Accesso, sicurezza informatica, tutela dei dati personali (e responsabilità)

La base giuridica

La disciplina comunitaria (Regolamento UE 679/2016, apparato normativo *self executing*) e quella nazionale (d.lgs. n. 196/2003) si curano di garantire la tutela dei dati personali, sotto una molteplicità di profili; per coloro che operano all'interno della Pubblica Amministrazione, particolare attenzione viene richiesta sin dal momento di stesura dell'atto (c.d. *privacy by design*) al fine di evitare una **diffusione illecita**, dovendo redigere i testi omettendo di inserire dati personali eccedenti o non pertinenti, in riferimento allo scopo[1], rispettando al contempo di accertare la base giuridica che legittima il trattamento, *ex* art. 6, par. 3, lettera b), del GDPR (*General Data Protection Regulation*), costituita esclusivamente da una norma primaria, *ex* art. 2 *ter*, comma 1 del Codice in materia di protezione dei dati personali.

I dati "particolari" e la loro diffusione

A rafforzare la tutela l'art. 7 *bis*, «*Riutilizzo dei dati pubblicati*», del d.lgs. n. 33/2013, dispone che gli obblighi di pubblicazione dei dati personali diversi dai dati "*sensibili*" e dai dati "*giudiziari*" (quelli previsti del 9 «*Trattamento di categorie particolari di dati personali*» e 10 «*Trattamento dei dati personali relativi a condanne penali e reati*» del GDPR), comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali[2], 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.

Su questo aspetto di "trasparenza", secondo il modello FOIA (*Freedom of Information Act*) dei siti istituzionali, l'ANAC[3] se da una parte, ha rammentato che l'utilizzo di filtri o soluzioni similari che impediscono la ricercabilità e il riutilizzo delle informazioni, è contrario al perseguimento degli obiettivi generali della **trasparenza amministrativa**, invitando gli Organismi Indipendenti di Valutazione, in quanto soggetti competenti ad attestare l'avvenuta pubblicazione dei dati, al puntuale rispetto della normativa anche in materia di apertura dei dati e di indicizzazione delle pagine contenute nella sezione "*Amministrazione trasparente*", dall'altra, ha segnalato, con un ragionamento *a contrario*, che gli obblighi di pubblicazione dei dati personali "*sensibili e giudiziari*" (ora definiti "*particolari*") non possono essere diffusi indistintamente attraverso siti istituzionali, seguendo un trattamento ne impedisce la indicizzazione e la rintracciabilità tramite i motori di ricerca *web* e il loro riutilizzo.

Inoltre, al terzo comma del cit. art. 7 *bis*, viene precisato che la P.A. possa disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non ha l'obbligo di pubblicare o sulla base di specifica previsione di legge o regolamento, nel rispetto dei limiti indicati dall'articolo 5 *bis*, «*Esclusioni e limiti all'accesso civico*» del decreto Trasparenza, «*procedendo alla indicazione in forma anonima dei dati personali eventualmente* presenti».

A completare il quadro normativo sull'accessibilità, nei termini sia del c.d. accesso "*civico semplice*" (*ex* art. 5, comma 1 del d.lgs. n. 33/2013, pubblicazioni obbligatorie) che "*civico generalizzato*" (*ex* art. 5, comma 2, del d.lgs. n. 33/2013, pubblicazioni ulteriori, ovvero dove non vi è un obbligo giuridico di pubblicare) il comma quattro dell'art. 7 *bis* impone a tutte le P.A. – nei casi di pubblicazioni

obbligatorie – di «*rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione*», confermando un obbligo di ridurre all'essenziale i dati da pubblicare.

I divieti di diffusione

Il divieto di pubblicazione (ostensibilità), presente nei successivi commi, se non nei casi previsti dalla legge, si estende:

- alle «*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*» i dati particolari (*ex* sensibili);
- quelli previsti dall'articolo 24, «*Esclusione dal diritto di accesso*», commi 1 e 6, della legge 7 agosto 1990, n. 241;
- i dati di cui all'articolo 9, «*Disposizioni per la tutela del segreto statistico*», del decreto legislativo 6 settembre 1989, n. 322;
- quelli previsti dalla normativa europea in materia di tutela del segreto statistico;
- quelli che siano espressamente qualificati come riservati dalla normativa nazionale ed europea in materia statistica;
- quelli relativi alla diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale[4].

