amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 2/2022

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sánchez-Mesa Martínez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Gaetano Natullo, Carmen Pérez González, Marcin Princ, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Il caso "bonus Covid" in favore dei titolari di cariche pubbliche: i rilievi sollevati all'INPS dal Garante per la protezione dati personali

di Filippo Lorè

(Docente a contratto per l'insegnamento - "Trattamento dei dati sensibili" presso l'Università degli studi di Bari "A. Moro")

Sommario

1. Introduzione. — 2. L'istruttoria del Garante per la protezione dati personali. — 3. Conclusioni.

Abstract

This work traces the arguments produced by the Italian Data Protection Authority in the injunction measure issued to INPS, in the context of the "Covid bonus" case paid to subjects with VAT numbers. The Authority's investigation activity mainly focuses on the analysis of the methods through which the anti-fraud assessment work carried out by the Institute was carried out, aimed at ascertaining that, among the applicants for the economic measure, subjects vested with offices were found policies. It is highlighted that for the process of raising awareness of the privacy issue, decisive and further impulses are required, with the primary purpose of guaranteeing the fundamental rights and freedoms of the data subjects.

** Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review.*

ISSN 2036-7821

1. Introduzione.

Come noto, fin dall'entrata in vigore della Direttiva 95/46/CE[1], in ogni Stato dell'Unione risiede una o più autorità pubbliche indipendenti, oggi incaricate, ai sensi dell'art. 51, par. 1, del Regolamento UE 2016/679[2], di sorvegliare l'applicazione della normativa *privacy*, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali, e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Tali «autorità di controllo», indipendenti, dispongono di poteri di indagine, correttivi, autorizzativi e consultivi[3]. Di tal che, in Italia, ai sensi dell'art. 2-*bis* del D.lgs. n. 196/2003, come modificato dal D.lgs. n. 101/2018, a rivestire questo ruolo è il Garante per la protezione dei dati personali, competente ad adottare provvedimenti correttivi e ad irrogare le sanzioni amministrative pecuniarie, ai sensi dell'articolo 83 del medesimo Regolamento[4].

Di recente, suscitando non poco clamore mediatico, il Garante italiano ha dichiarato illecito il trattamento di dati personali effettuato dall'Istituto Nazionale di Previdenza Sociale (INPS) e, di conseguenza, ha ingiunto allo stesso Istituto, a titolo di sanzione, di pagare la somma di trecentomila euro, nonché di cancellare i dati non necessari, trattati in violazione del principio di minimizzazione, e implementare un'adeguata valutazione di impatto sulla protezione dei dati personali. La sanzione è conseguente ad alcune violazioni dell'INPS, commesse nell'ambito degli accertamenti effettuati per verificare la reale spettanza della misura economica, relativa al bonus Covid[5], erogato per i mesi di marzo e aprile 2020 (per i titolari di partita IVA), a favore di soggetti titolari di cariche politiche[6]. Nelle settimane successive all'erogazione di siffatto bonus era, difatti, emerso, da articoli di organi di stampa, che tale misura assistenziale era stata percepita da alcuni deputati e da migliaia di amministratori di Enti locali, inducendo così l'Ufficio dell'Autorità garante ad avviare un'istruttoria sulle attività di monitoraggio, vigilanza e controllo attivate dall'INPS, con il precipuo scopo di accertare che tali operazioni si fossero

[1] DIRETTIVA 95/46/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

[2] REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[3] Cfr. art. 58, Reg. UE 2016/679

[4] Cfr. art. 153, c.1, D.lgs. n. 196/2003

[5] D.l. 17 marzo 2020, n. 18 (convertito, con modificazioni dalla l. 24 aprile 2020, n. 27) e D.l. 19 maggio 2020, n. 34 (convertito, con modificazioni dalla l. 17 luglio 2020, n. 77)

[6] GARANTE, Provvedimento del 25 febbraio 2021, docweb n. 9556958, disponibile all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958

ISSN 2036-7821

espletate in adesione alla rilevante normativa in materia di protezione dei dati personali[7].

Le principali criticità rilevate dall'Autorità di controllo attengono al presunto mancato rispetto dei quattro elementi fondamentali che costituiscono l'architrave del sistema normativo del Reg. UE 2016/679, ovvero i principi di liceità, correttezza e trasparenza del trattamento, di minimizzazione dei dati, nonché di *privacy by design e by default* e di *accountability*.

È utile ricordare che il legislatore europeo, nel 2016, la normativa italiana, poi, con il D.Lgs n. 101/2018, introducono talune novità in materia, al fine, tra gli altri, di tutelare i diritti e delle libertà fondamentali delle persone fisiche. Il predetto Regolamento, risulta essere strumento imprescindibile per garantire che le persone dispongano di un migliore controllo sulle proprie informazioni personali[8] e che tali dati siano trattati per una finalità legittima, lecita, corretta e trasparente[9]. Allo stesso tempo, il legislatore eurounitario spinge per l'affermazione di un cambio di paradigma, basato sul meccanismo di fiducia tra gli *stakeholders*, mediante un approccio basato sul rischio, e sostiene l'adesione ai principi fondamentali, quali, tra gli altri, la tutela della vita privata, fin dalla progettazione e per impostazione predefinita[10]. Si tratta del principio di *privacy by design e by default*, sancito dall'art. 25 del Regolamento[11].

