

Ordinanza di ingiunzione nei confronti di Comune di Palermo - 15 aprile 2021

[doc. web n. 9587053]

Registro dei provvedimenti
n. 140 del 15 aprile 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito "Regolamento");

VISTO il d. lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gdpd.it, doc. web n. [9107633](#) (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal Segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali (doc. web n. 1098801);

Relatore il prof. Pasquale Stanzione;

PREMESSO

1. Premessa

Questa Autorità ha ricevuto un reclamo da parte del sig. XX, regolarizzato e integrato, da ultimo, in data XX, con il quale è stato lamentato che i dati personali dell'interessato, contenuti nella domanda di sussidi alimentari di cui all'ordinanza del Capo del Dipartimento della protezione civile n. XX del XX, presentata al Comune di Palermo (per il tramite del sito <https://protezionecivile.comune.palermo.it>), sarebbero stati acquisiti da un soggetto non autorizzato.

In particolare, il reclamante ha lamentato che alle sue informazioni avrebbe avuto accesso un operatore, riconducibile all'Associazione "XX" (il sig. XX), il quale, secondo quanto rappresentato, avrebbe utilizzato tali informazioni per finalità estranee a quelle connesse all'attività di erogazione del predetto sussidio, avendo l'interessato presentato la domanda tramite il summenzionato sito e non tramite la predetta Associazione.

2. Istruttoria

In riscontro alle richieste di informazioni del XX (prot. n. XX), ai sensi dell'art. 157 del Codice, il Comune ha dichiarato che:

per dare attuazione alla OCDPC n. XX del XX, il Comune di Palermo, "al fine di procedere nel più breve tempo possibile, all'erogazione dei benefici previsti, ha ritenuto di utilizzare la Piattaforma informatica denominata "Centrale Unica Aiuti Alimentari", in linea dal XX per gestire le offerte alimentari a favore delle famiglie bisognose, accessibile dal sito del Comune al link: <https://protezionecivile.comune.palermo.it/...>";

inoltre, "Per coadiuvare i richiedenti a inserire la dichiarazione necessaria all'erogazione del contributo, l'A.C., si è avvalsa del supporto di soggetti esterni (Enti del Terzo Settore, Sindacati e Parrocchie) [(c.d. OpT)] dislocati strategicamente a coprire l'intero territorio cittadino al fine di garantire "assistenza agli utenti nella compilazione della richiesta per l'erogazione dei buoni spesa per l'emergenza epidemiologica da Covid-19", in ausilio alla Centrale della Protezione Civile Comunale";

le organizzazioni coinvolte “sono state accreditate ad inizio aprile (XX) con successive integrazioni a metà aprile (XX) [...]”; un ultimo step di accreditamento ha riguardato alcune sedi sindacali da metà maggio (XX). Con la chiusura del 3^o lotto programmata per fine maggio (XX) è di fatto cessata l'operatività degli OpT e le schede del 4^o lotto e successivi sono state gestite con il solo personale comunale [...] e dagli operatori del COC [...]. Con la chiusura della procedura standard di presentazione delle istanze sulla Piattaforma si è conclusa la collaborazione con gli OpT designati per gli appuntamenti in presenza, avviata il XX; le credenziali verranno cessate a chiusura del lotto 4^o”;

“Ogni OpT, di documentata esperienza, capacità ed affidabilità in relazione ai compiti ad esso affidati nonché idonea organizzazione tecnica, organizzativa e di risorse, è stato designato Responsabile del Trattamento dei dati, con apposita nota di “Designazione del Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679”, comprensiva delle istruzioni per il trattamento dati”, al fine di offrire l'attività di “assistenza agli utenti nella compilazione della richiesta per l'erogazione dei buoni spesa per l'emergenza epidemiologica da Covid 19”;