Il quadro di riferimento involge una serie di attività che vanno, *in primis,* dall'esigenza cogente di assumere una serie di misure sulla sicurezza dei dati, individuando le modalità di pubblicazione e i responsabili delle pubblicazioni, onere già previsto nel PNA 2019[5]; dall'altro (e non secondariamente) di apprestare delle soluzioni ICT

(*Information and Communication Technology*) in grado di scongiurare la diffusione accidentale o illecita, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (c.d. *data breach*), nonché accertare che le pubblicazioni (*alias* diffusione *on line* dei dati) permangano il tempo strettamente necessario definito dalla legge (c.d. diritto all'oblio)[6].

Giova rilevare che il danneggiato che lamenti la lesione dell'interesse non patrimoniale all'illecito trattamento dei dati personali può limitarsi a dimostrare l'esistenza del danno e del nesso di causalità rispetto al trattamento illecito, mentre spetta al danneggiante (titolare del trattamento), eventualmente in solido con il responsabile, dimostrare di aver adottato tutte le misure idonee per evitare il danno.

Tale schema è parzialmente confermato dall'art. 82 comma 3, del Regolamento UE 679/2016 che, sulla base del **principio di responsabilizzazione** (*accountability*) addossa al titolare del trattamento dei dati – eventualmente in solido con il responsabile – il rischio tipico d'impresa (*ex* art. 2050 c.c.): il pregiudizio non patrimoniale non è *in re ipsa*, ma deve essere allegato e provato da parte dell'attore, a pena di uno snaturamento delle funzioni della responsabilità aquiliana.

La posizione attorea è, tuttavia, agevolata dal regime più favorevole dell'onere della prova, descritto all'art. 2050 c.c., rispetto alla regola generale del danno aquiliano, nonché dalla possibilità di dimostrare il danno anche solo tramite presunzioni semplici e dal risarcimento secondo equità[7].

Il titolare del trattamento, per non incorrere in responsabilità, deve dimostrare che l'evento dannoso non gli è in alcun modo imputabile e non può limitarsi alla prova

negativa di non aver violato le norme (e, quindi, di essersi conformato ai precetti), ma occorre la prova positiva di aver valutato autonomamente il rischio, purché tipico – cioè prevedibile – e attuato **misure organizzative e di sicurezza** tali da eliminare o ridurre il rischio connesso alla sua attività: l'accertamento del danno non patrimoniale è un accertamento di fatto, rimesso al giudice di merito e resta ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale e al suo essere maturata in un dato contesto temporale e sociale[8].

Serve, in parole diverse, dimostrare di aver adottato tutte le misure di sicurezza che la tecnica e "*le regole d'arte*" consentono, in relazione all'avanzamento dello sviluppo dell'ICT, dando concreta dimostrazione del costante monitoraggio delle più recenti misure.

I termini di pubblicazione

In questo senso, giova rammentare che la pubblicazione di dati personali oltre il tempo previsto dalla legge se può definirsi lecita per la durata *ex lege*, non può ritenersi consentita per un tempo eccedente i termini imposti dalla disposizione, in quanto gli eventuali dati personali (anche afferenti la vita privata, ad es. lo stato di famiglia o una domanda di rateizzazione) non possono ricondursi alle esigenze di trasparenza amministrativa con la permanenza *on line*, costituendo un illecito trattamento sanzionabile.

La scadenza dei termini di pubblicazione impone la rimozione degli atti (compresa l'indicizzazione) quando è presente un dato personale e vige una disciplina specifica sulla visibilità *on line*, differenziando le funzioni della trasparenza del d.lgs. n. 33/2013 rispetto agli altri provvedimenti oggetto di pubblicazione obbligatoria.

Il diritto all'obblio e la deindicizzazione comporta che "*perdurante reperibilità*" sul *web* di contenuti non corretti e

inesatti presenta un impatto "*sproporzionatamente negativo*" sulla sfera privata del titolare del dato, in palese violazione con la disciplina di riferimento, specie in particolare proprio nel trattamento dei dati sulla "*salute*"[9] che è uno dei criteri principali da tenere in considerazione per un corretto **bilanciamento tra diritto all'oblio e diritto/dovere all'informazione** a causa del suo maggiore impatto sulla vita privata, rispetto ai dati personali "*comuni*"[10].

