che possano consentirne l'identificazione. Tale decisione rimane comunque sindacabile da parte del Garante che assicura il rispetto dei già menzionati principi in materia di protezione dei dati personali. In ogni modo, si evidenzia che i soggetti destinatari degli obblighi di pubblicazione contenuti nel d.lgs. n. 33/2013 sono tenuti, anche in tale ambito, al rispetto dei principi di minimizzazione, pertinenza e non eccedenza, nonché delle disposizioni a tutela dei dati particolari.

"Non risulta, pertanto, giustificato diffondere, fra l´altro, dati quali, ad esempio, l´indirizzo di abitazione o la residenza, il codice fiscale di persone fisiche, le coordinate bancarie dove sono accreditati i contributi o i benefici economici (codici IBAN), la ripartizione degli assegnatari secondo le fasce dell´Indicatore della situazione economica equivalente-Isee, l´indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative, etc. Si evidenzia, inoltre, che il riutilizzo dei dati personali pubblicati ai sensi dei predetti artt. 26 e 27, non è libero, ma subordinato – come stabilito dallo stesso art. 7 del d.lgs. n. 33/2013 – alle specifiche disposizioni di cui alla direttiva comunitaria 2003/98/CE e al d.lgs. n. 36 del 24 gennaio 2006 di recepimento della stessa, che non pregiudicano in alcun modo il livello di tutela delle persone con riguardo al trattamento dei dati personali"[45].

L'assolvimento degli obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici descritti nel paragrafo precedente deve essere coordinato con le disposizioni che regolano la predisposizione dell´albo dei beneficiari di provvidenze di natura economica (d.P.R. 7 aprile 2000, n. 118).

Per tale motivo, alla luce di un'interpretazione sistematica del quadro normativo emergente dalla recente novella in tema di trasparenza e al fine di non duplicare in capo alle pubbliche amministrazioni gli oneri di pubblicazione, deve ritenersi che l'adempimento delle prescrizioni contenute negli artt. 26 e 27 del d.lgs. n. 33/2013, con le relative modalità ed eccezioni descritte nel

[45] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*, 15 maggio 2014, doc. web 3134436.

paragrafo precedente, assorbe gli obblighi previsti dagli artt. 1 e 2 del d.P.R. n. 118.

Gran parte delle indicazioni fornite dal Garante per la protezione dei dati personali contenute nelle linee guida del 15 maggio 2014 sono state riprese dall'Autorità Nazionale Anticorruzione con la delibera n. 1310 del 28 dicembre 2016: *Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016*.

Le linee guida del Garante del 15 maggio 2014, come già rilevato, hanno lo scopo di definire un quadro unitario di misure e accorgimenti diretti a individuare opportune cautele che i soggetti pubblici, e gli altri soggetti parimenti destinatari delle norme vigenti, sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa. Pertanto, le predette linee guida sostituiscono le precedenti "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" del 2 marzo 2011 (doc. web n. 1793203).

Le linee guida del 15 maggio 2014 vanno lette in relazione al profilo del diverso regime giuridico applicabile, le disposizioni che regolano gli obblighi di pubblicità dell'azione amministrativa per finalità di trasparenza vanno distinte da quelle che regolano forme di pubblicità per finalità diverse (es.: pubblicità legale). Come più volte rilevato, gli obblighi di pubblicazione online di dati per finalità di trasparenza sono quelli indicati nel d.lgs. n. 33/2013 e agli obblighi introdotti dalla predetta normativa si applicano le indicazioni contenute nella parte prima delle suddette linee guida.

Accanto a questi obblighi di pubblicazione permangono altri obblighi di pubblicità online di dati, informazioni e documenti della pubblica amministrazione, contenuti in specifiche disposizioni di settore diverse da quelle approvate in materia di trasparenza, come, fra l´altro, quelli volti a far conoscere l´azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli atti a garantire la pubblicità legale degli atti amministrativi (es.: pubblicità integrativa dell´efficacia, dichiarativa, notizia). Si pensi, a titolo meramente esemplificativo, alle pubblicazioni ufficiali dello Stato, alle pubblicazioni di deliberazioni, ordinanze e determinazioni sull´albo pretorio online degli enti locali (oppure su analoghi albi di altri enti, come ad esempio le Asp), alle pubblicazioni matrimoniali, alla pubblicazione degli atti concernenti il cambiamento del nome, alla pubblicazione della comunicazione di avviso deposito delle cartelle esattoriali a persone irreperibili, ai casi di pubblicazione dei ruoli annuali tributari dei consorzi di bonifica, alla pubblicazione dell´elenco dei giudici popolari di corte d´assise, etc. A tali obblighi si riferiscono le indicazioni contenute nella parte seconda delle linee guida del 15 maggio 2014.

Il d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, ha operato una significativa estensione dei confini della trasparenza intesa oggi come «accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche». Il legislatore ha attribuito un ruolo di primo piano alla trasparenza affermando, tra l'altro, che essa concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Essa è anche da considerare come condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integrando il diritto ad una buona amministrazione e concorrendo alla realizzazione di una amministrazione aperta, al servizio del cittadino. Oggi, dunque, la trasparenza è anche regola per l'organizzazione, per l'attività amministrativa e per la realizzazione di una moderna democrazia. In tal senso si è espresso anche il Consiglio di Stato laddove ha ritenuto che "la trasparenza viene a configurarsi, ad un tempo, come un mezzo per porre in essere una azione amministrativa più efficace e conforme ai canoni costituzionali e come un obiettivo a cui tendere, direttamente legato al valore democratico della funzione amministrativa" (Cons. Stato., Sez. consultiva per gli atti normativi, 24 febbraio 2016, n. 515, parere reso sullo schema di decreto n.

97/2016). Le disposizioni in materia di trasparenza amministrativa, inoltre, integrano l'individuazione del livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche a fini di trasparenza, prevenzione, contrasto della corruzione e della cattiva amministrazione, a norma dell'art. 117, co. 2, lett. m), della Costituzione (art. 1, co. 3, d.lgs. 33/2013). La trasparenza assume, così, rilievo non solo come presupposto per realizzare una buona amministrazione ma anche come misura per prevenire la corruzione, promuovere l'integrità e la cultura della legalità in ogni ambito dell'attività pubblica, come già l'art. 1, co. 36 della legge 190/2012 aveva sancito. Dal richiamato comma si evince, infatti, che i contenuti del d.lgs. 33/2013 «integrano l'individuazione del livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche a fini di trasparenza, prevenzione, contrasto della corruzione e della cattiva amministrazione». La stessa Corte Costituzionale (sent. 20/2019) ha considerato che con la legge 190/2012 «la trasparenza amministrativa viene elevata anche al rango di principio-argine alla diffusione di fenomeni di corruzione» e che le modifiche al d.lgs. 33/2013, introdotte dal d.lgs. n. 97/2016, hanno esteso ulteriormente gli scopi perseguiti attraverso il principio di trasparenza, aggiungendovi la finalità di «tutelare i diritti dei cittadini» e "promuovere la partecipazione degli interessati all'attività amministrativa". La Corte ha riconosciuto, inoltre, che i principi di pubblicità e trasparenza trovano riferimento nella Costituzione italiana in quanto corollario del principio democratico (art. 1 Cost.) e del buon funzionamento dell'amministrazione (art. 97 Cost.). L'ampliamento dei confini della trasparenza registrato nel nostro ordinamento, appena illustrato, è stato realizzato con successive modifiche normative che sono state accompagnate da atti di regolazione dell'Autorità finalizzati a fornire indicazioni ai soggetti tenuti ad osservare la disciplina affinché l'attuazione degli obblighi di pubblicazione non fosse realizzata in una logica di mero adempimento quanto, invece, di effettività e piena conoscibilità dell'azione amministrativa.

Come rilevato da attenta dottrina[46], una delle novità importanti è contenuta nell'art. 2, il quale non si limita solo a richiamare lo scopo della trasparenza intesa come accessibilità totale: non si tratta solo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche, ma anche di tutelare i diritti fondamentali. La trasparenza è, infatti, condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto a una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino.

Lo scopo della norma è quello di garantire la conoscibilità dei documenti e dei dati relativi prodotti dalle amministrazioni, nonché la libertà di accesso a dati e documenti (oggetto di pubblicazione obbligatoria) in possesso della pubblica amministrazione attraverso l'accesso civico "semplice", ma anche attraverso l'accesso civico "generalizzato" relativamente ai dati e ai documenti detenuti dalle amministrazioni ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria (aspetto questo che sarà ripreso e approfondito nel prosieguo).

Tutti i documenti, le informazioni e i dati oggetto di accesso civico, ivi compresi quelli oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'art. 7 del d.lgs n. 33/2013.

Il decreto introduce, al riguardo, la nozione di accesso civico, per distinguerla da quella di accesso ai sensi degli articoli 22 ss. della legge n. 241/1990 sul procedimento amministrativo (articolo 5). Con essa, s'intende, il diritto di chiunque di richiedere alle pubbliche amministrazioni i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria, nei casi in cui questa sia stata omessa. A differenza del diritto di accesso agli atti di cui alla legge 241/1990, la richiesta di accesso civico non è sottoposta ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente, siamo, infatti, in presenza di un diritto a titolarità diffusa. Non è soggetto, inoltre, a motivazione.