agli OpT è stato assegnato il compito di “Ricevere il richiedente [...] Aiutare a completare l'iter previsto dalla piattaforma [...] Stampare l'autocertificazione per far firmare l'utente [...] procedendo, [...] all'upload della stessa e del documento di identità [...] Verificare lo stato della pratica attraverso la funzione della Piattaforma “OPT – Verifica Stato Pratica” che consentirà all'addetto di recuperare l'anagrafica dell'utente, [...] Custodire il cartaceo fino alla consegna successiva a personale comunale incaricato dal responsabile del Trattamento”;

a seguito della creazione della scheda individuale e della compilazione dell'autocertificazione, da parte del richiedente direttamente sull'apposita piattaforma messa a disposizione da codesto Comune, “La routine a disposizione dei punti di raccolta (OpT) abilita i responsabili ivi incaricati ad interrogare il database tramite l'inserimento del codice fiscale dell'utente per accedere alla scheda individuale e, verificata la corrispondenza tra il numero di pratica assegnato dalla piattaforma all'autodichiarazione con quello riportato sulla copia cartacea sottoscritta, nonché la presenza di un valido documento di identità, effettuavano la conferma di ricezione della pratica. La routine permette anche la ricerca non massiva con almeno i primi 3 caratteri del codice fiscale per favorire l'individuazione delle schede individuali dei cittadini che non portavano con sé il numero di codice fiscale. L'interrogazione delle schede visualizza anche i passaggi salienti dello stato di avanzamento della pratica, senza fornire dettagli sugli eventuali step non superati”;

“Tutte le attività utente sono tracciate attraverso un sistema di log che da evidenza delle connessioni effettuate e delle azioni eseguite”.

In risposta ad un'ulteriore richiesta di informazioni, effettuata con nota del XX (prot. n. XX), il Comune ha dichiarato, con nota del XX (prot. n. XX), che:

- “non sono state rilasciate << specifiche credenziali per gli operatori individuati presso gli stessi Enti da autorizzare all'accesso alla piattaforma per lo svolgimento dell'attività di assistenza nella compilazione delle richieste>> ma solo le credenziali di accesso intestate al titolare del trattamento dati, che non ha richiesto altre abilitazioni”;

- le funzioni operative, connesse all'accesso alla piattaforma, “sono state disabilitate in data XX alle ore XX la prima ed in data XX alle ore XX la seconda. Da tale ultimo momento anche se l'operatore ha effettuato l'accesso al sistema non ha potuto accedere a nessuna funzione applicativa”;

- “con il livello di abilitazione delle credenziali concesse agli Enti di terzo settore designati, si accedeva a tutte le pratiche del data-base classificate allo stadio di dichiarazione integrativa presente e non convalidata dall'OPT, anche in forma di storico sintetico per la visualizzazione dello stato di lavorazione delle istanze”;

- le scelte tecniche e organizzative effettuate sono state “orientate a dare la possibilità ai cittadini [...] di rivolgersi all'OPT più facilmente accessibile in relazione alla dimora o agli spostamenti abituali; così come i << criteri di ricerca stabiliti (ricorso al solo codice fiscale del richiedente, anche solo limitatamente ai primi tre caratteri)>> sono stati orientati, per la parte che attiene alle credenziali concesse agli Enti di terzo settore designati, all'identificazione quanto più univoca possibile delle schede da interrogare”;

- gli operatori autorizzati accedono all'“anagrafica dichiarata dal cittadino”, alla “autocertificazione sottoscritta” e allo “stato di lavorazione della pratica”;

- con riferimento ai log relativi a tutti gli accessi effettuati alla posizione del reclamante, allegati, “non è tecnicamente possibile risalire alle singole interrogazioni effettuate durante le sessioni di log-in effettuate con le credenziali in oggetto, se non per quelle che hanno prodotto effetti diretti sulla procedura, quali tutti quelli relativi al caricamento delle dichiarazioni e dei documenti richiesti per perfezionare l'istanza”, le quali “danno evidenza che nessuna attività procedurale sul data base è stata svolta dalla Associazione “XX” [...] attività invece svolte dall'Associazione Adra Italia”.