I dati riferiti alla salute non possono essere oggetto di diffusione e la loro ostensione mediante l'accesso civico generalizzato è esclusa, come ad es. la richiesta di conoscere i dati di distribuzione dei casi di COVID-19 registrati da una regione, suddivisi «*per comune, sesso, età, esito (guariti, deceduti, casi attivi), domicilio (al proprio domicilio oppure casa di riposo/microcomunità/RSA), data delle diagnosi di infezione, numero ed esiti dei tamponi eseguiti per paziente*», nonché concernenti «*numero, distribuzione per comune e data dei contatti telefonici della Centrale a ciò deputata con le persone prese in carico per infezione da COVID-19*»: i dati aggregati sono ammissibili mentre i dati personali puntuali suddivisi «*per ogni comune*» presentano un elevato potenziale di pregiudizio che *«il disvelamento di alcune delle informazioni richieste (ad esempio, il domicilio o la data di insorgenza della malattia) potrebbe arrecare alla protezione dei dati personali, appartenenti, per loro natura, alla categoria dei dati particolari, in ragione dell'esiguità demografica che caratterizza molti Comuni…, tale da consentire la verosimile identificazione dei soggetti colpiti dal* virus», donde, ne è preclusa la diffusione[11].

In generale, si può anche affermare che la diffusione di dati personali – in presenza di una popolazione o campione limitato – ben può, mediante il loro incrocio con informazioni verbali facilmente acquisibili, almeno in taluni casi, far risalire all'identità dei soggetti coinvolti e, conseguentemente, al

loro stato di salute (anche le iniziali dei nomi sono insufficienti per garantire l'anonimato)[12].

L'omessa rimozione dei dati oltre i termini leciti di pubblicazione

In termini diversi, l'omessa rimozione dall'albo pretorio *on line*, ma anche dalla *home page* di un sito istituzionale, dei dati personali oltre i termini previsti da una norma di legge (c.d. base giuridica) costituisce una violazione alla disciplina sulla tutela dei dati personali che non è ammissibile, non potendo giustificare tale inadempimento dall'assenza di professionalità interne, né all'inerzia del tecnico esterno incaricato di configurare il sito internet dell'Amministrazione, ovvero dalla mancanza di adeguate misure di sicurezza informatica (*software*), atteso che il titolare del trattamento è la persona giuridica, non il legale rappresentante o l'amministratore, visto che la disciplina deroga al principio della imputabilità personale della sanzione, di cui alla legge n. 689/1981, configurando, nello specifico regime sanzionatorio ivi dettato, un'autonoma responsabilità della persona giuridica (la quale dovrà a sua volta verificare le singole responsabilità).

La responsabilità per la violazione delle norme di sicurezza dei dati

La responsabilità non può ritenersi oggettiva ma, analogamente a quanto previsto dal d.lgs. n. 231/2000 in tema di responsabilità da reato degli enti, va configurata come "*colpa di organizzazione*", da intendersi, in senso normativo, come rimprovero derivante dall'inottemperanza da parte dell'Amministrazione dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione degli illeciti, peraltro attinente alle misure specifiche di sicurezza informatica (comprese di prevenzione della corruzione) per evitare tale genere di rischio[13].

La permanenza nel web di dati personali contenuti nei provvedimenti oltre il termine previsti dalla legge (ad es. art. 124 del d.lgs. n. 267/2000) configura una violazione degli obblighi di pubblicazione laddove non esista un diverso parametro legislativo o regolamentare che preveda la relativa diffusione.

Non può invocarsi efficacia esimente alla circostanza che il ritardo nella rimozione dal sito web dei dati personali possa dipendere da fattori esterni o imprevedibili, ovvero dipesa da una disfunzione degli applicativi informatici gestiti esternamente, visto che tale rischio (probabile e, quindi, prevenibile) risulta pienamente riconducibile alla sfera di signoria dell'Ente e del suo apparato amministrativo/tecnico: sarà indispensabile approntare un corretto ed esaustivo **registro dei rischi** (misure di sicurezza e DPIA, valutazione impatto dei rischi sulla protezione dei dati) in linea con il Piano Triennale per l'informatica della Pubblica Amministrazione e con le indicazioni AGID che, in tale ambito del Piano, definisce la "*sicurezza informatica*" di importanza fondamentale per garantire la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, direttamente collegata ai principi di *privacy* previsti dall'ordinamento giuridico.