"La giuridicizzazione di un tale ambito di trasparenza si traduce nella pubblicità di una serie di informazioni, che conferma la distanza, sul piano del diritto positivo, tra accesso e trasparenza, in quanto il primo,

[46] D. Urania Galletta, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *Fedaralismi.it*, 2016.

come posizione qualificata da un criterio di collegamento specifico tra richiedente l'accesso e il dato che si vuole conoscere, non ha evidentemente spazio per operare laddove quel dato sia pubblico perché accessibile all'intera collettività. In tale ottica la trasparenza, pur sempre riferibile al duplice versante organizzativo e "attivo" dell'amministrazione e quindi al procedimento amministrativo, acquista una sua ragion d'essere anche, e forse soprattutto, al di fuori dello schema e del momento procedimentale in senso stretto"[47].

Con l'accesso civico il legislatore introduce un meccanismo rimediale di assoluta novità, riconoscendo in capo a chiunque un vero e proprio diritto di accesso civico a quelle informazioni e a quei dati (siano o meno contenuti in atti giuridici in senso stretto) per i quali risulti non adempiuto l'obbligo di pubblicità: un diritto di accesso, quindi, svincolato dai requisiti di legittimazione dell'accesso previsto dalla legge n. 241 del 1990, azionabile senza formalità, senza necessità di motivare l'istanza, senza dover dimostrare l'utilità dell'atto che si intende conoscere rispetto alle esigenze difensive del richiedente, ma fondato sul solo presupposto dell'inadempimento in cui l'amministrazione è incorsa rispetto agli obblighi di pubblicità.

Gli obblighi di pubblicazione, previsti dal decreto, integrano una "situazione che fronteggia (...) un diritto soggettivo a conoscere, che spetta a "chiunque", ossia ai cittadini in quanto tali (senza necessità di dimostrare l'interesse differenziato che giustifichi tale pretesa) (art. 3). Agli obblighi di pubblicazione corrisponde dunque non un *need to know* (una conoscenza utile al soddisfacimento di un interesse, di un bisogno particolare), ma un vero *right to know*. Un diritto conseguentemente assistito da un meccanismo di implementazione (in caso di inadempimento dell'obbligo di pubblicazione) attivabile da chiunque, quasi nella forma dell'azione popolare"[48].

Il legislatore nel 2016 al fine di dare forza e vigore al principio del controllo diffuso della generalità dei cittadini, inteso come controllo democratico e carattere essenziale della trasparenza pubblica delle istituzioni pubbliche, ha introdotto nel nostro ordinamento giuridico l'istituto dell'accesso civico "generalizzato": "Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis" (art. 5, c. 2, del d.lgs. n. 33/2013).

La Corte Costituzionale, chiamata ad esprimersi sul tema del bilanciamento tra diritto alla riservatezza dei dati personali, inteso come diritto a controllare la circolazione delle informazioni riferite alla propria persona, e quello dei cittadini al libero accesso ai dati ed alle informazioni detenuti dalle pubbliche amministrazioni, ha riconosciuto che entrambi i diritti sono «contemporaneamente tutelati sia dalla Costituzione che dal diritto europeo, primario e derivato» (Corte Cost., 23 gennaio 2019, n. 20).

Ritiene la Corte che, se da una parte il diritto alla riservatezza dei dati personali, quale manifestazione del diritto fondamentale all'intangibilità della sfera privata, attiene alla tutela della vita degli individui nei suoi molteplici aspetti e trova sia riferimenti nella Costituzione italiana (artt. 2, 14, 15 Cost.), sia specifica protezione nelle varie norme europee e convenzionali, dall'altra parte, con eguale rilievo, si incontrano i principi di pubblicità e trasparenza, riferiti non solo, quale corollario del principio democratico (art. 1 Cost.) a tutti gli aspetti rilevanti della vita pubblica e istituzionale, ma anche, ai sensi dell'art. 97 Cost., al buon funzionamento dell'amministrazione e ai dati che essa possiede e controlla. Principi che, nella legislazione interna, si manifestano nella loro declinazione soggettiva, nella forma di un diritto dei cittadini ad accedere ai dati in possesso della pubblica amministrazione, come stabilito dall'art. 1, co. 1, del d.lgs. n. 33/2013.

Il bilanciamento tra i due diritti è, quindi, necessario, come lo stesso Considerando n. 4

[47] F. Patroni Griffi, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *Federalismi.it*, 2013.

[48] B. Ponti, *Il codice della trasparenza amministrativa: non solo riordino, ma ridefinizione complessiva del regime della trasparenza amministrativa on-line*, in *www.neldiritto.it*.

del Regolamento (UE) 2016/679 indica, prevedendo che «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».

In particolare, nella richiamata sentenza, la Corte precisa che il bilanciamento della trasparenza e della privacy va compiuto avvalendosi del test di proporzionalità che "richiede di valutare se la norma oggetto di scrutinio, con la misura e le modalità di applicazione stabilite, sia necessaria e idonea al conseguimento di obiettivi legittimamente perseguiti, in quanto, tra più misure appropriate, prescriva quella meno restrittiva dei diritti a confronto e stabilisca oneri non sproporzionati rispetto al perseguimento di detti obiettivi". L'art. 3 Cost., integrato dai principi di derivazione europea, sancisce l'obbligo, per la legislazione nazionale, di rispettare i criteri di necessità, proporzionalità, finalità, pertinenza e non eccedenza nel trattamento dei dati personali, pur al cospetto dell'esigenza di garantire, fino al punto tollerabile, la pubblicità dei dati in possesso della pubblica amministrazione.

Pertanto, al principio di trasparenza, nonostante non trovi espressa previsione nella Costituzione, si riconosce rilevanza costituzionale, in quanto fondamento di diritti, libertà e principi costituzionalmente garantiti (artt. 1 e 97 Cost.).

Il quadro delle regole in materia di protezione dei dati personali si è consolidato con l'entrata in vigore, il 25 maggio 2018, del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito RGPD) e, il 19 settembre 2018, del decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali – decreto legislativo 30 giugno 2003, n. 196 - alle disposizioni del Regolamento (UE) 2016/679.

Occorre evidenziare che l'art. 2-ter del d.lgs. n. 196 del 2003, introdotto dal d.lgs. 101/2018, in continuità con il previgente articolo 19 del Codice, dispone al comma 1 che la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ai sensi dell'art. 6, paragrafo 3, lett. b) del Regolamento (UE) 2016/679, "è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento». Inoltre, il comma 3 del medesimo articolo stabilisce che «La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1».

Il regime normativo per il trattamento di dati personali da parte dei soggetti pubblici è, quindi, rimasto sostanzialmente inalterato, essendo confermato il principio che esso è consentito unicamente se ammesso da una norma di legge o, nei casi previsti dalla legge, di regolamento.

La nuova tipologia di accesso (d'ora in poi "accesso generalizzato"), delineata nel novellato art. 5, comma 2 del d.lgs. n. 33/2013, ai sensi del quale "chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, secondo quanto previsto dall'art. 5-bis", si traduce, in estrema sintesi, in un diritto di accesso non condizionato dalla titolarità di situazioni giuridicamente rilevanti ed avente ad oggetto tutti i dati e i documenti e informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli per i quali è stabilito un obbligo di pubblicazione.

La ratio della riforma risiede nella dichiarata finalità di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico (art. 5, comma 2, d.lgs. n. 33/2013).

A questa impostazione, come mette in luce l'ANAC nella determinazione n. 1309 del 28 dicembre 2016 redatta d'intesa con il Garante per la protezione dei dati personali, consegue, nel novellato decreto 33/2013, il rovesciamento della precedente prospettiva che comportava l'attivazione del diritto di accesso civico solo strumentalmente all'adempimento degli obblighi di pubblicazione; ora è proprio la libertà di accedere ai dati e ai documenti, cui corrisponde una diversa versione dell'accesso civico, a divenire centrale nel nuovo sistema, in analogia agli ordinamenti aventi il *Freedom of Information Act* (FOIA), ove il diritto

all'informazione è generalizzato e la regola generale è la trasparenza mentre la riservatezza e il segreto eccezioni.

In coerenza con il quadro normativo, il diritto di accesso civico generalizzato si configura come diritto a titolarità diffusa, potendo essere attivato "da chiunque" e non essendo sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente. A ciò si aggiunge un ulteriore elemento, ossia che l'istanza "non richiede motivazione". In altri termini, tale nuova tipologia di accesso civico risponde all'interesse dell'ordinamento di assicurare ai cittadini (a "chiunque"), indipendentemente dalla titolarità di situazioni giuridiche soggettive, un accesso a dati, documenti e informazioni detenute da pubbliche amministrazioni e dai soggetti indicati nell'art. art. 2-bis del d.lgs. 33/2013 come modificato dal d.lgs. n. 97/2016.

L'accesso generalizzato deve essere anche tenuto distinto dalla disciplina dell'accesso ai documenti amministrativi di cui agli articoli 22 e seguenti della legge 7 agosto 1990, n. 241.

La finalità dell'accesso documentale ex legge 241/90 è, in effetti, ben differente da quella sottesa all'accesso generalizzato ed è quella di porre i soggetti interessati in grado di esercitare al meglio le facoltà - partecipative e/o oppositive e difensive – che l'ordinamento attribuisce loro a tutela delle posizioni giuridiche qualificate di cui sono titolari. Più precisamente, dal punto di vista soggettivo, ai fini dell'istanza di accesso ex legge 241 il richiedente deve dimostrare di essere titolare di un «interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso». Mentre la legge 241/90 esclude, inoltre, perentoriamente l'utilizzo del diritto di accesso ivi disciplinato al fine di sottoporre l'amministrazione a un controllo generalizzato.