La presente trattazione, mediante i rilievi posti dal Garante per la protezione dei dati personali, si ripropone di scandagliare un principio cardine della legislazione in materia di protezione dei dati personali: l'*accountability* del titolare del trattamento, ossia il soggetto che determina le finalità e i mezzi dello stesso trattamento[12]. L'*accountability*, che si sostanzia nella responsabilizzazione del titolare, affinché quest'ultimo "sia in grado" (*to be able to*) di "rendicontare" (*account*) il rispetto dei

---

[7] F. ANGELI, *Emergenza Covid-19 e protezione dei dati personali*, in ECONOMIA E SOCIETÀ REGIONALE, 2, 2020, Permalink: http://digital.casalini.it/10.3280/ES2020-002014

[8] Per la definizione del diritto alla riservatezza nella giurisprudenza della Corte di Cassazione si rinvia, fra le tante pronunce, a: Cass. Civ., Sez. 1, sentenza 27 maggio 1975, n. 2129; Cass. Civ., Sez. 3, sentenza 9 giugno 1998, n. 5658; Cass. Civ., Sez. 1, sentenza 30 giugno 2001, n. 8889. Sulla tutela dei dati personali, cfr. C. CHIARIELLO, *Il valore costituzionale della Carta di Nizza: un problema ancora aperto anche alla luce della sentenza n. 269/2017 della Corte costituzionale*, in Giurcost.org, fasc. n. 2/2018, 7 marzo 2018, p. 378; CGUE, Sentenza Stauder, 12 novembre 1969 (C-29/69); M. PARPAGLIONI, *La tutela dei dati personali come presupposto logico-giuridico del divieto di discriminazione*, nota a Cass. 11 agosto 2014, n. 17859, RGL, 2015, II, 78.

[9] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo e al Consiglio, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, 25 febbraio 2020

[10] *Ibidem*

[11] F. LORÈ - P. MUSACCHIO, *Cybersecurity* e protezione dei dati personali ai tempi dell'*accountability*: verso un cambio di prospettiva? in *Amministrativ@mente*, n. 1, 2021

[12] R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR*, in Ciberspazio e diritto: rivista internazionale di informatica giuridica, 1/2, 2018, Permalink: http://digital.casalini.it/10.1400/263843 - Permalink: https://doi.org/10.1400/263843

principi della normativa rilevante in materia, impone al titolare l'adozione di misure tecniche e organizzative adeguate per rispettare (ed essere in grado di dimostrarlo) la normativa europea[13], tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone stanziate nello Spazio Economico Europeo[14].
Di recente, a seguito del ricorso dell'INPS, è intervenuta la sentenza n. 4735 / 2022 della XVIII sezione civile del Tribunale di Roma. In essa si afferma che non sarebbe stato violato il principio di *privacy by design e by default* poiché i dati personali trattati sono stati acquisiti da banche dati pubbliche, dunque, l'uso dei dati per finalità di controllo era prevedibile da parte degli interessati, anche alla luce del considerando 47, Regolamento UE 2016/679, secondo cui «[…] l'interessato, al momento e nell'ambito della raccolta dei dati, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine». Inoltre, secondo il Tribunale non sussisteva, per il trattamento eseguito dall'INPS, l'obbligo di svolgere una DPIA.

2. L'istruttoria del Garante per la protezione dati personali.
Ciò evidenziato, è opportuno ricostruire i fatti, con riguardo all'istruttoria avviata dal Garante, nel procedimento *de quo*, dalla quale è emerso che l'Istituto Nazionale Previdenza Sociale, in attuazione del disposto normativo, aveva provveduto ad erogare il "bonus Covid" a favore di tutti i richiedenti, ritenuti in possesso dei requisiti, individuati sulla base di riscontri automatizzati delle informazioni dichiarate dai richiedenti, incrociati con le banche dati detenute dallo stesso Istituto (cc.dd. "controlli di primo livello")[15]. Successivamente, anche a seguito di notizie diramate dagli organi di stampa, la Direzione centrale antifrode, anticorruzione e trasparenza dell'INPS ha avviato dei "controlli di secondo livello", nell'ambito dei quali, «si sono rese necessarie verifiche non realizzabili sulla base dei dati presenti nei soli archivi dell'Istituto per quanto riguarda la posizione dei parlamentari e dei titolari di cariche presso le amministrazioni locali e regionali che percepiscono indennità di mandato, in considerazione della sua natura di reddito assimilato al lavoro dipendente, nonché in ragione della loro peculiare posizione previdenziale»[16].
Mediante l'acquisizione dei dati anagrafici di deputati, amministratori regionali e locali, desumibili dalla lettura degli *open data* presenti nelle pagine *web* della Camera

[13] F. LORÈ - P. MUSACCHIO, *Ibidem*
[14] Cfr. art. 25, Reg. UE 2016/679.
[15] Sul *web scraping*, le banche dati e il riuso delle informazioni, cfr. Cass. Civ., Sez. 1, sentenza 4 febbraio 2016, n. 2196.
[16] GARANTE, Provvedimento del 25 febbraio 2021, docweb n. 9556958, disponibile all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958

ISSN 2036-7821

dei deputati[17] e del Ministero dell'interno[18], l'INPS ha calcolato, in maniera automatizzata, il presunto codice fiscale di tali soggetti[19], ponendolo in raffronto con il codice fiscale effettivo indicato nelle domande presentate dai richiedenti il "bonus Covid", al fine di stabilire se tra i predetti richiedenti vi fossero anche deputati, senatori e soggetti titolari dell'incarico di amministratore regionale o locale. Soltanto successivamente a quanto narrato, il Ministero del lavoro e delle politiche sociali ha reso, all'INPS, un parere in cui confermava che l'erogazione del bonus dovrebbe essere ritenuta incompatibile con le indennità percepite da parlamentari, consiglieri regionali e soggetti con mandati elettorali o incarichi politici. Di tal guisa, l'INPS, come risulta dalle stesse dichiarazioni dell'Istituto, ha operato il raffronto dei dati personali, anteriormente alla fine del mese di maggio 2020, dunque senza aver prima determinato se gli incarichi di parlamentare e di amministratore regionale o locale costituissero una condizione ostativa alla spettanza del "bonus Covid". Lo stesso Istituto, come riferito, ha proceduto alla raccolta di dati personali, attingendo da un *set* di banche dati esterne, detenute e rese fruibili dalla Camera dei deputati e dal Dipartimento per gli affari interni e territoriali del Ministero dell'interno, dalla cui analisi si deduceva l'assenza del codice fiscale degli interessati, ossia tutto ciò che consente di identificare univocamente una persona fisica. Ulteriormente, allo scopo di operare il raffronto con le domande dei richiedenti il bonus, l'INPS ha impiegato nome, cognome, data e luogo di nascita dei soggetti interessati, per ricavarne, in maniera automatizzata, i presunti codici fiscali di ciascuno, in base ai parametri contenuti nel D.M. 12 marzo 1974, n. 2227[20]. Di tal che, l'Istituto eseguiva un lavoro di raffronto dei codici fiscali ricavati con quelli riportati dagli interessati nelle domande presentate per l'erogazione del bonus, potendo, dunque, individuare chi, tra i parlamentari e gli amministratori locali, aveva inoltrato la relativa domanda[21]. Inoltre, dall'istruttoria dell'Autorità garante è emerso, altresì, in violazione dei principi applicabili alle operazioni di trattamento, che «i controlli in argomento