Accesso ai curricula

Il Garante privacy[14], con riferimento a un diniego di accesso civico generalizzato alla copia «*dei curricula dei 13 partecipanti alla selezione, mediante proposta di candidatura (avviso pubblico…) per la nomina dell'amministratore unico della società* in house *del Comune*», nonché – ove esistenti – anche la copia, in presenza di un diniego parziale da parte degli interessati, premette che:

- la disciplina stabilisce «*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» (*ex* 5, comma 2, d.lgs. n. 33/2013);

- l'art. 5 *bis* del d.lgs. n. 33/2013 prevede che l'accesso civico debba essere rifiutato, fra l'altro, «*se il diniego è necessario per evitare un pregiudizio concreto alla tutela [della] protezione dei dati personali, in conformità con la disciplina legislativa in materia*»;
- per dato personale si intende «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)» e si considera "identificabile" «la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*» (*ex* 4, par. 1, n. 1, RGPD).
- trattasi di ostensione, tramite l'istituto dell'accesso civico generalizzato, di tutti *curricula* ove non tutti i soggetti controinteressati si sono opposti all'accesso.

Ciò posto, distingue le valutazioni da effettuare in ordine alla possibile ostensione di dati personali (o documenti che li contengono) tramite l'istituto dell'accesso civico rispetto all'accesso documentale, ai sensi della legge n. 241 del 7 agosto 1990, evidenziando che mediante l'accesso civico chiunque ha diritto «*di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7*», sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (*ex* art. 3, comma 1, del d.lgs. n. 33/2013).

Di conseguenza, dovrà essere vagliato il regime di pubblicità con l'eventuale esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati (i titolari dei *curricula*), in base al quale decidere se rifiutare o meno l'accesso ai dati, informazioni o documenti richiesti, rispettando, in ogni caso, i principi del GDPR di «*limitazione della finalità*» e di «*minimizzazione dei dati*», in base ai quali i dati personali devono essere «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*», nonché «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*» (*ex* art. 5, par. 1, lett. b e c).

Se coloro che vengono nominati, ai sensi 14, commi 1, lett. b, e 1 *bis*, del d.lgs. n. 33/2013, vedono obbligatoriamente pubblicato il loro *curriculum vitae*, diversa questione è con riferimento ai partecipanti all'avviso non nominati (ossia, coloro che hanno solo presentato la candidatura, ma non sono stati selezionati per l'incarico societario).

Quest'ultimi possono ricevere un pregiudizio (*ex* art. 5 *bis*, comma 2, lett. a), del d.lgs. n. 33/2013) dai dati personali contenuti (ad es. esperienze e competenze professionali, istruzione e formazione, competenze personali, competenze comunicative, competenze organizzative e gestionali, pubblicazioni, presentazioni, progetti, conferenze, seminari, riconoscimenti e premi, appartenenza a gruppi/associazioni, referenze, menzioni, corsi, certificazioni, ecc.) atteso che non sempre si desidera portare a conoscenza di soggetti estranei in relazione ai casi e al contesto in cui possono essere utilizzati da terzi: l'accesso civico generalizzato non opera per coloro che hanno presentato la candidatura ad amministratore unico di una società *in house* ma non sono stati scelti per l'incarico.

In termini diversi, la diffusione mediante l'accesso ai *curricula* «*potrebbe determinare un'interferenza ingiustificata*

e sproporzionata nei diritti e libertà dei soggetti controinteressati, arrecando a questi ultimi proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5 bis*, comma 2, lett. a), del d. lgs. n. 33/2013 (art. 5, par. 1, lett. b e c, del RGPD)*»: tali operano per tutti, anche per coloro che non hanno presentato opposizione all'accesso civico[15].