Dunque, l'accesso agli atti di cui alla legge 241/90 continua certamente a sussistere, ma parallelamente all'accesso civico (generalizzato e non), operando sulla base di norme e presupposti diversi. Tenere ben distinte le due fattispecie è essenziale per calibrare i diversi interessi in gioco allorché si renda necessario un bilanciamento caso per caso tra tali interessi. Tale bilanciamento è, infatti, ben diverso nel caso dell'accesso 241 dove la tutela può consentire un accesso più in profondità a dati pertinenti e nel caso dell'accesso generalizzato, dove le esigenze di controllo diffuso del cittadino devono consentire un accesso meno in profondità (se del caso, in relazione all'operatività dei limiti) ma più esteso, avendo presente che l'accesso in questo caso comporta, di fatto, una larga conoscibilità (e diffusione) di dati, documenti e informazioni.

Data l'innovatività della disciplina dell'accesso generalizzato, che si aggiunge alle altre tipologie di accesso, sembra opportuno suggerire ai soggetti tenuti all'applicazione del decreto trasparenza l'adozione, anche nella forma di un regolamento interno sull'accesso, di una disciplina che fornisca un quadro organico e coordinato dei profili applicativi relativi alle tre tipologie di accesso, con il fine di dare attuazione al nuovo principio di trasparenza introdotto dal legislatore e di evitare comportamenti disomogenei tra uffici della stessa amministrazione.

In particolare, tale disciplina potrebbe prevedere: 1. una sezione dedicata alla disciplina dell'accesso documentale; 2. una seconda sezione dedicata alla disciplina dell'accesso civico ("semplice") connesso agli obblighi di pubblicazione di cui al d.lgs. n. 33; 3. una terza sezione dedicata alla disciplina dell'accesso generalizzato. Tale sezione dovrebbe disciplinare gli aspetti procedimentali interni per la gestione delle richieste di accesso generalizzato. Si tratterebbe, quindi, di: a) provvedere a individuare gli uffici competenti a decidere sulle richieste di accesso generalizzato; b) provvedere a disciplinare la procedura per la valutazione caso per caso delle richieste di accesso.

La regola della generale accessibilità è temperata dalla previsione di eccezioni poste a tutela di interessi pubblici e privati che possono subire un pregiudizio dalla diffusione generalizzata di talune informazioni. Dalla lettura dell'art. 5 bis, co. 1, 2 e 3 del d.lgs. n. 33/2013 si possono distinguere due tipi di eccezioni, assolute o relative.

Al ricorrere di queste eccezioni, le amministrazioni, rispettivamente, devono o possono rifiutare l'accesso generalizzato. La chiara identificazione di tali eccezioni rappresenta un elemento decisivo per consentire la corretta applicazione del diritto di accesso generalizzato.

Tra le eccezioni assolute all'accesso generalizzato, Salvo che non sia possibile un accesso parziale, con oscuramento dei dati, alcuni divieti di divulgazione sono previsti dalla normativa vigente in materia di tutela della riservatezza con riferimento a: dati idonei a rivelare lo stato di salute, ossia a qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici (art. 22, comma 8, del Codice; art. 7-bis, comma 6, d.lgs. n. 33/2013); dati idonei a rivelare la vita sessuale (art. 7-bis, comma 6, d.lgs. n. 33/2013); dati identificativi di persone fisiche beneficiarie di aiuti economici da cui è possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati (limite alla pubblicazione previsto dall'art. 26, comma 4, d.lgs. n. 33/2013).

Resta, in ogni caso, ferma la possibilità che i dati personali per i quali sia stato negato l'accesso generalizzato possano essere resi ostensibili al soggetto che abbia comunque motivato nell'istanza l'esistenza di «un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso», trasformando di fatto, con riferimento alla conoscenza dei dati personali, l'istanza di accesso generalizzato in un'istanza di accesso ai sensi della legge 241/1990.

Accanto alle eccezioni assolute, la normativa ha individuato limiti relativi a tutela di interessi privati. Il d.lgs. n. 33/2013 ha previsto, all'art. 5-bis, comma 2, che l'accesso generalizzato è rifiutato se il diniego è necessario per evitare il pregiudizio concreto alla tutela degli interessi privati specificamente indicati dalla norma e cioè:

a) protezione dei dati personali

b) libertà e segretezza della corrispondenza

c) interessi economici e commerciali di una persona fisica o giuridica, ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali.

L'art. 5-bis, comma 2, lett. a), del d.lgs. n. 33/2013 prevede che l'accesso generalizzato deve essere rifiutato laddove possa recare un pregiudizio concreto «alla protezione dei dati personali, in conformità con la disciplina legislativa in materia». Le informazioni riferite a persone giuridiche, enti e associazioni non rientrano nella nozione di dato personale.

Con riferimento alle istanze di accesso generalizzato aventi a oggetto dati e documenti relativi a (o contenenti) dati personali, l'ente destinatario dell'istanza deve valutare, nel fornire riscontro motivato a richieste di accesso generalizzato, se la conoscenza da parte di chiunque del dato personale richiesto arreca (o possa arrecare) un pregiudizio concreto alla protezione dei dati personali, in conformità alla disciplina legislativa in materia. La ritenuta sussistenza di tale pregiudizio comporta il rigetto dell'istanza, a meno che non si consideri di poterla accogliere, oscurando i dati personali eventualmente presenti e le altre informazioni che possono consentire l'identificazione, anche indiretta, del soggetto interessato devono essere tenute in considerazione le motivazioni addotte dal soggetto controinteressato, che deve essere obbligatoriamente interpellato dall'ente destinatario della richiesta di accesso generalizzato, ai sensi dell'art. 5, comma 5, del d.lgs. n. 33/2013. Tali motivazioni costituiscono un indice della sussistenza di un pregiudizio concreto, la cui valutazione però spetta all'ente e va condotta anche in caso di silenzio del controinteressato.

Il soggetto destinatario dell'istanza, nel dare riscontro alla richiesta di accesso generalizzato, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei dati personali in esso presenti, laddove l'esigenza informativa, alla base dell'accesso generalizzato, possa essere raggiunta senza implicare il trattamento dei dati personali. In tal modo, tra l'altro, si soddisfa anche la finalità di rendere più celere il procedimento relativo alla richiesta di accesso generalizzato, potendo accogliere l'istanza senza dover attivare l'onerosa procedura di coinvolgimento del soggetto "controinteressato" (art. 5, comma 5, del d.lgs. n. 33/2013).

Al riguardo, deve essere ancora evidenziato che l'accesso generalizzato è servente rispetto alla conoscenza di dati e documenti detenuti dalla pubblica amministrazione "Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di

promuovere la partecipazione al dibattito pubblico" (art. 5, comma 2, del d.lgs. n. 33/2013). Di conseguenza, quando l'oggetto della richiesta di accesso riguarda documenti contenenti informazioni relative a persone fisiche (e in quanto tali dati personali) non necessarie al raggiungimento del predetto scopo, oppure informazioni personali di dettaglio che risultino comunque sproporzionate, eccedenti e non pertinenti, l'ente destinatario della richiesta dovrebbe accordare l'accesso parziale ai documenti, oscurando i dati personali ivi presenti.

Ai fini della valutazione del pregiudizio concreto, vanno prese in considerazione le conseguenze – anche legate alla sfera morale, relazionale e sociale – che potrebbero derivare all'interessato (o ad altre persone alle quali esso è legato da un vincolo affettivo) dalla conoscibilità, da parte di chiunque, del dato o del documento richiesto, tenuto conto delle implicazioni derivanti dalla previsione di cui all'art. 3, comma 1, del d.lgs. n. 33/2013, in base alla quale i dati e i documenti forniti al richiedente tramite l'accesso generalizzato sono considerati come pubblici, sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 7 del d.lgs. n. 33/2013).

Tali conseguenze potrebbero riguardare, ad esempio, future azioni da parte di terzi nei confronti dell'interessato, o situazioni che potrebbero determinare l'estromissione o la discriminazione dello stesso individuo, oppure altri svantaggi personali e/o sociali. In questo quadro, può essere valutata, ad esempio, l'eventualità che l'interessato possa essere esposto a minacce, intimidazioni, ritorsioni o turbative al regolare svolgimento delle funzioni pubbliche o delle attività di pubblico interesse esercitate, che potrebbero derivare, a seconda delle particolari circostanze del caso, dalla conoscibilità di determinati dati. Analogamente, vanno tenuti in debito conto i casi in cui la conoscibilità di determinati dati personali da parte di chiunque possa favorire il verificarsi furti d'identità o di creazione di identità fittizie.

Per verificare l'impatto sfavorevole che potrebbe derivare all'interessato dalla conoscibilità da parte di chiunque delle informazioni richieste, l'ente destinatario della richiesta di accesso generalizzato deve far riferimento a diversi parametri, tra i quali, anche la natura dei dati personali oggetto della richiesta di accesso o contenuti nei documenti ai quali di chiede di accedere, nonché il ruolo ricoperto nella vita pubblica, la funzione pubblica esercitata o l'attività di pubblico interesse svolta dalla persona cui si riferiscono i predetti dati.