[17] Sito istituzionale della Camera dei Deputati, Camera dei deputati, rivenibile al seguente link: http://dati.camera.it/sparql

[18] Sito istituzionale del Dipartimento per gli affari interni e territoriali del Ministero dell'interno, rinvenibile al seguente link: https://dait.interno.gov.it/elezioni/open-data/amministratori-locali-in-carica

[19] Come prescritto dal Decreto del Ministero delle finanze del 12 marzo 1974, n. 2227.

[20] Pagnanelli, V. 2021. Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali, Rivista italiana di informatica e diritto, 1, 2021, pp. 11-26.

[21] R. PINARDI, S. SCAGLIARINI, *Il 'bonus Covid' in favore dei titolari di cariche pubbliche: quale bilanciamento tra privacy e trasparenza?*, in *Federalismi.it*, 14, 2021, pp. 138-163. Seppur in un momento successivo ai fatti, nota degna di rilievo in ottica di semplificazione dei processi, è il "nuovo" art. 2-ter, comma 1-bis, del novellato Codice privacy, che meglio regolamenta le operazioni di comunicazione e diffusione dei dati personali tra Pubbliche Amministrazioni, "in coerenza al compito svolto o al potere esercitato" dalle stesse, mediante la creazione e la gestione di grandi banche dati e App governative, passando per la digitalizzazione di molti servizi pubblici e assecondando il principio dell'interoperabilità dei sistemi e delle informazioni possedute dalle amministrazioni pubbliche.

ISSN 2036-7821

hanno avuto a oggetto, non solo i dati personali di coloro che hanno effettivamente percepito il bonus Covid, ma anche dei soggetti richiedenti che, a seguito di presentazione della relativa domanda, sono stati esclusi dal riconoscimento dell'indennità, già all'esito dei controlli di primo livello». L'Autorità, nel Provvedimento in commento, statuisce che, se lo scopo dei suddetti controlli, risiedeva nello scongiurare indebite percezioni delle indennità da parte di parlamentari e amministratori locali, allora il trattamento dei dati personali dei richiedenti che erano stati esclusi dall'erogazione del bonus risultava ultroneo e in discontinuità con il principio di limitazione delle finalità[22].

La mancanza di un'adeguata progettazione del trattamento, ad avviso del Garante, è rinvenibile «nell'omissione di idonee misure volte ad attuare, in modo efficace, il Regolamento, e di garantire che, per impostazione predefinita, fossero trattati i soli dati necessari per ogni specifica finalità del trattamento, eliminando così i molteplici profili di rischio probabile per i diritti e le libertà fondamentali degli interessati»[23].

Un primo profilo di violazione contestato all'INPS dal Garante, *de jure condito*, è individuabile nel mancato rispetto del principio di esattezza del dato personale, prescritto nell'art. 5, par. 1, lett. d), Reg. UE 2016/679[24]. A tenore di tale disposizione, i dati personali devono essere esatti e, se necessario, aggiornati, vincolando il titolare del trattamento a porre in essere tutte le misure ragionevoli per cancellare o rettificare, tempestivamente, i dati inesatti, rispetto alle finalità per le quali sono trattati[25]. Nel caso di specie, ad avviso dell'Ufficio dell'Autorità, il calcolo del codice fiscale non era in grado di «assicurare, con assoluta certezza, la qualità dei dati utilizzati per i controlli», poiché esso può comportare errori se attuato sulla base di dati incompleti o non precisi (soggetti con due o più nomi separati o meno da virgola), o in presenza di casi di omocodia, vale a dire fattispecie nelle quali l'Agenzia delle Entrate assegna diversi codici fiscali a interessati che abbiano identico nome, cognome, data e luogo di nascita. L'obbligo di garantire l'esattezza dei dati deve essere colto nel contesto della finalità del trattamento dei dati[26]. Senonché, da

[22] A. CICCIA MESSINA, *Profili di criticità e di invalidità delle norme sanzionatrici del GDPR*, in CIBERSPAZIO E DIRITTO: rivista internazionale di informatica giuridica, 1, 2021, pp. 3-22.

[23] GARANTE, Provvedimento del 25 febbraio 2021, docweb n. 9556958, disponibile all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958

[24] Sul principio di esattezza dei dati cfr. CGUE, C-553/07, College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer, 7 maggio 2009.

[25] S. SCAGLIARINI, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, In CONSULTA ONLINE, 2, 2021, pp. 489-532. A rafforzare tale principio è l'art. 16 dello stesso Regolamento, ancorato alla tutela del *data subjects*, laddove attribuisce all'interessato il diritto di ottenere dal titolare la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo, nonché l'integrazione dei dati personali incompleti.