Sanzionata la diffusione di dati personali

Il **Garante per la protezione dei dati personali**[16] interviene **censurando una P.A.** (nello specifico un'Azienda Ospedaliera) con la **sanzione amministrativa pecuniaria** di euro 80.000,00 (ottantamila) **a seguito di una segnalazione** con la quale si lamentava la diffusione incontrollata di dati personali di candidati a un concorso pubblico (c.d. *data breach*): in particolare: «*è stato rappresentato che accedendo all'URL http://… era possibile visualizzare un elenco di codici alfanumerici, corrispondenti al "codice iscrizione" dei candidati a uno specifico concorso (XX). A ciascuno di tali codici era associato un collegamento ipertestuale che permetteva l'accesso a un'area del portale nella quale erano contenuti alcuni documenti presentati dai candidati a integrazione della domanda di partecipazione al concorso. Digitando i codici nelle caselle di inserimento dei dati presenti nella pagina accessibile all'URL http://…, era consentito l'accesso a una maschera nella quale erano riportati i dati inseriti dai candidati con la possibilità di modificarli (cfr., segnalazione e relazione di servizio del XX). Attraverso l'URL http://…, era possibile visualizzare, inoltre, ulteriori documenti allegati dagli stessi candidati, contenenti anche dati relativi alla salute (es. titoli di preferenza e certificazione medica)*».

In sede istruttoria, si giunge ad acclarare che:

- la piattaforma gestionale utilizzata per l'attuazione dei concorsi apparteneva ad una società affidataria (mediante MEPA) del servizio di gestione della procedura concorsuale *on line*;
- l'affidataria non aveva fornito alcuna attestazione di conformità relativamente ai dati e ai documenti forniti (mancava un'adeguata sicurezza del processo, «*privo di precauzioni di protezione e al cui interno i file erano "conservati in cartelle, denominate con nome e cognome del candidato e il codice assegnato dalla procedura. I file sono resi disponibili in formato PDF non firmato"*»);
- la P.A. sarebbe venuta a conoscenza dell'evento segnalato solo in occasione della nota di richiesta di elementi da parte del Garante *privacy*;
- viene rilevato che il trattamento dei dati personali degli interessati, nelle modalità assunte, è stato effettuato dalla P.A. in violazione del principio di liceità, correttezza e trasparenza (*ex* 5, par. 1, lett. a) del Regolamento UE 679/2016) e dell'art. 13 del Regolamento UE 678/2016 (mancava un'adeguata "*informativa*")[17];
- in violazione dell'art. 28 del GDPR, in quanto la P.A. aveva omesso di regolamentare il rapporto con l'affidataria società mediante un contratto o altro atto giuridico che disciplinasse il trattamento effettuato per suo conto;
- risulta l'assenza di un idoneo presupposto di liceità e in violazione del divieto di diffusione dei dati sulla salute (*ex* 6 par. 1, lett. c) ed e) del GDPR e artt. 2 *ter* e 2 *septies*, comma 8 del Codice in materia di protezione dei dati);
- violazione dell'art. 32 del Regolamento UE 679/2016, per mancata adozione di adeguate misure tecniche e organizzative volte a garantire la riservatezza e l'integrità dei dati personali trattati.

Dall'analisi del provvedimento emerge che:

- «*per cause legate all'imperizia nel trattamento dei dati da parte del fornitore del servizio di cui si è avvalsa l'Azienda ospedaliera per la gestione della procedura, si è verificata una diffusione di dati personali dei candidati al concorso in assenza di idoneo presupposto di liceità*», specie ove si consideri la diffusione ha avuto ad oggetto anche dati relativi alla salute, rispetto ai quali la disciplina in materia di protezione dei dati personali, in ragione della particolare delicatezza di tale categoria di dati, prevede espressamente che "*non possono essere diffusi*" (*ex* 2 *septies*, comma 8 del Codice in materia di protezione dei dati);
- il trattamento, di cui è titolare la P.A., risulta essere stato effettuato «*in violazione degli articoli 5, lett. a), 6 par. 1, lett. c) ed e) del Regolamento e degli artt. 2-ter e 2* septies*, par. 8 del Codice*»;
- sono mancate le adeguate misure di sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (*ex* 5, par. 1, lett. f), del Regolamento UE 679/2016);
- dalla consultazione della sezione "*Amministrazione trasparente*" della P.A. è emerso che sono stati pubblicati numerosi atti e documenti (es. graduatorie, ricorsi amministrativi, deliberazioni) relativi alla medesima procedura concorsuale e contenenti dati personali, anche relativi a categorie particolari e alla salute, dei partecipati al concorso (che sarà oggetto di autonomo rilievo).