Riguardo al primo profilo, la presenza di dati sensibili e/o giudiziari può rappresentare un indice della sussistenza del predetto pregiudizio, laddove la conoscenza da parte di chiunque che deriverebbe dall'ostensione di tali informazioni – anche in contesti diversi (familiari e/o sociali) – possa essere fonte di discriminazione o foriera di rischi specifici per l'interessato. In linea di principio, quindi, andrebbe rifiutato l'accesso generalizzato a tali informazioni, potendo invece valutare diversamente, caso per caso, situazioni particolari quali, ad esempio, quelle in cui le predette informazioni siano state deliberatamente rese note dagli interessati, anche attraverso loro comportamenti in pubblico.

Analoghe considerazioni sull'esistenza del pregiudizio concreto possono essere fatte per quelle categorie di dati personali che, pur non rientrando nella definizione di dati sensibili e giudiziari, richiedono una specifica protezione quando dal loro utilizzo, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, possano derivare rischi specifici per i diritti e le libertà fondamentali degli interessati (si pensi, ad esempio, ai dati genetici, biometrici, di profilazione, sulla localizzazione o sulla solvibilità economica).

Tra gli altri fattori da tenere in considerazione ai fini della valutazione della sussistenza del pregiudizio in esame, merita rilievo anche la circostanza che la richiesta di accesso generalizzato riguardi dati o documenti contenenti dati personali di soggetti minori, la cui conoscenza può ostacolare il libero sviluppo della loro personalità, in considerazione della particolare tutela dovuta alle fasce deboli.

Riguardo al secondo profilo, va considerato altresì che la sussistenza di un pregiudizio concreto alla protezione dei dati personali può verificarsi con più probabilità per talune particolari informazioni – come ad esempio situazioni personali, familiari, professionali, patrimoniali – di persone fisiche destinatarie dell'attività amministrativa o intervenute a vario titolo nella stessa e che, quindi, non ricoprono necessariamente un ruolo nella vita

pubblica o non esercitano funzioni pubbliche o attività di pubblico interesse.

8. *Smart working e protezione dei dati personali nella Pubblica Amministrazione*

«Michel de Montaigne ci ricordava che "la vie est un mouvement inégal, irrégulier et multiforme" (*Essais*, Livre III, Chap. III, De trois commerces). Questo movimento è oggi sempre più influenzato dall'incessante innovazione scientifica e tecnologica. I ritmi della vita conoscono accelerazioni e mutamenti profondi», così Stefano Rodotà apriva uno dei suoi tanti studi dedicati al rapporto tra nuove tecnologie e diritti della persona[49]. Tutto ciò lo abbiamo constatato, ormai da più di due anni, a seguito dell'improvvisa e inattesa accelerazione impressa dalla pandemia da Sars-CoV-2 alla transizione digitale, che ci ha imposto di ripensare, con altrettanta rapidità, il nostro modo di concepire questa nuova dimensione della vita. Come rilevato da Antonello Soro, "la devoluzione alla dimensione immateriale di quasi tutte le nostre attività è un processo neutro, ma comporta, se non assistito da adeguate garanzie, l'esposizione a inattese vulnerabilità in termini non solo di sicurezza informatica, ma anche di soggezione a intrusioni e controlli sempre più penetranti e pericolosi, poiché meno percettibili rispetto a quelli "tradizionali"[50].

Pensiamo, ad esempio, al contesto lavorativo e, al fenomeno, in particolare, dello *smart working*, generalmente necessitato e improvvisato, che ha catapultato migliaia di lavoratori in una dimensione delle cui implicazioni, il più delle volte, non si ha la piena consapevolezza e di cui occorre impedire un uso improprio. L'inarrestabile processo di digitalizzazione e l'emergere di nuovi processi economici sono questioni ampiamente trattati nella letteratura sociologica ed economico-aziendale, nonché entrati da tempo nell'agenda delle istituzioni europee. Le analisi si concentrano, in particolare, "sui fattori innovativi e sulle caratteristiche degli scenari in divenire, con l'obiettivo di discernere ciò che costituisce un'autentica rottura rispetto al passato e ciò che rappresenta invece un'accelerazione di tendenze già presenti nei processi di ristrutturazione produttiva delle imprese e nelle trasformazioni del lavoro"[51]. Lo *smart working*, potendo favorire una nuova articolazione dei processi produttivi in grado di accrescere efficienza e flessibilità, potrebbe costituire una forma diffusa, alternativa, di organizzazione del lavoro. Per questo motivo andranno affrontati con serietà e lungimiranza tutti i problemi emersi in questi mesi, a seguito della pandemia: dalle dotazioni strumentali alla garanzia di connettività, alla sicurezza delle piattaforme, all'effettività del diritto alla disconnessione, senza il quale si rischia di rendere vana la necessaria distinzione tra sfera privata e attività lavorativa.

Lo *smart working* è una rivoluzione culturale, organizzativa e di processo. Una rivoluzione poiché scardina alla base consuetudini e approcci tradizionali e consolidati nel mondo del lavoro subordinato, fondandosi su una cultura orientata ai risultati e su una valutazione legata alle reali performance. Secondo la definizione data il Ministero del Lavoro e delle Politiche Sociali, lo *smart working* è una modalità di esecuzione del rapporto subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi, cicli e obiettivi, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività".

La legge 22 maggio 2017 n. 81 (art. 18-24) ha fornito allo *smart working* una cornice normativa e ha posto le basi legali per la sua applicazione anche nel settore pubblico. La

[49] S. Rodotà, *Persona, libertà, tecnologia. Note per una discussione*, in www.dirittoequestionipubbliche.org/page/2005_n5/mono_S_Rodota.pdf.

[50] A. Soro, *Relazione 2019* del Garante per la protezione dei dati personali (www.garanteprivacy.it).

[51] P. Tullini, *Uso delle tecnologie al lavoro. Il controllo a distanza e le garanzie del lavoratore*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, Giappichelli, 2017, 4; A. Bellavista, *Sorveglianza sui lavoratori, protezione dei dati personali e azione collettiva nell'economia digitale*, in C. Alessi, M. Barbera, L. Guaglianone (a cura di), *Impresa, lavoro e non lavoro nell'economia digitale*, Bari, Cacucci Editore, 2019, 151 ss.; P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, Giappichelli, 2017; A. Sartori, *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Torino, Giappichelli, 2020; C. Colapietro, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Giornale di diritto del lavoro e di relazioni industriali*, 2017, 439 ss.; G. Ziccardi, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *Labour & Law Issues*, 2016, 1 ss.

legge all'art. 18 definisce il lavoro agile (*smart working*) come "modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva". Obiettivo dichiarato è promuovere il lavoro agile per "incrementare la competitività e agevolare la conciliazione dei tempi di vita e di lavoro". Il comma 3, sempre del richiamato art. 18, precisa che le disposizioni normative si applicano anche ai "rapporti di lavoro alle dipendenze delle amministrazioni pubbliche". Con la successiva direttiva n. 3 del 2017 del Ministro per la Pubblica Amministrazione ha preso avvio "ufficialmente" la stagione del "lavoro agile" o *smart working* nelle pubbliche amministrazioni. Detta direttiva contiene gli indirizzi per l'attuazione dei commi 1 e 2 dell'art. 14 della legge 7 agosto 2015, n. 124, che delegava il Governo alla riorganizzazione delle amministrazioni pubbliche, prevedendo l'introduzione di nuove e più agili misure di conciliazione dei tempi di vita e di lavoro dei propri dipendenti, e individua le linee guida per la nuova organizzazione del lavoro, finalizzate a promuovere la conciliazione dei tempi di vita e di lavoro dei dipendenti. Le finalità dichiarate sono quelle dell'introduzione delle più innovative modalità di organizzazione del lavoro, basate sull'utilizzo della flessibilità, sulla valutazione per obiettivi, sulla rilevazione dei bisogni del personale dipendente, il tutto, come già rilevato, alla luce dei bisogni di conciliazione dei tempi di vita e di lavoro[52].

Alcuni vantaggi per i lavoratori sono difficilmente confutabili, primo fra tutti la conciliazione tra tempi di vita e di lavoro. Lavorando da casa, infatti, si riesce a gestire meglio il proprio ritmo di lavoro, valorizzando il tempo a disposizione e abbattendo i costi legati agli spostamenti. L'introduzione dello *smart working*, impattando sul benessere e sulla qualità della vita dei propri dipendenti, può essere considerata una misura di welfare aziendale e si riflette in positivo anche sulla produttività. Vi sono poi altri aspetti di profonda innovazione che vanno evidenziati, sia per i lavoratori che per le amministrazioni, come, ad esempio, la valorizzazione delle risorse umane e una maggiore responsabilizzazione. Altri effetti positivi del lavoro agile possono essere individuati nel fatto che ci si concentra sui risultati del lavoro e non sugli aspetti formali, ma anche: nella razionalizzazione nell'uso delle risorse e sull'aumento della produttività, quindi risparmio in termini di costi e miglioramento dei servizi offerti; nella promozione dell'uso delle tecnologie digitali più innovative e l'utilizzo dello *smart working* come leva per la trasformazione digitale e per lo sviluppo delle conoscenze digitali; nel rafforzamento dei sistemi di misurazione e valutazione delle performance basate sui risultati e sui livelli di servizio; nell'abbattimento delle differenze di genere; nella riduzione delle forme di "assenteismo fisiologico".