[26] FRA – AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, CORTE EUROPEA DEI DIRITTI DELL'UOMO (CONSIGLIO D'EUROPA), GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Manuale del diritto europeo in materia di protezione dei dati*, 2018, p. 143

ISSN 2036-7821

tali elementi normativi l'INPS ha tracciato la propria strategia difensiva[27] (nelle quali erroneamente avanzava, quale base giuridica del trattamento, il legittimo interesse in luogo dell'interesse pubblico), affermando, invano, che «la esattezza dei dati richiesta non attiene alla correttezza del dato in sé, ma in relazione alle finalità per le quali sono trattati; e, nel caso di specie, il riscontro dell'esattezza è risultato anche dal confronto dei dati ricavati con i codici fiscali già raccolti dall'Istituto, provenienti direttamente dagli interessati, e riportati nella identità di *log in* inserita per la presentazione delle domande per ottenere il beneficio». In tal senso, l'INPS ha osservato che il trattamento dei dati si è svolto attraverso l'elaborazione automatizzata dei dati riportati nell'open data[28], e secondo le regole del DM 12 marzo 1974, pertanto si possono escludere errori nell'acquisizione e nell' elaborazione degli stessi .

In secondo luogo, l'Autorità ha rilevato la violazione del principio di *accountability*. Come già accennato, tra le nuove prescrizioni del Regolamento UE 2016/679 vi è infatti tale principio, che potrebbe essere tradotto in "responsabilizzazione" del titolare del trattamento[29], poiché egli, ai sensi dell'art. 24[30], «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», misure che includono l'attuazione di politiche adeguate in materia di protezione dei dati[31].

D'altronde, l'art. 5 del medesimo Regolamento, dopo aver elencato i principi del trattamento nel primo paragrafo, stabilisce che il titolare del trattamento è competente per il rispetto del paragrafo 1 e, sotto il profilo meramente sostanziale, in grado di comprovarlo («responsabilizzazione»). Nel caso di specie, il trattamento eseguito dall'INPS non è stato supportato da un'adeguata documentazione atta a

[27] L'art. 6, par. 1, Reg. UE 2016/679, così recita: "il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti".

[28] D. URANIA GALETTA, *Open Government, Open Data e azione amministrativa*, Istituzioni del Federalismo, Rivista di studi giuridici e politici, 3/2019, pp. 663-683.

[29] G. RUSSO – M. POLINI, *I principi di accountability e di effettività nel nuovo regolamento*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali*, 2017, Maggioli editore, Santarcangelo di Romagna, 2017, p. 131

[30] S. FRANCA, *La semplificazione nelle modalità di trattamento dei dati personali da parte della pubblica amministrazione*, in DIRITTO PUBBLICO, Rivista fondata da Andrea Orsi Battaglini, 2/2021, pp. 635-665.

[31] G. RUSSO – M. POLINI, *Ibidem*

ISSN 2036-7821

comprovare quali livelli (apicali) decisionali siano stati coinvolti (tra cui il DPO dell'Istituto), quali valutazioni tecniche siano state effettuate, quali siano le ragioni sottese alle determinazioni assunte e, ancora, quali misure siano state adottate in relazione al trattamento dei dati personali in esame (si pensi alla valutazione di impatto *privacy*). L'INPS, a pare del Garante, oltre ad aver fornito una rappresentazione non propriamente esaustiva degli elementi della vicenda, non è stato «in grado di comprovare le ragioni delle decisioni assunte nell'ambito del complesso trattamento di dati personali effettuato, al fine di dimostrare all'Autorità il rispetto della normativa in materia di protezione dei dati personali, in violazione del principio di responsabilizzazione[32].

Corollario del principio di *accountability* del titolare, pertanto, è costituito dai nodali principi di *privacy by design* e *privacy by default* (protezione dei dati personali fin dalla progettazione e per impostazione predefinita), desumibili dalla lettura dell'art. 25 del Reg. UE 2016/679. Come osservato, infatti, vi è molta *privacy by design* nel principio di *accountability*[33], poiché il titolare è tenuto a procedere costantemente alla valutazione dei rischi del trattamento allo scopo di determinare, adeguatamente, le misure di sicurezza da applicare al trattamento, sì da garantire il rispetto del principio di minimizzazione[34]. Sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso, orbene, il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione[35], volte ad attuare in modo efficace i principi di sicurezza dei dati, la minimizzazione, secondo una evoluzione qualitativa del dato[36], e a integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti fondamentali degli interessati. In questa prospettiva, i principi in esame rivelano la loro utilità, poiché arricchiscono e specificano i caratteri della progettazione del trattamento[37]. Appunto, la valutazione, da parte del Titolare, di questi aspetti in un momento precedente all'avvio delle operazioni di trattamento, fa sì che vengano giustificate le misure adottate (e quelle non adottate), sulla base di una «istruttoria» interna che si snoda dalla progettazione

[32] GARANTE, Provvedimento del 25 febbraio 2021, docweb n. 9556958, disponibile all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958

[33] G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in «*Le Nuove Leggi Civili Commentate*», 1/2017, p. 1 ss., spec. par. 5.1.

[34] Sul principio di minimizzazione dei dati cfr. CGUE, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a. [GC], 8 aprile 2014.

[35] F. PIZZETTI, Intelligenza artificiale, protezione dei dati personali e regolazione, I Diritti nella "rete" della rete, Giappichelli Editore, 2016, pp. 128-132.

[36] G. BELLOMO, *Metodo democratico, partiti politici, nuove tecnologie e basi giuridiche per il trattamento dei dati personali: alcuni spunti di riflessione*, DPCE Online, v. 46, 1, 2021.

[37] B. BORRILLO, *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, Dirittifondamentali.it, 2, 2020, 1-31.

ISSN 2036-7821

sino alla conclusione del trattamento[38]. Di tal guisa, nel Provvedimento in esame, il Garante ha rilevato, oltre alla mancata predeterminazione delle condizioni ostative alla spettanza (o meno) del bonus e al trattamento di dati non necessari, la mancata considerazione, sempre per l'INPS, dei rischi che il trattamento presentava per i diritti e le libertà degli interessati, tra cui non solo quello derivante da possibili inesattezze delle modalità di calcolo del loro codice fiscale, ma anche le ricadute derivanti dal clamore mediatico suscitato sulla vicenda. Ricadute che, fatalmente, hanno investito non soltanto i soggetti richiedenti la misura *de qua*, bensì l'intera categoria degli interessati, composta da deputati e amministratori regionali e locali, molti dei quelli, ricorda l'Autorità, «senza che potessero essere in grado di capire, al momento della domanda, se fossero effettivamente legittimati a chiederlo».