La vicenda, esemplare dell'importanza di una valida rete informatica studiata sin dall'origine (in ossequio ai principi di *privacy by design* e *by default*) per evitare una diffusione

dei dati personali non autorizzata, amplifica l'esigenza di garantire la protezione dei dati personali, determinando un elevato livello di precisione e perizia:

- sia nel definire i rapporti con il soggetto gestore, con la sottoscrizione di un contratto nel quale sono definiti gli obblighi e responsabilità in materia, compreso la titolarità del trattamento che la puntuale sicurezza dei dati (c.d. "*accountability*");
- sia nello stabilire concretamente delle misure di sicurezza interne capaci di vigilare sull'attività e monitorare costantemente tutte quelle operazioni di trattamento che possano causare la "*diffusione*" di dati personali, al di fuori dei casi ammessi;
- in presenza di dati riferiti alla salute le garanzie devono essere maggiori, e di conseguenza la struttura tecnologica non può presentare tali carenze (come nel caso di specie).

Proiezioni

La tutela dei dati personali non potrà avvenire se non attraverso una rete internet adeguata e sicura, con l'utilizzo degli strumenti di *Information and Communication Technology* capaci di contenere e anticipare l'evoluzione della tecnica, adeguandosi costantemente alla società digitale e al *cyberspazio*, aumentando le professionalità specifiche nella P.A., senza lasciare alcuna libertà all'improvvisazione (o alla c.d. buona volontà del singolo) ma strutturando le reti con **investimenti adeguati e formazione continua**.

La diffusione dei servizi della società dell'informazione, l'identità digitale (SPID), l'ingresso massiccio dei *social* nelle istituzioni (vedi, le dirette di *Facebook* del Governo in epoca COVID-19)[18] impongono sicuramente la "transizione digitale" della P.A. e lo *smart working*, come forma ordinaria della prestazione da remoto, cambiando i modi di rapportarsi tra cittadino ed istituzioni, compresi i meccanismi

decisionali non in presenza.

Si potrebbe affermare che l'*on line* diviene pervasivo di ogni relazione umana: solo con una rete sicura e con delle misure di sicurezza adeguate si potrà garantire la tutela dei dati personali, limitare ogni traccia digitale, cautelando una "*soglia minima*" di libertà di essere disconnessi, assecondando quella parte di "*riservatezza*" («*to be let alone*», nella sua originaria definizione di diritto a *"a essere lasciato solo*") che ancora è pur sempre possibile.

Note

[1] Cfr. Corte Giustizia Unione Europea, sez. III, 16 gennaio 2019, n. 496/17, ove si stabilisce che ogni trattamento di dati personali deve, da un lato, essere conforme ai principi relativi alla qualità dei dati enunciati all'articolo 6 della direttiva n. 95/46 o all'articolo 5 del Regolamento UE 2016/679 e, dall'altro, rispondere a uno dei principi legittimanti un trattamento dati enumerati all'articolo 7 di detta direttiva o all'articolo 6 di detto regolamento. Più in particolare, i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e risultare adeguati, pertinenti e limitati a quanto è necessario rispetto a tali finalità, mentre il loro trattamento è lecito, secondo l'articolo 7, lettera c), della stessa direttiva o l'articolo 6, paragrafo 1, lettera c), dello stesso Regolamento, se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

[2] Per diffusione s'intende che i dati personali vengano comunicati a più soggetti indeterminati, in qualunque forma, Cass. pen., sez. III, 9 giugno 2006, n. 22059, di converso il reato di trattamento illecito di dati personali non è integrato se il trattamento dei dati avvenga per fini esclusivamente personali, senza una loro diffusione o destinazione a una comunicazione sistematica, Cass. pen., sez. V, 22 ottobre 2008, n. 46454.

[3] ANAC, Comunicato del Presidente, «*Indicazioni in merito alla indicizzazione delle pagine della sezione 'Amministrazione trasparente'*», 1° luglio 2020.

[4] Per i "*dati relativi alla salute*" è previsto un espresso divieto di diffusione, *ex* art. 2 *septies*, comma 8, del d.lgs. n. 196/2003, dove opera anche l'art. 7 *bis*, comma 6, del d.lgs. n. 33/2013, che al riguardo prevede, analogamente, come «*Restano fermi i limiti… alla diffusione dei dati idonei a rivelare lo stato di salute*», Garante per la protezione dei dati personali, «*Parere su una istanza di accesso civico*», doc. *web* n. 9084520, Registro provvedimento n. 2 del 10 gennaio 2019.