Con nota del XX (prot. n. XX), sono stati richiesti elementi all'Associazione "XX", la quale, con nota del XXo, ha dichiarato che:

- "L'associazione era dotata di un accesso [alla banca dati della protezione civile] tramite password fornita dalla protezione civile. Tale accesso era monitorato dalla stessa protezione civile e non consentiva di vedere i dati di tutte le persone che avessero presentato istanza ma soltanto di quelle materialmente recatesi presso la sede e che avessero fornito il loro codice fiscale. Soltanto inserendo il codice fiscale dell'utente era infatti possibile per l'operatore dell'associazione effettuare una ricerca tramite il terminale dell'associazione onde verificare lo stato dell'istanza";

-sulla citata piattaforma risultavano "aperte solo le seguenti funzioni: 1) verifica stato pratica e 2) acquisizione autocertificazione. In base a questa seconda funzione era possibile per gli utenti consegnare l'autocertificazione generata dal sistema ai responsabili dell'associazione i quali, ricevutala, flaggavano sul sistema la voce "acquisita autocertificazione";

- "Autorizzati a poter accedere a tale banca dati onde erogare i suddetti servizi erano [due soggetti, tra cui il sig. XX], ad entrambi è stato fornito dalla presidente l'uso di un pc con connessione. Allorquando l'utente si presentava essi provvedevano a verificare tramite il codice fiscale l'avvenuta presentazione dell'istanza e, qualora non avesse l'utente provveduto a stamparla autonomamente, i responsabili gli stampavano l'autocertificazione generata dal sistema";

- "L'attività ovviamente veniva conclusa nel mese di Maggio in corrispondenza con il termine del Lockdown con la consegna dell'ultimo blocco di plichi contenenti le autocertificazioni ai responsabili della protezione civile del comune di Palermo".

A seguito di un'ulteriore richiesta di informazioni del XX (prot. n. XX), la predetta Associazione, con nota del XX, ha dichiarato che:

- "le credenziali fornite erano una per ogni associazione con la quale dovevano "lavorare" tutti i soci che di volta in volta avessero il turno";

- "l'operatore poteva avere accesso a tutte le pratiche del sistema. Di ogni scheda individuale l'operatore poteva visualizzare ESCLUSIVAMENTE se la domanda fosse registrata o meno";

- "ogni operatore autorizzato dell'associazione, per il tramite del codice fiscale di un soggetto che avesse presentato la domanda, poteva, inserendo appunto il codice fiscale visualizzare i dati personali NOME COGNOME CODICE FISCALE E REDDITI DICHIARATI NELLA AUTOCERTIFICAZIONE nonché poteva scaricare la suddetta autocertificazione reddituale".

Con successiva comunicazione del XX, la medesima Associazione ha allegato la email con la quale il Comune di Palermo, in data XX, aveva inviato all'Associazione le credenziali per l'accesso al sistema gestione Centrale Unica Aiuti, nella quale è specificato che "dette credenziali non dovranno essere modificate e saranno utilizzate da tutti gli operatori che si avvicenderanno nella turnazione".

3. La normativa in materia di protezione dei dati personali

Ai sensi del Regolamento, per "dato personale" si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato)". Inoltre, "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" (art. 4, par. 1, n. 1).

Il titolare del trattamento, in generale, è tenuto a rispettare i principi in materia di protezione dei dati, fra i quali, in particolare, quello di "integrità e riservatezza", in base al quale i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. 1, lett. f), del Regolamento).

Inoltre, il titolare del trattamento è tenuto a rispettare i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita (data protection by design e by default, art. 25 del Regolamento), ai sensi dei quali, rispettivamente:

- "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso [...] mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad

attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati” (par. 1);

- “mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica” (par. 2).

Infine, sul piano della sicurezza del trattamento, l'art. 32 del Regolamento impone che il titolare (e il responsabile) del trattamento “Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche”, metta in atto “misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio”, tra cui, in particolare, “la pseudonimizzazione e la cifratura dei dati personali”, “la capacità di assicurare su base permanente la riservatezza” e “una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento” (par. 1); “Nel valutare l'adeguato livello di sicurezza, [...] tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati” (par. 2).