In questo scenario, la tecnologia riveste un ruolo di primaria importanza. *smart working* e trasformazione digitale si abilitano vicendevolmente: da una parte, infatti, lo *smart working* ha bisogno delle tecnologie per rendere concrete le sue pratiche e i suoi modelli, dall'altra rappresenta esso stesso una grande leva per la realizzazione della pubblica amministrazione digitale.

Il 12 maggio 2020 *Twitter* ha annunciato: "(..) if our employees are in a role and situation that enables them to work from home and they want to continue to do so forever, we will make that happen". In pratica: cari dipendenti, se lo volete, potete scegliere di lavorare da casa per sempre.

Per far sì che le nuove tecnologie rappresentino un fattore di progresso, e non di regressione sociale, valorizzando, invece di comprimere, le libertà affermate sul terreno gius-lavoristico, è assolutamente

[52] L'art. 14 della legge 7 agosto 2015, n. 124, stabilisce che le amministrazioni adottino misure tali da permettere, entro tre anni, ad almeno il 10% delle lavoratrici e dei lavoratori pubblici che lo richiedano di avvalersi delle nuove modalità di lavoro agile, mantenendo in ogni caso inalterate le opportunità di crescita e di carriera per questi lavoratori.
Viene anche precisato che l'adozione di queste misure organizzative e il raggiungimento degli obiettivi descritti costituiscono oggetto di valutazione nell'ambito dei percorsi di misurazione della performance sia organizzativa che individuale all'interno di ogni ente.

indispensabile garantirne la sostenibilità sotto il profilo costituzionale, democratico e la conformità ad alcuni principi irrinunciabili. Pertanto, il ricorso alle tecnologie ICT per rendere la prestazione lavorativa non deve essere l'occasione per il monitoraggio sistematico e ubiquitario del lavoratore, ma deve avvenire nel rigoroso rispetto delle disposizioni contemplate nello Statuto dei lavoratori, a tutela dell'autodeterminazione del lavoratore, che presuppone un'adeguata formazione e informazione di quest'ultimo. Ponendo in particolare risalto il vincolo finalistico all'attività lavorativa che legittima l'esenzione dalla procedura concertativa o autorizzativa circa gli eventuali controlli mediante strumenti utilizzati per rendere la prestazione lavorativa.

Dopo svariati interventi del Governo, nel corso degli ultimi due anni, riguardanti lo *smart working*, con il decreto legge "Proroghe" del 30 aprile 2021 (G.U. Serie Generale n.103 del 30-04-2021) è stata cancellata la soglia minima del 50% per lo *smart working* nella pubblica amministrazione. Fino alla definizione della disciplina del lavoro agile nei contratti collettivi del pubblico impiego, e comunque non oltre il 31 dicembre 2021, le amministrazioni pubbliche potranno continuare a ricorrere alle modalità semplificate relative al lavoro agile, ma sono liberate da ogni rigidità. Al riguardo, il ministro per la pubblica amministrazione, Renato Brunetta, ha precisato: "Facciamo tesoro della sperimentazione indotta dalla pandemia e del prezioso lavoro svolto dalla ministra Dadone - sottolinea il ministro - per introdurre da un lato la flessibilità coerente con la fase di riavvio delle attività produttive e commerciali che stiamo vivendo e dall'altro lato la piena autonomia organizzativa degli uffici. Fino a dicembre le amministrazioni potranno ricorrere allo *smart working* a condizione che assicurino la regolarità, la continuità e l'efficienza dei servizi rivolti a cittadini e imprese. Un percorso di ritorno alla normalità, in piena sicurezza, concordato con il Comitato tecnico-scientifico e compatibile con le esigenze del sistema dei trasporti". A regime, dall'inizio del 2022, la norma conferma l'obbligo per le amministrazioni di adottare i Pola (Piani organizzativi del lavoro agile) entro il 31 gennaio di ogni anno, riducendo però dal 60% al 15%, per le attività che possono essere svolte in modalità agile, la quota minima dei dipendenti che potrà avvalersi dello smart working. Il "decreto proroghe", come sintetizzato in una nota del Ministro per la Pubblica Amministrazione, prevede che: il lavoro agile non sia più ancorato a una percentuale (soglia del 50% prima prevista), ma al rispetto di principi di efficienza, efficacia e *customer satisfaction*; sia mantenuto inalterato il necessario rispetto delle misure di contenimento del fenomeno epidemiologico e della tutela della salute adottate dalle autorità competenti; si proceda al rinvio alla contrattazione collettiva circa la definizione degli istituti del lavoro agile, ma ne consente fino al 31 dicembre 2021 l'accesso attraverso le modalità semplificate di cui all'art. 87 del decreto legge n. 18 del 2020 (quindi senza la necessità del previo accordo individuale e senza gli oneri informativi a carico della parte datoriale). In caso di mancata adozione del Pola, il lavoro agile sarà svolto da almeno il 15% del personale che ne faccia richiesta. Inoltre, consente implicitamente alle amministrazioni che entro il 31 gennaio 2021 avranno adottato il Pola, con le percentuali previste a legislazione allora vigente, di modificare il piano alla luce della disciplina sopravvenuta. Con Decreto del Presidente del Consiglio dei Ministri del 23 settembre 2021 viene stabilito che dal 15 ottobre 2021 la modalità ordinaria di svolgimento della prestazione lavorativa nella pubblica amministrazione torna ad essere quella in presenza. Si torna, pertanto, al regime previgente all'epidemia pandemica, disciplinato dalla legge 22 maggio 2017, n. 81, recante "Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato" (la legge Madia), così come modificata dai successivi provvedimenti normativi. Spetterà alle singole amministrazioni definire l'organizzazione degli uffici. Nel frattempo, sono in corso le trattative per i rinnovi dei contratti pubblici, che garantiranno, una volta concluse, una regolazione puntuale dello *smart working*. Il Piano integrato della pubblica amministrazione (PIAO, introdotto dal decreto legge 80/2021) assorbirà i contenuti dei Piani organizzativi del lavoro agile (POLA) e rappresenterà per tutte le pubbliche amministrazioni, a partire dal 31 gennaio 2022, uno strumento di semplificazione e di pianificazione delle attività e delle strategie da attuare. Le premesse per il DPCM del 23

settembre 2021 – che mette quindi la parola "fine" all'utilizzo del lavoro agile quale strumento di contrasto al fenomeno epidemiologico e stabilisce che, a decorrere dal 15 ottobre 2021, la modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni è soltanto quella svolta in presenza – sono state poste dal decreto legge 21 settembre 2021, n. 127, con cui il Governo ha esteso a tutto il personale delle pubbliche amministrazioni l'obbligo di possedere e di esibire, per l'accesso al luogo di lavoro, la certificazione verde COVID-19 (il c.d. *green pass*).

Con il decreto legge dell'8 ottobre 2021, n. 139, in attuazione delle disposizioni contenute nel DPCM del 23 settembre 2021, sono state indicate le modalità organizzative per gestire il rientro in presenza del personale dipendente a partire dal 15 ottobre 2021. Il decreto stabilisce che ciascun ufficio è tenuto ad adottare le misure organizzative necessarie per consentire il graduale rientro in sede di tutto il personale in servizio a decorrere dal 15 ottobre ed entro il 31 ottobre, assicurando, da subito la presenza in servizio dei dipendenti preposti alle attività di sportello e ricevimento degli utenti (front office) e di quelli assegnati ai settori preposti all'erogazione di servizi all'utenza (back office), anche attraverso la flessibilità degli orari di sportello e di ricevimento, flessibilità da definirsi previa intesa con le organizzazioni sindacali. L'art. 1, comma 3, del decreto 8 ottobre 2021, nel precisare che "il lavoro agile non è più una modalità ordinaria di svolgimento della prestazione lavorativa", ha disposto, "nelle more della definizione degli istituti del rapporto di lavoro connessi al lavoro agile da parte della contrattazione collettiva e della definizione delle modalità e degli obiettivi del lavoro agile da definirsi (…) nell'ambito del Piano integrato di attività e organizzazione (PIAO)", che l'accesso al lavoro agile possa essere comunque autorizzato nel rispetto di alcune condizioni: "a) lo svolgimento della prestazione di lavoro in modalità agile non deve in alcun modo pregiudicare o ridurre la fruizione dei servizi a favore degli utenti; b) l'amministrazione deve garantire un'adeguata rotazione del personale che può prestare lavoro in modalità agile, dovendo essere prevalente, per ciascun lavoratore, l'esecuzione della prestazione in presenza; c) l'amministrazione mette in atto ogni adempimento al fine di dotarsi di una piattaforma digitale o di un *cloud* o comunque di strumenti tecnologici idonei a garantire la più assoluta riservatezza dei dati e delle informazioni che vengono trattate dal lavoratore nello svolgimento della prestazione in modalità agile; d) l'amministrazione deve aver previsto un piano di smaltimento del lavoro arretrato, ove sia stato accumulato; e) l'amministrazione, inoltre, mette in atto ogni adempimento al fine di fornire al personale dipendente apparati digitali e tecnologici adeguati alla prestazione di lavoro richiesta; f) l'accordo individuale di cui all'art. 18, comma 1, della legge 22 maggio 2017, n. 81, deve definire, almeno: 1) gli specifici obiettivi della prestazione resa in modalità agile; 2) le modalità e i tempi di esecuzione della prestazione e della disconnessione del lavoratore dagli apparati di lavoro, nonché eventuali fasce di contattabilità; 3) le modalità e i criteri di misurazione della prestazione medesima, anche ai fini del proseguimento della modalità della prestazione lavorativa in modalità agile; g) le amministrazioni assicurano il prevalente svolgimento in presenza della prestazione lavorativa dei soggetti titolari di funzioni di coordinamento e controllo, dei dirigenti e dei responsabili dei procedimenti amministrativi; h) le amministrazioni prevedono, ove le misure di carattere sanitario lo richiedano, la rotazione del personale impiegato in presenza, nel rispetto di quanto stabilito dal presente articolo. Al riguardo, il Ministro per la Pubblica amministrazione, il 31 novembre 2021, ha pubblicato lo schema di "Linee guida per *lo smart working* nella Pubblica amministrazione", che anticipano ciò che sarà definito entro l'anno nei contratti di lavoro.