Senonché, il Garante ha ritenuto violate le prescrizioni dell'art. 35 del Reg. UE 2016/679, che impongono, in taluni casi, lo svolgimento di una valutazione di impatto, invero, non condotta dall'INPS, poiché, secondo quanto dichiarato dall'Istituto, nelle interlocuzioni formali intercorse con l'Autorità, nel «mero incrocio di codici fiscali ai fini dell'individuazione di possibili erogazioni indebite» non risultava ravvisabile «alcun rischio elevato per i diritti e le libertà delle persone fisiche», tale da richiedere l'adozione di misure speciali e diverse rispetto a quelle ordinariamente adottate, che prevedono «l'assoluta riservatezza in ordine all'attività ispettiva svolta e ai destinatari della stessa». L'Istituto, facendo erroneamente leva sulla base giuridica del legittimo interesse (non applicabile al comparto pubblico), ha rimarcato l'assunto secondo il quale non ricorre l'elevato rischio per i diritti e le libertà degli interessati, poiché il trattamento dei dati personali avrebbe interessato un numero di soggetti limitati, le operazioni si sarebbero caratterizzate da volume informativo contenuto di informazioni personali, neanche di carattere particolare, reperibili da chiunque. Ancor più, l'INPS, nelle proprie memorie difensive, ha osservato che il trattamento non impedisce agli interessati di esercitare un diritto, ma è soltanto finalizzato alla verifica della sussistenza del requisito per l'erogazione del bonus.

Tuttavia, alla luce dei criteri rivenienti dallo studio delle Linee guida in materia di valutazione d'impatto sulla protezione dei dati[39], il raffronto ha coinvolto "tutti i richiedenti" il bonus Covid, dunque alcuni milioni di persone, venendo così soddisfatto il criterio, tanto discusso, del "trattamento di dati su larga scala"[40].

---

[38] S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi.it*, n. 24, 2017.

[39] WP248 rev.01 (adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018)

[40] G. ZICCARDI, *Il futuro del GDPR tra profilazione, trattamenti automatizzati, marketing e misure di sicurezza, in Società delle tecnologie esponenziali e General Data Protection Regulation: profili critici nella protezione dei dati*, Milano: Ledizioni, 2018 - Permalink: http://digital.casalini.it/4439284

ISSN 2036-7821

Parimenti, ad avviso del Garante, è soddisfatto il criterio della «creazione di corrispondenze o combinazione di insiemi di dati», operazione che, evidentemente, presenta rilevantissimi rischi per i diritti e le libertà degli interessati - soprattutto se il lavoro di raffronto delle banche dati, finalizzato al calcolo del codice fiscale degli interessati, genera, in output, informazioni non esatte. Secondo l'Autorità, dunque, viene in evidenza come l'Istituto di Previdenza, titolare del trattamento, non abbia messo in atto misure tecniche ed organizzative, così come richiesto dal legislatore eurounitario, secondo logiche di *risk based approach*, traducibili nell'implementazione dell'analisi del rischio, atta ad individuare possibili pregiudizi per i diritti fondamentali degli individui. Di tal che, nel caso di specie, l'INPS ha dunque agito inopinatamente, poiché il trattamento comportava un'operazione di raffronto, su larga scala, di dati personali acquisiti anche da banche dati esterne all'Istituto, con i dati relativi ai richiedenti il bonus[41].

A questa violazione, si aggiunge il mancato coinvolgimento del *Data Protection Officer* (anche Responsabile Protezione Dati, RPD)[42], sin dalla fase di progettazione delle predette attività. Con riguardo a questo aspetto, giova ricordare che il Regolamento generale in materia di *data protection* prescrive, in maniera chiara, al titolare, di coinvolgere la suddetta figura, «tempestivamente e adeguatamente», in tutte le questioni riguardanti la protezione dei dati personali[43]. In tal senso, non lascia adito a dubbi nemmeno il Manuale della Commissione Europea per i Responsabili per la protezione dati, laddove sancisce che «dopo aver creato il registro delle attività di trattamento della sua organizzazione, il passo successivo per il RPD consiste nell'eseguire una revisione approfondita di tutte le attività di trattamento dei dati personali registrate, per verificare se soddisfano i requisiti del Regolamento in tutti gli aspetti rilevanti», così da essere in grado di valutare, alla luce delle conclusioni raggiunte, se il trattamento nel suo insieme può essere considerato conforme al principio imperativo di liceità e correttezza. Questa valutazione della conformità al Regolamento, come specifica il predetto Manuale, è «separata e diversa dalla valutazione del rischio»[44]. Il coinvolgimento, sin dalla fase di progettazione, del Responsabile della protezione dati dell'Istituto, avrebbe certamente prodotto

[41] S. TORREGIANI, *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa. Rivista italiana di informatica e diritto*, 3, 2021, pp. 47-65.

[42] C. CICCIA ROMITO, *Il Data Protection Officer in ambito pubblico: il Garante fa chiarezza*, in Quotidiano Giuridico, Ipsoa, 9, 2021, in riferimento al Provvedimento dell'Autorità Garante per la protezione dei dati personali n. 186/2021.

[43] Cfr. Art. 38, par. 1, Reg. UE 2016/679

[44] D. KORFF, M. GEORGES, CON IL CONTRIBUTO DEL GARANTE ITALIANO PER LA PROTEZIONE DEI DATI PERSONALI & DEI PARTNER DEL PROGETTO, Manuale RPD - Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea, versione approvata dalla Commissione, luglio 2019, p. 196. Invero, i principi generali del trattamento, come osservato in dottrina, hanno una valenza che copre ogni aspetto della disciplina e devono essere rispettati, by design e by default, in ogni fase dello sviluppo del trattamento dei dati.