[5] ANAC, Delibera n. 1064 del 13 novembre 2019, «*Approvazione in via definitiva del Piano Nazionale Anticorruzione 2019*», dove si prescrive che nei singoli PTPCT (Piani triennali di prevenzione della corruzione e della trasparenza), per regolare il flusso delle informazioni sulla sez. "*Amministrazione Trasparente*", sia essenziale l'indicazione dei nominativi dei soggetti responsabili della trasmissione dei dati, degli uffici tenuti alla individuazione e/o alla elaborazione dei dati, di quelli cui spetta la pubblicazione; nella sez. del PTPCT per ciascun obbligo, sono espressamente indicati i nominativi dei soggetti e gli uffici responsabili di ognuna delle citate attività, in mancanza è ritenuto responsabile il RPCT (Responsabile della prevenzione della corruzione e della trasparenza).

[6] La pubblicazione di un'informazione concernente una persona determinata, a distanza di tempo da fatti e avvenimenti che la riguardano, non può che integrare la violazione del fondamentale diritto all'oblio, Cass., sez. I, 20 marzo 2018, n. 6919.

[7] Cass. civ., sez. I, 8 gennaio 2019, n. 207; 25 gennaio 2017, n. 1931 e 23 maggio 2016, n. 10638.

[8] Cass. civ., sez. I, Ord., 17 settembre 2020, n. 19328.

[9] Sono i dati attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute, *ex* art. 4, par. 1, n. 15; considerando n. 35 del Regolamento UE 679/2016.

[10] Garante per la protezione dei dati personali, «*Diritto all'oblio: cittadini italiani tutelati anche al di fuori dei confini europei. Google dovrà cancellare gli* url *anche dai risultati di ricerca nelle versioni extraeuropee*», Newsletter n. 437 del 26 gennaio 2018.

[11] Garante per la protezione dei dati personali, «*Parere su istanza di accesso civico – 3 settembre 2020*», Registro dei provvedimenti n. 155 del 3 settembre 2020, doc. *web* n. 9461036.

[12] 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*», Registro dei provvedimenti n. 243 del 15 maggio 2014, doc. *web* n. 3134436, dove si evidenzia che «*la prassi seguita da alcune amministrazioni di sostituire il nome e cognome dell'interessato con le sole iniziali è di per sé insufficiente ad anonimizzare i dati personali contenuti negli atti e documenti pubblicati online. Inoltre, il rischio di identificare l'interessato è tanto più probabile quando, fra l'altro, accanto alle iniziali del nome e cognome permangono ulteriori informazioni di contesto che rendono comunque identificabile l'interessato (si pensi, ad esempio, alle informazioni relative alla residenza oppure quando si possiede un doppio nome e/o un doppio cognome)*».

[13] Cass. civ., sez. II, ord. 3 settembre 2020, n. 18292.

[14] Garante per la protezione dei dati personali, «*Parere su istanza di accesso civico – 17 settembre 2020*», registro dei provvedimenti n. 156 del 17 settembre 2020.

[15] Cfr. ANAC, delibera n. 1309 del 28 dicembre 2016, «*Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013. Art. 5- bis, comma 6, del d.lgs. n. 33 del 14/03/2013 recante «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*», nello specifico punto 8.1. «*I limiti derivanti dalla protezione dei dati personali*».

[16] Garante per la protezione dei dati personali, «*Provvedimento del 17 settembre 2020*», Registro dei provvedimenti n. 160 del 17 settembre 2020, doc. *web* n. 9461168.

[17] Cfr. Corte Europea dei Diritti dell'Uomo del 5 settembre 2017, Ricorso n. 61496/08 – Causa Barbulescu c. Romania, spec. n. 140 e Parere 2/2017 sul trattamento dei dati sul posto di lavoro, adottato dal «*Gruppo di lavoro art. 29 per la protezione dei dati*», l'8 giugno 2017.

[18] Vedi LUCCA, *L'arido latrato del nuovo dpcm: la "di(e)ttatura" COVID-19. Riflessioni minime sul senso della misura*, mauriziolucca.com, 17 ottobre 2020.

Articolo a cura di **Maurizio Lucca**

https://www.ictsecuritymagazine.com/articoli/accesso-sicurezza-informatica-tutela-dei-dati-personali-e-responsabilita/