Il 24 marzo 2022 il Governo ha adottato il decreto legge n. 24 (c.d. decreto riaperture), recante "Misure urgenti per il superamento delle misure di contrasto alla diffusione dell'epidemia da COVID-19, in conseguenza della cessazione dello stato di emergenza". Il provvedimento governativo stabilisce, con decorrenza 1° aprile 2022, la cessazione dello stato di emergenza da Covid-19 e introduce misure per il graduale ritorno alla normalità in tutti i settori. Ritorno alla normalità significa l'obbligo per le amministrazioni pubbliche di rispettare la disciplina dettata dalla legge n. 81/2017.

Il decreto legge 80/2021 all'art. 6, comma 6, (convertito dalla legge 6 agosto 2021, n. 113) introduce il nuovo "Piano Unico" della

Pubblica Amministrazione, il "Piano Integrato di Attività e Organizzazione", che deve accorpare, tra gli altri, i piani della performance, del lavoro agile, della parità di genere, dell'anticorruzione. I POLA confluiranno quindi in questo nuovo Piano unico, che avrà durata triennale con aggiornamento annuale e dovrà essere pubblicato dalle amministrazioni entro il 31 dicembre di ogni anno.

L'emergenza sanitaria, determinata dalla pandemia da Sars-CoV-2, è stata per lo *smart working* un importante trampolino di lancio nel nostro Paese[53]; anche se questo innovativo istituto è stato introdotto dal legislatore a partire dal 2017, per lungo tempo esso ha rappresentato uno strumento di nicchia. Nel corso dell'esplosione della pandemia, il ricorso allo strumento dello *smart working* ha garantito la continuità operativa del Paese e, al termine dello stato emergenziale, il c.d. lavoro agile potrebbe imporsi come soluzione funzionale e stabile a un nuovo e più sostenibile equilibrio socio-economico. Se lo stato di emergenza ha permesso al lavoro agile di farsi conoscere ai tanti che ne ignoravano l'esistenza e le potenzialità, ha anche temporaneamente mutato l'istituto sia nella forma (rendendolo semplificato), sia nelle finalità (rendendolo strumento anti-contagio). Nella succitata normativa si ribadisce, anche per la pubblica amministrazione, la centrale importanza nello *smart working* della fissazione degli obiettivi e della valutazione delle performance e dei risultati raggiunti. Con l'istituto in questione si passa dalla misurazione del tempo lavorativo e della presenza in ufficio alla valutazione dei risultati raggiunti.

La legge n. 81/2017, come già ricordato, ha introdotto per la prima volta in Italia una formale regolamentazione del fenomeno dello *smart working*: modalità di esecuzione del rapporto di lavoro subordinato volta a "agevolare la conciliazione dei tempi di vita e di lavoro" e in virtù della quale le prestazioni possono essere rese "in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale" (art. 18, comma 1). Tuttavia, il quadro normativo di riferimento è generale: da un lato non fornisce alcuna prescrizione in materia di protezione dei dati personali, limitandosi (all'art. 21) a un rinvio alle previsioni di cui all'art. 4 Statuto dei Lavoratori e, dall'altro rimanda a un accordo fra le parti la disciplina degli aspetti più rilevanti. Mutando le condizioni logistiche e strumentali della prestazione lavorativa occorre tener conto che cambia necessariamente anche il contesto in cui occorre garantire la protezione dei dati. Per tale motivo, all'improvvisazione iniziale occorre, ora, dare spazio alle regole.

La normativa in materia di protezione dei dati personali non può essere vista come un ostacolo, essa, infatti, presenta istituti di flessibilità per eventi eccezionali, senza che ciò comporti la sospensione dei diritti civili. L'unica nazione europea che ha sospeso, in nome dell'epidemia i diritti dell'interessato (artt. 15-22 del RGPD) è stata l'Ungheria. La pandemia può, infatti, rappresentare il pretesto per introdurre e rafforzare forme di autoritarismo. "Que la pandemia no sea un pretexto para el autoritarismo", che la pandemia non sia un pretesto per l'autoritarismo. Questo è il titolo del "Manifesto", che vede come primo firmatario il premio Nobel per la letteratura Mario Vargas Llosa, pubblicato sul sito della sua Fundación Internacional para la Libertad (FIL)[54]. "Su entrambe le sponde dell'Atlantico - si legge ancora nel documento - risorgono lo statalismo, l'interventismo e il populismo con un impeto che fa pensare a un cambio di modello lontano dalla democrazia liberale e dall'economia di mercato".

Riuscire a conciliare lo *smart working* con la protezione dei dati personali dei lavoratori e con la sicurezza dei dati trattati fuori dalla sede di lavoro sarà una delle sfide dei prossimi anni. La modalità semplificata di ricorso al lavoro agile, senza l'accordo individuale con i lavoratori, più volte oggetto di proroga, va inserita nell'ambito di una cornice normativa più chiara e certa. Nel corso di questi anni sono stati presentati diversi disegni di legge collegati, in particolare, alla manovra di bilancio per il 2021; tra i tanti, segnalo il disegno intitolato "Disposizioni in materia di lavoro agile nelle pubbliche amministrazioni", tra i punti centrali di questo dovrebbero esserci il diritto del lavoratore alla disconnessione e il potenziamento della

[53] Il Ministro per la Pubblica Amministrazione, con il D.M. 4 novembre 2020, ha anche istituito l'Osservatorio nazionale del lavoro agile nelle amministrazioni pubbliche.

[54] *https://fundacionfileggeorg/*

formazione digitale dei lavoratori delle amministrazioni pubbliche.

Con il passaggio al digitale del mondo del lavoro, le occasioni di controllo a distanza dei lavoratori crescono notevolmente. Ogni nuova tecnologia ICT agevola l'attività lavorativa, ma cela alcuni rilevanti problemi applicativi, nascenti dall'art. 4 dello Statuto dei lavoratori[55].

Il predetto articolo pone dei paletti precisi per l'uso delle nuove tecnologie. La norma vieta l'uso di ogni strumento che consenta il controllo a distanza dei lavoratori, facendo limitate eccezioni per gli "strumenti di lavoro" e gli apparecchi il cui utilizzo sia stato autorizzato da un accordo sindacale o, in assenza, da un provvedimento dell'Ispettorato del lavoro. In questa visione, molti degli strumenti utilizzati dal lavoratore rischiano di entrare in conflitto con il dettato normativo. I limiti che lo Statuto dei lavoratori ha posto al potere organizzativo e, soprattutto, disciplinare del datore di lavoro sono notevoli. Lo scopo, anche dopo la riforma, è quello di salvaguardare la personalità e la dignità del lavoratore e, quindi, la sua integrità fisica e morale anche all'interno dei luoghi di lavoro in applicazione dei principi costituzionali. Il legislatore del *Jobs act* ha voluto riscrivere l'art. 4 dello Statuto[56], con l'intento di renderlo più vicino alla realtà dell'organizzazione dell'impresa. La novella ha fatto venir meno il principio del divieto assoluto e la storica contrapposizione tra il primo e il secondo comma della vecchia formulazione, che negli ultimi anni aveva alimentato le più ampie interpretazioni da parte della giurisprudenza e del Garante per la protezione dei dati personali. Ciò ha consentito al legislatore l'apertura, contenuta nel comma 2 della nuova norma, di grande rilevanza pratica per gli strumenti tecnologici "mobili" (*pc*, *tablet*, *smartphone*, *Gps*, ecc.) che potranno essere utilizzati dai lavoratori anche senza l'accordo con le Rsa/Rsu ovvero senza autorizzazione amministrativa. Ricorrendo una delle esigenze di controllo previste dallo Statuto, il datore di lavoro potrà monitorare lo *smart worker* tramite gli strumenti di lavoro anche al fine di verificare la sua diligenza nell'adempimento dei propri obblighi, con possibili conseguenze sul piano disciplinare. L'ultimo comma dell'art. 4 dello Statuto prevede che le informazioni ottenute "sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal d.lgs. 30 giugno 2003, n. 196", e oggi ancor più alla luce del Regolamento (UE) 2016/679 (*Regolamento Generale sulla Protezione dei Dati* - RGPD). In caso di omissione dell'informativa, il datore di lavoro non solo viola la disciplina in materia di protezione dei dati personali, ma rende anche censurabile qualsiasi atto disciplinare venga emanato sulla base delle informazioni raccolte tramite controllo a distanza.