4. Valutazioni preliminari dell'Ufficio e notifica della violazione

L'Ufficio, con atto del XX (prot. n. XX), che qui deve intendersi integralmente riprodotto, ha avviato, ai sensi dell'art. 166, comma 5, del Codice, con riferimento alle specifiche situazioni di illiceità in esso richiamate, un procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento nei confronti del Comune di Palermo, in quanto la piattaforma informatica denominata “Centrale Unica Aiuti Alimentari”, accessibile dal sito del Comune al link: <https://protezionecivile.comune.palermo.it/...>, utilizzata per gestire le offerte alimentari a favore dei soggetti richiedenti, ai sensi dell'OCDPC n. XX del XX, era priva delle necessarie misure tecniche e organizzative tali da assicurare un'adeguata tutela dei diritti e delle libertà degli interessati, comportando, quindi, la violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento.

5. Memorie difensive e audizione

Il Comune di Palermo, con la nota del XX (prot. n. prot. XX, ha inviato al Garante, ai sensi dell'art. 166, commi 6 e 7, del Codice e dell'art. 18, comma 1, della l. 24 novembre 1981, n. 689, i propri scritti difensivi in relazione alle violazioni notificate.

Al riguardo, si ricorda che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice, intitolato “Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante”.

Nello specifico, quanto alla condotta tenuta, è stato evidenziato, fra l'altro, che:

- “si è messo a punto un sistema di erogazione buoni spesa che è riuscito a contemperare tutte le esigenze: semplicità di accesso per l'utente, tempestività della risposta, erogazione del beneficio direttamente con accredito su tessera sanitaria senza necessità di consegna “fisica” alla persona riducendo così al minimo la necessità di spostamento delle persone e le occasioni di contagio” (p. 1);

- “Le informazioni richieste all'utente sono state ridotte al minimo: dati anagrafici per individuare i soggetti e recapiti per inviare le informazioni, oltre che, ovviamente, situazione economica per valutare il diritto al beneficio, ma limitata all'essenziale, al solo mese di marzo 2020 [...] al fine di rispettare il principio di minimizzazione dei dati personali sancito dall'art. 5 comma c del GDPR. [...] non è stato chiesto ISEE in quanto dato ultroneo e non essenziale: il buono spesa è stato erogato in considerazione della situazione economica dell'utente limitata al mese di marzo 2020. Di conseguenza il dato conosciuto dagli operatori non è indicativo della situazione economica dell'utente, ma soltanto della situazione in cui l'utente si è venuto a trovare - temporaneamente - per l'emergenza covid, quindi riferito ad un solo mese e nel dettaglio solo al mese di marzo” (p. 2);

- “Inizialmente l'accesso degli opt è stato limitato alle persone del proprio bacino di utenza, proprio per limitare le possibilità di accesso. Poi, visto l'andamento dell'utenza che si presentava di fatto presso opt diversi anche perché la residenza anagrafica non sempre corrisponde con il domicilio reale, si è reso necessario estendere l'accesso a tutte le istanze e consentire all'utenza di presentarsi presso l'opt che risultava essere il più confacente al suo domicilio e ai suoi spostamenti” (p. 2);

- È stato anche necessario consentire l'accesso alla pratica con un numero limitato di caratteri del codice fiscale, perché spesso l'utente errava la registrazione del proprio codice fiscale e per ritrovare la pratica si procedeva con 3/4 caratteri in modo da poter comunque individuare la pratica e l'errore" (p. 2);

- "La possibilità di accesso alle pratiche già concluse si è resa necessaria per consentire agli opt di dare informazioni agli utenti sulla loro posizione e lo stato della pratica" (p. 2);