ISSN 2036-7821

quantomeno un controllo sull'applicazione delle "idonee misure", la cui implementazione è imposta al titolare del trattamento, a mente dell'art. 32 del Reg. UE 2016/679, sulla base del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche, con la conseguente, fisiologica, garanzia di un livello di sicurezza, proporzionato al rischio.

Nondimeno, nell'ambito del procedimento *de quo*, l'Autorità, sempre a tutela dei soggetti che ricoprono incarichi di carattere politico, rileva la violazione dei principi di liceità, correttezza e trasparenza, sanciti dall'art. 5, par. 1, lett. a), del Regolamento[45], poiché, secondo i rilievi prodotti dall'Ufficio del Garante, le operazioni di trattamento, componendosi dall'incrocio delle informazioni, rivenienti, come riferito, da fonti differenti e per tutti i richiedenti la misura assistenziale, si sarebbero dovute, proprio in virtù delle diverse cariche ricoperte nello scenario politico italiano, eseguire all'esito della determinazione di regole riferite alla verifica dei criteri di spettanza della misura economica agli interessati, sulla cui sfera giuridica si è inciso mediante l'impossibilità di conoscere, in maniera trasparente, i presupposti della misura assistenziale. L'Istituto, infatti, trasmetteva una richiesta di parere al Ministero del lavoro e delle politiche sociali, in un momento successivo al trattamento, quando ormai l'incrocio dei dati personali era stato già posto in essere[46].

Invero, il principio di correttezza, disciplinando principalmente la relazione tra l'interessato e il titolare del trattamento, impone a quest'ultimo il rispetto di norme etiche o deontologiche, anche non codificate, o l'attuazione di accorgimenti in grado di rendere equilibrate le singole posizioni. Così facendo, il trattamento sarà adeguato alle esigenze degli interessati, oltre lo «stretto dato normativo»[47], e i medesimi saranno «consapevoli». Nondimeno, il principio di correttezza influisce sulla comprensibilità delle operazioni di trattamento (in relazione alle finalità dello stesso), che devono essere conosciute dall'interessato già al momento della raccolta dei suoi dati personali.

Analoghe riflessioni possono essere condotte con riferimento alla violazione del principio di minimizzazione dei dati personali. Infatti, ai sensi dell'art. 5, par. 1, lett. c), del Regolamento, i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Siffatto principio si riflette sull'esigenza di ridurre al minimo il numero dei dati trattati, le tipologie di trattamento, i tempi di conservazione dei dati e, non da ultimo, il numero di interessati coinvolti.

---

[45] Sul principio di autodeterminazione informativa cfr. BUNDESVERFASSUNGSGERICHT, sentenza n. 209, del 15 dicembre 1983. Sul principio di trasparenza del trattamento cfr. Corte EDU, K.H. e a. c. Slovacchia, n. 32881/04, 28 aprile 2009; Corte EDU, Haralambie c. Romania, n. 21737/03, 27 ottobre 2009; CGUE, C-201/14, Smaranda Bara e a. c. Casa Naţională de Asigurări de Sănătate e a., 1° ottobre 2015.

[46] N. BERNARDI (a cura di), *Privacy – Protezione e trattamento dei dati*, IPSOA, Milano, 2020, p. 79.

[47] N. BERNARDI (a cura di), *Ibidem*

ISSN 2036-7821

Nel caso di specie, invece, il Garante ha correttamente fatto emergere come le operazioni di trattamento dati, «deragliate» dai binari della funzione istituzionale, non risultavano mirate ai soli "politici" beneficiari del bonus, bensì a tutti coloro i quali avevano presentato la relativa domanda, frustrando, in tal modo, il principio finalistico, vale a dire accertare l'indebita percezione del bonus da parte di una individuata categoria di interessati.

Ulteriore aspetto, meritevole di riflessione, attiene, invero, alla ripetizione della misura di sostegno al reddito (come riferito, prima con il decreto Cura Italia, poi con il successivo decreto Rilancio), stimabile, in un ammontare complessivo, in una somma maggiore di mille euro, e alla sua collocazione tra gli obblighi di pubblicità, a memoria dell'art. 26, d.lgs n. 33/2013, dalla cui lettura, al comma 4, si evince, nella ricerca del bilanciamento tra esigenze di trasparenza amministrativa e protezione delle informazioni personali, che «è esclusa la pubblicazione dei dati identificativi delle persone fisiche destinatarie dei provvedimenti di cui al presente articolo, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati»[48].

Senonché, occorre evidenziare anche che, durante l'attività ispettiva, il Garante, verificate le richieste, pervenute all'Istituto, mirate all'«ostensione dei documenti e degli elenchi dei dati dei soggetti richiedenti o beneficiari del bonus Covid che rivestono la carica di parlamentare nonché di amministratore regionale o locale», ha diramato puntuali raccomandazioni, invitando gli Uffici dell'INPS a distinguere, preliminarmente, i soggetti titolari di cariche politiche che, seppur a fronte di una richiesta, avevano ottenuto espresso diniego al godimento dell'indennità, da quelli, invece, risultati beneficiari del "bonus Covid". Quanto ai primi, sulla base delle motivazioni suesposte, il Garante evidenziava che tale trattamento, a cura dell'Istituto, si era concretizzato in violazione del principio di minimizzazione del dato, secondo quanto sancito dall'art. 5, par. 1, lett. c, Regolamento, e che, perciò, «i predetti dati – essendo stati trattati in violazione della disciplina rilevante in materia di trattamento dei dati – "non possono essere utilizzati" (art. 2-decies del Codice). Inoltre, come conseguenza della rilevata illiceità è stato ingiunto all'INPS di

[48] A. CORRADO, La "trasparenza" nella legislazione italiana, in M. A. SANDULLI, (a cura di), Codice dell'azione amministrativa, Giuffrè, Milano, 2017, p.1414. La difesa del sistema democratico, in questi ultimi anni, è passata (e questo è un processo in continuo divenire) attraverso una profonda elaborazione giurisprudenziale di leggi, decreti e linee guida che, se da un lato impongono e regolamentano la nitidezza degli atti amministrativi, dall'altro si ergono a baluardo delle libertà fondamentali degli individui. L'accesso del pubblico ai documenti ufficiali, confortato al Considerando 154 al reg. UE 2016/679, e il diritto alla protezione dei dati personali sono due imperativi che, nella loro attuazione, si trasformano in due mere esigenze derivanti dalla tutela della privacy e dall'obbligo della trasparenza della pubblica amministrazione. Il principio di trasparenza dell'azione amministrativa, accanto all'azione consultiva del Garante, rafforzata negli ultimi anni, ha trovato nella recente normativa una concreta ed efficace applicabilità, producendo due effetti benefici, ossia, l'avvicinamento del cittadino alle istituzioni e la creazione di un sistema di prevenzione del fenomeno corruttivo, sempre più incisivo e rigoroso.