Il datore di lavoro non può, però, monitorare sistematicamente l'attività del lavoro, il Garante già con le Linee guida del 1° marzo 2007[57] aveva ribadito come l'accesso indiscriminato agli strumenti in dotazione al personale rappresenti un illecito. Il Garante riconosce la facoltà del datore di verificare l'esatto adempimento della prestazione professionale e il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, purché ciò avvenga nel rispetto della libertà e della dignità dei lavorati oggetto di controllo, nonché, in particolare, in ossequio della normativa in materia di protezione dei dati personali. Il Garante (con il provvedimento n. 303/2016) aveva affermato che il ricorso a programmi che operano in *background*, come tali non percepibili dai lavoratori, che permettano una verifica costante e indiscriminata degli accessi degli utenti alla rete e all'e-mail fossero in contrasto con il Codice in materia di protezione dei dati personali e con lo Statuto dei lavoratori. Sempre il Garante, con il provvedimento 547/2016) ribadiva che le modifiche introdotte dal *Jobs act* non permettevano comunque

[55] A. Bellavista, *Il controllo sui lavoratori*, Torino, Giappichelli, 1995.

[56] A. Bellavista, *Il nuovo art. 4 dello Statuto dei lavoratori*, in G. Zilio Grandi e M. Biasi (a cura di), *Commentario breve alla riforma "Jobs Act"*, Padova, Wolters Kluwer, 2016, 717 ss.; E. Barraco, S. Iacobucci, *Strumenti di lavoro e controllo a distanza*, in *Diritto e pratica del lavoro*, 2018, 1942 ss.; M.T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.lgs. 151/2015): spunti per un dibattito*, in *Labour & Law Issues*, 2016, 1 ss.; A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *Rivista italiana di diritto del lavoro*, 2016, 513 ss.

[57] Garante per la protezione dei dati personali, *Lavoro: le linee guida del Garante per posta elettronica e internet*, 1 marzo 2007, in www.garanteprivacy.it, doc. web n. 1387522.

l'effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore.

Qualora legittimi nell'ambito della disciplina lavoristica, i controlli devono avvenire nel rispetto dei principi di trasparenza, minimizzazione, proporzionalità e progressività nel trattamento, così come previsto dall'art. 5 del RGPD.

Con il parere dell'8 giugno 2017, il Gruppo di lavoro ex art. 29 ("WP29"), ora Comitato europeo per la protezione dei dati, si è pronunciato in merito al trattamento dei dati personali dei lavoratori, integrando quanto già previsto in passato con il Parere n. 8/2001 ("Parere sul trattamento di dati personali nell'ambito dei rapporti di lavoro") ed il "Documento di lavoro sulla sorveglianza delle comunicazioni elettroniche sul luogo di lavoro" del 2002.

Come precisato dal WP29, tale nuovo parere è finalizzato ad aggiornare le regole per il trattamento dei dati personali dei lavoratori alla luce dell'evoluzione delle tecnologie informatiche (es.: sistemi per il controllo del lavoro da remoto, geolocalizzazione, *Data Loss Prevention*) nonché alla piena operatività del Regolamento UE n. 2016/679.

Nel documento in esame il WP29 ha, dapprima, ricordato che nell'effettuare il trattamento di tale tipologia di dati personali i datori di lavoro devono tenere ben presenti i diritti fondamentali dei lavoratori, ivi incluso il diritto alla loro riservatezza e, successivamente, individuato le basi giuridiche di tale trattamento, precisando che queste ultime possono ravvisarsi, alternativamente: nell'esecuzione di obblighi derivanti da un contratto di lavoro, ove presente (es.: finalità retributive - ai sensi dell'art. 6.1, lett. b) del GDPR); nell'adempimento di obbligazioni previste dalla legge (es.: calcolo della ritenuta d'imposta - ex art. 6.1, lett. c) del GDPR); nell'interesse legittimo del datore di lavoro (es.: prevenzione della perdita di materiali aziendali e/o miglioramento della produttività dei lavoratori - ex art. 6.1, lett. f) del GDPR).

Il WP29, invece, esclude dalle basi giuridiche del trattamento dei dati personali dei lavoratori il mero consenso di questi ultimi in quanto, a causa del rapporto di "dipendenza", e quindi di debolezza, nei confronti del datore di lavoro, lo stesso consenso non potrebbe mai ritenersi liberamente prestato né, per le stesse ragioni, liberamente revocabile.

Con particolare riferimento all'interesse legittimo del datore di lavoro, poi, il WP29 ricorda a ciascun datore di lavoro di valutare preventivamente se il trattamento da porre in essere sia necessario e proporzionato per il perseguimento di una finalità legittima, nonché di mettere in atto idonee misure di sicurezza dirette a bilanciare tale finalità con i diritti e le libertà fondamentali dei lavoratori, redigendo, se necessario, anche una valutazione di impatto del trattamento ai sensi dell'art. 35 del RGPD.

Il WP29 consiglia ai datori di lavoro specifiche misure di sicurezza idonee a prevenire eventuali violazioni della riservatezza degli interessati, tra cui, ad esempio, l'esclusione delle cd. "aree sensibili" (ospedali o luoghi religiosi) dalle zone sottoposte a monitoraggio, il divieto di monitoraggio delle cartelle/dei file e/o delle comunicazioni personali dei dipendenti e/o, ancora, la previsione di un monitoraggio "a campione", rispetto ad una sorveglianza continuata nel tempo (Al riguardo, Garante, provvedimento 24 maggio 2017, n. 24, in www.garanteprivacy.it, doc. web n. 6495708).

Il WP29 ricorda, inoltre, che nel caso in cui il trattamento dei dati dei lavoratori si fondi sull'interesse legittimo del titolare, quest'ultimo è sempre tenuto a garantire agli interessati il diritto di opporsi al trattamento, esercitando l'omonimo diritto loro conferito dall'art. 21 del GDPR.

Mediante il suddetto parere, il WP29 ha individuato 9 scenari tipici di trattamento di dati personali dei lavoratori - per lo più basati su un interesse legittimo del titolare del trattamento - che possono presentare dei rischi per i diritti e le libertà fondamentali di questi ultimi. Per ognuno di tali scenari, il WP29 ha inoltre rammentato che il datore di lavoro deve procedere, nel rispetto dei principi di "privacy by design" e "privacy by default" previsti dal RGPD, alla previa individuazione della base giuridica del trattamento, alla verifica della necessità delle operazioni di trattamento e all'esame della correttezza e proporzionalità dello stesso rispetto alle finalità perseguite: 1) Trattamento dei dati dei candidati presenti sui *social network*; 2) Trattamento dei dati dei lavoratori presenti sui social network; 3) Monitoraggio della strumentazione informatica dei lavoratori; 4) *Mobile Device Management*; 5) *Wearable*

Devices; 6) Rilevazione della presenza dei lavoratori; 7) Trattamenti di dati mediante sistemi di videosorveglianza; 8) Geolocalizzazione dei veicoli; 9) Trasferimento dei dati personali dei lavoratori a terzi.

Mediante il predetto parere il WP29 ha introdotto, alla luce delle nuove tecnologie informatiche ICT e della nuova disciplina introdotta dal GDPR, delle specifiche regole per il trattamento dei dati dei lavoratori.

Tali disposizioni rappresentano un punto di riferimento di particolare importanza per i datori di lavoro che intendono trattare i dati personali dei propri lavoratori, in quanto, da un lato, definiscono le basi giuridiche di tale tipologia di trattamento e, dall'altro, tramite esempi pratici, approfondiscono il generico concetto di "legittimo interesse" del titolare, così come previsto dall'art. 6.1 lett. f) del RGPD. Il parere, inoltre, ricorda ai datori di lavoro di adottare sempre, nel rispetto del principio di "*accountability*" (responsabilizzazione) previsto dal RGPD (in particolare, art. 24), misure preventive volte alla protezione della riservatezza dei lavoratori redigendo, se del caso, anche una valutazione di impatto del trattamento che abbia ad oggetto il bilanciamento tra il proprio legittimo interesse e l'impatto delle nuove tecnologie informatiche utilizzate sui diritti e le libertà fondamentali degli interessati.

Diversi, come già rilevato, sono gli strumenti che potrebbero entrare potenzialmente in conflitto con l'art. 4 dello Statuto. Si pensi, ad esempio, all'utilizzo della video chiamata, diventata il mezzo più comune di gestione della prestazione lavorativa per chi opera in regime di *smart working*. Secondo il succitato art. 4, l'uso può essere lecito sole se questa è fatta rientrare nella nozione di "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", unica categoria per la quale non è richiesta la stipula dell'accordo sindacale o una procedura alternativa di autorizzazione amministrativa. Sul punto, le Autorità di controllo hanno manifestato un approccio più restrittivo alla nozione di strumenti di lavoro. Altro sistema che suscita diffuse perplessità e che ha forti potenzialità di controllo è il meccanismo che avvisa con una sorta di "semaforo" verde, giallo o rosso sulla presenza davanti al pc e sul collegamento alla rete aziendale di un lavoratore. Anche questo programma è di uso comune, ma può entrare in conflitto con l'impianto dell'art. 4, poiché indubbiamente genera un controllo a distanza. In tali casi, occorrerà l'accordo sindacale o l'autorizzazione amministrativa, e sarà necessario valutare la legittimità del trattamento, che non deve tradursi in una forma di monitoraggio, nonché fornire al lavoratore l'informativa, ai sensi dell'art. 13 RGPD, ed eseguire una valutazione d'impatto, ai sensi dell'art. 35 RDPD.