- "La registrazione di tutti gli accessi degli operatori, anche per le sole visualizzazioni, non si ritiene opportuna per la tipologia di attività svolta, considerato il notevole numero di informazioni date agli utenti: gli operatori non potrebbero ricordare e dimostrare l'utilità di ogni accesso" (p. 2);

- "Prima ancora della conclusione delle attività di erogazione, tutt'ora in corso con il perdurare dell'emergenza e della chiusura delle attività, passato il primo momento di forte emergenza e riorganizzato l'ufficio con personale di altri reparti, sono stati chiusi gli accessi a tutti gli opt esterni, riportando tutto il carico di lavoro ai dipendenti comunali, con notevole sforzo di questa Amministrazione" (p. 2);

- più in generale, "il legislatore ha disciplinato in materia civile e penale le conseguenze delle circostanze, stabilendo in particolare esimenti ad esclusione della pena, e soprattutto scriminanti che escludono il reato e l'antigiuridicità di una condotta di per sé illecita. Vi rientrano la legittima difesa, lo stato di necessità, l'esercizio di un diritto, il consenso dell'avente diritto, l'adempimento di un dovere, l'uso legittimo delle armi. Le stesse norme sulla protezione dei dati personali ammettono deroghe in caso di emergenza sanitaria e fino al termine dell'emergenza sanitaria. Riteniamo il fatto lecito ab origine. Ciò comporta importanti conseguenze: a) eliminano l'antigiuridicità del fatto, nel senso che il fatto commesso non è un reato; b) è inapplicabile qualsiasi tipo di sanzione" (p. 3).

Il Comune, nei propri scritti difensivi, ha anche fornito un quadro del particolare contesto emergenziale in cui il trattamento in questione è stato effettuato, rappresentando, in particolare, che "nei mesi di marzo/aprile, la chiusura improvvisa e assoluta di tutte le attività ha messo la popolazione nell'impossibilità di provvedere a sé stessa. [...] In questa situazione di estrema difficoltà, il Governo ha emanato diverse misure di sostegno, ma anche di deroga alle normali procedure perché bisognava provvedere e provvedere in fretta. [...] La situazione rischiava di diventare insostenibile, per ripetuti episodi in varie città italiane tra cui anche Palermo di attacchi ai supermercati ed istigazione alla rivolta per la fame che cominciava a serpeggiare tra la popolazione più colpita. Anche la Prefettura ha convocato il Comitato per l'Ordine e la Sicurezza Pubblica chiedendo al Comune misure tempestive" (p. 1).

In data XX si è tenuta un'audizione (prot. n. XX), mediante videoconferenza a distanza, con i rappresentanti del Comune di Palermo (il cui verbale è stato accettato con dichiarazione del XX, prot. n. XX), all'interno della quale, oltre a confermare quanto già affermato negli scritti difensivi, è stato aggiunto, in particolare, che:

- È stato all'uopo riadattato il servizio online già utilizzato per la distribuzione dei pacchi spesa. Rappresento le difficoltà operative in cui tale attività è stata organizzata, con il personale della struttura comunale in smart working, nella fase iniziale, quindi con tutte le difficoltà derivanti dall'uso delle piattaforme comunali con modalità di lavoro da remoto" (p. 2);

- "la maggior parte dell'utenza aveva la necessità di contattare più volte gli opt, per le seguenti ragioni: errori nella compilazione; incompletezza della documentazione presentata; difficoltà legate alla tipologia di utenza, distribuita su tutte le fasce sociali, compresi gli stranieri, anche non regolari; assenza di dispositivi e di competenze informatiche. Si evidenzia, al riguardo, che abbiamo trattato circa 53.000 domande tra aprile e maggio, di cui solo 18.000 evase positivamente" (p. 2);

- con riferimento alle modalità del coinvolgimento degli OpT, "a causa della circostanza che l'utenza sovente non si recava presso l'opt territorialmente di riferimento, si è stabilito di consentire l'accesso alla piattaforma a tutti gli opt, senza limitazioni territoriali. Ciò in ragione degli errori frequentemente riscontrati nella compilazione delle pratiche e nella conseguente necessità di dover consultare anche pratiche già definite, nonché in ragione delle frequenti richieste circa lo stato della pratica da parte dei richiedenti" (pp. 2-3);