ISSN 2036-7821

cancellare i dati personali trattati in violazione del principio di minimizzazione […]. Pertanto, nessuna richiesta di pubblicazione o accesso è possibile per i dati personali riferiti a tali categorie di soggetti».

Quanto alla seconda categoria di soggetti, in ordine agli obblighi di pubblicazione invocati dagli istanti, l'Ufficio dell'Autorità, muovendo i passi dall'art. 2-*ter*, Codice *privacy* novellato, ha rammentato che la disciplina in materia di trasparenza amministrativa non prevede la pubblicazione delle informazioni[49] riferite a soggetti tenuti a restituire somme, indebitamente percepite. Ove, invece, l'Istituto si trovi ad esaminare le richieste di accesso civico generalizzato «riguardo ai dati dei titolari di incarichi politici beneficiari del bonus Covid, anche eventualmente oggetto di restituzione», gli Uffici deputati dovranno operare una valutazione[50], caso per caso (interpellando, ove ne ricorrano i presupposti, l'Autorità, nella prevista funzione consultiva[51]), in conformità con la normativa di settore, le Linee guida ANAC in materia di accesso civico (ove, tra i limiti, espresso è il riferimento al «ruolo ricoperto nella vita pubblica, la funzione pubblica esercitata o l'attività di pubblico interesse svolta dalla persona cui si riferiscono i predetti dati»), i Provvedimenti, *ratione materiae*, del Garante[52], tenendo, altresì, adeguatamente conto della differente posizione ricoperta dai titolari di cariche politiche di livello nazionale e dagli amministratori di livello locale, per i quali, evidentemente, la fonte di reddito non attiene tanto all'attività politico-amministrativa esercitata, piuttosto dalla principale occupazione lavorativa svolta in una specifica comunità[53].

---

[49] F. PIZZETTI, *Sentenza n. 20/2019 della Consulta e riordino degli obblighi di pubblicità, trasparenza e diffusione delle informazioni della PA: il legislatore non trascuri il "riuso" delle fonti pubbliche*, in MediaLaws, n. 2, 2019.

[50] Risulta, infatti, necessario garantire che il bilanciamento dei diritti rilevanti, oggetto di commento, venga perseguito, caso per caso, mediante una ponderazione reale tra diritti opposti e di uguale rilevante valore, posto che i dati e i documenti forniti al richiedente tramite l'accesso generalizzato sono considerati <<pubblici>> e che ogni ulteriore attività di trattamento deve svolgersi nel rispetto dei limiti espressi dalla normativa in materia di protezione dei dati personali (Garante, 15.12.16., n. 521, doc. web. n. 5860807).

[51] GARANTE, Bonus Covid: Garante privacy invia chiarimenti all'Inps, comunicato stampa, 17 agosto 2020, doc. web.9448663.

[52] Il soggetto destinatario dell'istanza (laddove la stessa non risulti meramente esplorativa e finalizzata a paralizzare il buon andamento dell'amministrazione), nel dare riscontro alla richiesta di accesso generalizzato, in ossequio a quanto disposto dalla normativa privacy, nonché nel rispetto delle libertà fondamentali, dovrebbe privilegiare le modalità meno pregiudizievoli al libero godimento dei diritti degli individui coinvolti, optando per l'ostensione di documenti mediante l'oscuramento dei dati personali presenti, allorquando l'esigenza conoscitiva dell'istante possa essere soddisfatta senza alcun rilascio di informazioni riferite agli interessati.

[53] M. PLUTINO, *Tutela della riservatezza e "diritto" alla trasparenza nella nuova normativa del finanziamento ai partiti. Un compromesso insoddisfacente?* in Dirittifondamentali.it, 1, 2016, pp. 1-30, C. COLAPIETRO, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy*, in Federalismi.it, 14, 2020. Sulla prevalenza della tutela dei dati sensibili sulla generica esigenza della trasparenza amministrativa cfr. Cass. Civ., Sez. 2, sentenza 4 aprile 2019, n. 9382. In relazione alla recente sentenza n. 20/2019 cfr. A. CORRADO, *Gli obblighi di pubblicazione dei dati patrimoniali dei dirigenti alla luce delle indicazioni della Corte Costituzionale*, in Federalismi.it, 27 febbraio 2019; G. BRONZINI, *La sentenza n. 20/2019 della Corte costituzionale italiana verso un riavvicinamento all'orientamento della Corte di giustizia?*, in QuestioneGiustizia.it, 4 marzo 2019.

ISSN 2036-7821

3. Conclusioni.

In conclusione, dalle risultanze della vicenda in commento, emergono con forza alcune riflessioni, al netto delle motivazioni che fornirà la XVIII Sezione Civile del Tribunale di Roma a corredo della Sentenza n. 4735 / 2022, e degli ulteriori sviluppi giurisprudenziali che interverranno. La prima riguarda, in generale, il ruolo di tutela della riservatezza rivestito dal Garante *Privacy*, nel contesto pubblico. L'Istituto di Previdenza, nel caso di specie, ha reputato «eccessivo l'impianto di giudizio complessivo» dell'Autorità[54], pur mostrando collaborazione, giacché «non sono stati utilizzati dati sensibili o anche dati che non fossero visibili al pubblico». In tal senso, secondo l'INPS, «l'applicazione della privacy by design e by default può, per un Istituto che gestisce decine di milioni di prestazioni per lo Stato e i cittadini nella previdenza e nell'assistenza, creare nella pratica molte incertezze nel funzionamento dell'amministrazione, che tende sempre più a gestioni automatizzate e digitali, e nelle sue legittime azioni di controllo massivo e di antifrode in tempi rapidi che uno Stato equo, efficiente ed agile richiede». Con riferimento ai rischi per gli interessati, invece, l'INPS ha sostenuto che «è coerente e legittimo escludere l'obbligo di valutazione d'impatto, in considerazione del limitato e contenuto criterio di trattamento dei dati».