Meno questioni sembra creare l'uso delle chat (tipo *Whatsapp*) per scopi lavorativi, per le quali non servirebbero l'accordo sindacale o l'autorizzazione amministrativa, pur trattandosi di uno strumento potenzialmente invasivo, non pare profilarsi quella forma di controllo a distanza previsto dall'art. 4. Tuttavia, andrebbe sconsigliato l'uso delle chat come *Whatsapp* per finalità lavorative, poiché questo comporta la comunicazione e l'eventuale diffusione di dati e/o documenti che il datore di lavoro avrebbe poi difficoltà a controllare.

Sicuramente più problematica è la questione dell'utilizzo delle c.d. *werable technologies* (ad esempio, occhiali con GPS, braccialetti intelligenti, capi di abbigliamento interattivi) che offrono grandi opportunità di migliorare la qualità del lavoro, ma nello stesso tempo generano opportunità di controllo, per le quali non sarebbe facile far rientrare nella nozione di strumenti di lavoro, anche se la valutazione va compiuta caso per caso. In tali casi, oltre all'accordo sindacale o l'autorizzazione amministrativa, sarebbero necessari l'informativa, ai sensi dell'art. 13 RGPD, la valutazione d'impatto ai sensi dell'art. 35 RGPD e un'attenta analisi sulla possibilità di fondare tali trattamenti su basi giuridiche diverse dal consenso.

Il titolare del trattamento deve tener conto che il principio di *accountability* (responsabilizzazione) rappresenta il principio fondamentale del RGPD e si estende a qualsiasi iniziativa o misura intesa a favorire i trattamenti di dati da svolgersi in modalità *smart working*. Ciò significa che il titolare deve adottare comportamenti proattivi che dimostrino la concreta adozione di misure dirette ad assicurare l'applicazione del RGPD. Il titolare deve decidere in piena autonomia le modalità, le garanzie e i limiti del trattamento dei dati, in ossequio alla normativa in materia di protezione dei dati personali. Al riguardo, come previsto dall'art. 24 RGPD, su tali aspetti dovrà lasciare traccia delle proprie

decisioni anche in relazione allo *smart working*. Particolarmente delicata è la questione della sicurezza dei dati trattati mediante lavoro agile, situazione che rischia di legittimare comportamenti che possono mettere a rischio la conformità dell'azienda o della PA alla normativa in materia di protezione dei dati personali, nonché facilitare una cyber attacco con notevoli conseguenze negative sull'operatività della PA o dell'azienda e ingenti danni economici. Il titolare, oltre a predisporre misure tecniche e di sicurezza idonee atte a mitigare i rischi che gravano sulle attività di trattamento, dovrà integrare il registro dei trattamenti con nuovi elementi (trattamenti, banche dati, strumenti, esternalizzazioni, misure di sicurezza) che dovessero riguardare le attività in *smart working*; valutare, ai sensi del RGPD e dello Statuto dei Lavoratori, il potenziale invasivo di eventuali sistemi che consentano il monitoraggio dell'utilizzo degli strumenti e della rete aziendale, eventualmente sottoponendoli a valutazione d'impatto; valutare la necessità di integrare l'informativa ai lavoratori alla luce di eventuali nuovi trattamenti datoriali connessi allo *smart working*; ricalibrare l'ambito di autorizzazione dello *smart worker*, laddove necessario e applicando in maniera maggiormente restrittiva il principio di *need to know*; integrare/riformulare, in funzione del contesto delocalizzato, le istruzioni per la sicurezza dei dati da rendersi allo *smart worker*; avviare specifiche iniziative di formazione per conferire al lavoratore agile gli opportuni strumenti di conoscenza e consapevolezza; verificare che le soluzioni informatiche eventualmente sviluppate internamente, per consentire lo svolgimento del lavoro a distanza, siano conformi ai principi di *privacy by design*/*by default* e garantiscano la sicurezza dei dati ex art. 32 RGPD; verificare la contrattualistica e la conformità al RGPD delle soluzioni o piattaforme fornite da terzi, valutando la necessità/adeguatezza di eventuali *data processing agreement* da sottoscrivere ai sensi dell'art. 28 del RGPD. Le predette attività, in gran parte strettamente connesse tra loro, dovranno essere prodotte adottando una metodologia e un piano di azione dalla logica sincretica e coordinata.

Gli strumenti utilizzati dallo *smart worker* per prestare la propria attività lavorativa consentono una reperibilità e una connessione costante e continua. Ciò rischierebbe di compromettere il bilanciamento tra vita professionale e vita privata che è tra i presupposti dell'istituto del lavoro agile. In tale quadro si inserisce il diritto alla disconnessione, in virtù del quale il prestatore di lavoro deve essere protetto da una potenziale perenne connessione.

La flessibilità oraria e organizzativa, offerta dalle nuove tecnologie ICT in ambito lavorativo, da una parte può rappresentare un'importante opportunità per conciliare vita e lavoro, dall'altra rischia di accentuare il conflitto tra vita privata e vita lavorativa e dar luogo a quel fenomeno definito "time porosity", che indica i confini sfumati tra tempi di vita e tempi di lavoro[58]. La connessione ininterrotta fa sì che il lavoratore possa essere sempre contattato, essendo esposto "a uno stato permanente di allerta reattiva rispetto al soddisfacimento delle richieste datoriali"[59]. In tale contesto, è cominciata a emergere l'esigenza di tutelare la disconnessione, secondo la quale il lavoratore deve essere protetto da una potenziale perenne connessione, ossia una tutela diretta a individuare strumenti e modalità, con i quali lo *smart worker* possa interrompere i contatti, senza che ciò determini ripercussioni sul piano retributivo o venga a incidere sul corretto adempimento della prestazione lavorativa.

Nella legge n. 81/2017, la disconnessione viene riconosciuta, seppur senza fornire una definizione giuridica, all'art. 19, comma 1, il quale prevede che l'accordo sullo *smart working* debba contenere, oltre ai tempi di riposo del lavoratore, anche le "misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro". Nel contesto del diritto alla disconnessione, dunque, il prestatore di lavoro deve, in sostanza, essere libero di disattivare le strumentazioni tecnologiche e le piattaforme informatiche di lavoro. Nell'accordo individuale, sottoscritto dal datore di lavoro e dal lavoratore, devono, quindi, essere previsti i tempi di riposo e le misure tecniche ed organizzative cosicché il lavoratore possa interrompere i collegamenti informatici e disattivare i dispositivi elettronici sulla base

[58] R. Zucaro, *Il diritto alla disconnessione tra interesse collettivo e individuale. Possibili profili di tutela*, in *Law & Labour Issues*, 2019, 1 ss.

[59] D. Poletti, *Il diritto alla disconnessione nel contesto dei "diritti digitali",* in *Responsabilità civile e previdenza*, 2017, 1 ss.

delle prescrizioni ivi inserite. Essendo in presenza di una norma imperativa che necessita dell'eterointegrazione da parte della contrattazione collettiva, successivamente all'entrata in vigore della legge n. 81/207, infatti, il diritto alla disconnessione è stato espressamente disciplinato, nel pubblico, dal CCNL relativo al personale del comparto Istruzione e Ricerca 2016/2018, firmato il 18 aprile 2018. L'art. 22, comma 4, lett. C8), del CCNL in questione rinvia alla contrattazione integrativa la definizione di "criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio al fine di una maggiore conciliazione tra vita lavorativa e familiare (diritto alla disconnessione)".

Il D.M. del Ministro per la Pubblica Amministrazione del 19 ottobre 2020, all'art. 5, ha previsto che: "1. Il lavoro agile si svolge ordinariamente in assenza di precisi vincoli di orario e di luogo di lavoro. 2. In ragione della natura delle attività svolte dal dipendente o di puntuali esigenze organizzative individuate dal dirigente, il lavoro agile può essere organizzato per specifiche fasce di contattabilità. 3. Nei casi di prestazione lavorativa in modalità agile, svolta senza l'individuazione di fasce di contattabilità, al lavoratore sono garantiti i tempi di riposo e la disconnessione dalle strumentazioni tecnologiche di lavoro".

Nel corso di un'audizione in Parlamento, il 13 maggio 2020, il Garante per la protezione dei dati personali ha affermato con forza che è necessario assicurare in "modo più netto" il diritto alla disconnessione per tutelare la distanza tra spazi di vita privata e attività lavorativa ("una delle più antiche conquiste" in fatto di diritti sul lavoro. "Il ricorso alle tecnologie – ha aggiunto il Presidente del Garante – non può rappresentare l'occasione per il monitoraggio sistematico del lavoratore. Deve avvenire nel rispetto delle garanzie sancite dallo Statuto a tutela dell'autodeterminazione del lavoratore che presuppone, anzitutto formazione e informazione del lavoratore sul trattamento a cui i suoi dati saranno soggetti". "Non sarebbe legittimo fornire per lo *smart working* un computer dotato di funzionalità che consentono al datore di lavoro di esercitare un monitoraggio sistematico e pervasivo dell'attività compiuta dal dipendente tramite questo dispositivo". Pertanto, la disconnessione darebbe luogo a un nuovo diritto digitale, che si connoterebbe come un corollario del diritto alla privacy[60], in particolare come "diritto di essere lasciato in pace", come diritto alla tranquillità individuale.

[60] D. Poletti, *Il diritto alla disconnessione*, 17.