Simili argomentazioni dimostrano, da un lato, che è il percorso di sensibilizzazione e di diffusione della cultura della *privacy* nel contesto pubblico[55] richiede, ancor oggi, un forte impulso, e, dall'altro, che, in virtù della funzione deterrente della normativa in materia di protezione dei dati personali, solo nel momento in cui interviene l'Autorità, preposta al controllo del rispetto della normativa di settore, attraverso gli strumenti sanzionatori ad essa attribuiti dalla legge (resistenti, nonostante interventi normativi, quali il c.d. "Decreto aperture") [56], il dibattito sui temi dei diritti fondamentali degli interessati si pone all'attenzione dell'opinione pubblica, come dimostrano, d'altronde, i recenti Provvedimenti del Garante sull'uso delle certificazioni verdi Covid-19, da parte della Regione Campania[57], e sulla questione dei dati personali detenuti dall'Associazione Rousseau[58].

[54] INPS, Comunicato stampa del 9 marzo 2021, reperibile in www.inps.it.

[55] C. D'ORAZI, *I trattamenti di dati personali effettuati dalla P.A. Alla luce del Regolamento UE 679/2016*, in Rivista semestrale di diritto, 1/2020, pagg. 302 e seguenti, qui reperibile: https://www.iusinitinere.it/i-trattamenti-di-dati-personali-effettuati-dalla-p-a-alla-luce-del-regolamento-ue-679-2016-33413.

[56] Si pensi Dl. 8 ottobre 2021, n. 139, contiene disposizioni urgenti "per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di Pubbliche Amministrazioni e in materia di protezione dei dati personali". Il "Decreto Aperture", così come ribattezzato. Evidente è la collocazione dei soggetti che possono essere considerati "poteri pubblici", ai sensi del Gdpr, riconducendoli una volta per tutte entro i controlli ordinari del Garante per la protezione dei dati personali (viene abrogato, cioè, la normativa dell'art. 2-quinquiesdecies del "Codice Privacy").

[57] GARANTE, Provv. 25 maggio 2021, n. 207, doc. web n. 9590466.

[58] GARANTE, Provv. 1° giugno 2021, n. 223, doc. web n. 9592011.

ISSN 2036-7821

Nel contempo, con riferimento allo stato dell'arte dell'applicazione della normativa *privacy* nella Pubblica Amministrazione italiana, va segnalato che, se fino a qualche tempo fa, le preoccupazioni delle figure apicali dei soggetti pubblici erano, seppur normativamente, definite[59], oggi, a mente, altresì dei Consideranda 6 e 7 al Reg. UE 2016/679, l'accelerazione del progresso tecnologico e la conseguente digitalizzazione dei rapporti tra cittadini e pubbliche amministrazioni ha consentito che irrompessero, nelle medesime P.A., nuove esigenze di tutela, spesso non accompagnate dalle più ampie ed essenziali garanzie. Sia emblematica, in tal senso, la circostanza che dopo tre anni dall'entrata in vigore del reg. UE 2016/679, diversi "soggetti pubblici" non hanno provveduto alla nomina del *Data Protection Officer*, figura strategica che si pone quale elemento di assoluto rilievo, fondamentale per la corretta gestione delle *privacy policy*, a presidio di un miglioramento dell'organizzazione interna e di un adeguato livello di tutela dei cittadini[60].
In tale prospettiva, primario diviene il ruolo svolto dal Garante *Privacy* in ambito pubblico (così come in ambito privato), poiché, come affermato anche dalla recente giurisprudenza della Corte di giustizia UE, l'Autorità rappresenta il custode dei principi che regolano il governo della *privacy* e dunque il controllore della conformità dei trattamenti[61]. Grazie al *know-how* e all'esperienza di cui dispone, è auspicabile che il Garante renda possibile un allineamento tra quadro normativo e realtà empirica[62]. Ciò, in special modo, tornerà indispensabile, qualora, in un futuro (non molto lontano) si affermerà, nelle amministrazioni pubbliche, l'utilizzo degli algoritmi[63], come ausilio nelle decisioni amministrative, come da tempo già avviene in altre nazioni[64].

[59] S. CALZOLAIO, *Digital (and privacy) by default: l'identità costituzionale della amministrazione digitale*, in Giornale di storia costituzionale, 31, I, 2016, Macerata: EUM-Edizioni Università di Macerata, - Permalink: http://digital.casalini.it/10.1400/243267 - Permalink: https://doi.org/10.1400/243267.

[60] F. LORÈ, *Il ruolo del Responsabile della protezione dei dati personali nella pubblica amministrazione alla luce del Regolamento generale sulla protezione dei dati personali UE 2016/679*, in Amministrativ@mente, n. 7-8/2018.

[61] L. CALIFANO, *La protezione dei dati personali e il ruolo del Garante in ambito pubblico*, in MediaLaws - Rivista di diritto dei media, n. 1, 2018.

[62] L. CALIFANO, *Ibidem*

[63] L. AMMANNATI, *I 'signori' nell'era dell'algoritmo*, in Diritto pubblico, Rivista fondata da Andrea Orsi Battaglini, 2/2021, pp. 381-413.

[64] R. SHOKRI, *On the Privacy Risks of Model Explanations*, AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and SocietyJuly, 2021, pp. 231–241.

ISSN 2036-7821