- "frequenti errori di inserimento delle generalità derivanti dalla difficoltà di riportare correttamente il nome [...] hanno determinato la necessità di consentire la ricerca delle pratiche nella piattaforma con l'inserimento dei soli primi 3 caratteri del codice fiscale" (p. 3);

- "il servizio in questione è stato cautelativamente sospeso non appena il Comune è venuto a conoscenza delle criticità evidenziate nella notifica di violazione da parte del Garante. Attualmente è stato riattivato, dopo che sono stati apportati gli adeguamenti necessari a superare le predette criticità. Nella fase di riattivazione è stato limitato il numero degli operatori abilitati ad operare; sono stati ridotti a due i profili di autorizzazione, comprendenti le funzioni operative

specificamente assegnate. Attualmente è consentito l'accesso a 20 operatori, di cui 8 con profilo di autorizzazione completo (che comprende 5 funzioni operative). È stato introdotto l'obbligo di motivare le richieste di consultazione delle pratiche da parte degli utenti al fine di documentare gli accessi effettuati dagli operatori comunali. In relazione a ciò, con le migliorie apportate, è stata prevista la registrazione nei file di log anche delle operazioni di visualizzazione, comprensive del dettaglio dei dati visualizzati da parte degli operatori, anche se ciò ha determinato un appesantimento della procedura a causa della necessità di documentare ogni accesso in relazione alle attività concretamente svolte" (p. 3);

- "Con riferimento all'assegnazione di una sola coppia di credenziali per gli opt, ciò derivava dalla disponibilità fornita dagli opt di una postazione con un operatore, destinati allo svolgimento di tali attività. Non vi era da parte del Comune alcuna difficoltà ad assegnare più credenziali nel caso in cui un opt avesse fatto richiesta in tal senso" (p. 3).

6. Esito dell'istruttoria

Gli elementi adottati negli scritti difensivi e nella successiva audizione da parte del titolare del trattamento, seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, in quanto non sono in grado di dimostrare che la piattaforma informatica denominata "Centrale Unica Aiuti Alimentari", accessibile dal sito del Comune al link: <https://protezionecivile.comune.palermo.it/...>, fosse dotata di misure tecniche e organizzative tali da assicurare un'adeguata tutela dei diritti e delle libertà degli interessati. Infatti, in base alla documentazione acquisita in atti, si conferma la circostanza secondo cui era possibile, per un operatore autorizzato di qualsiasi OpT, consultare tutte le pratiche inserite nella citata piattaforma, visualizzare i dati anagrafici e la fascia economica ISEE dei richiedenti il buono alimentare e apprendere, di conseguenza, la condizione e situazione di fragilità economica in capo ai richiedenti medesimi.

A questo proposito, si confermano le criticità già rilevate in sede di avvio del procedimento per l'adozione dei provvedimenti correttivi e sanzionatori (nota del XX, prot. n. XX), in quanto:

a) per l'accesso alla piattaforma a ciascun OpT erano state fornite uniche credenziali, non modificabili, che non consentivano l'attribuzione univoca delle operazioni di trattamento svolte dagli operatori turnanti presso l'OpT a una persona fisica responsabile delle medesime. Ciò è documentato dalla email che il Comune ha inviato all'Associazione in data XX (e prodotta da quest'ultima con l'integrazione del XX), in cui, nel fornire le credenziali per l'accesso alla piattaforma, viene espressamente riportato che "Dette credenziali non dovranno essere modificate e saranno utilizzate da tutti gli operatori che si avvicenderanno nella turnazione". Quanto riferito dal Comune, secondo cui "Con riferimento all'assegnazione di una sola coppia di credenziali per gli opt, ciò derivava dalla disponibilità fornita dagli opt di una postazione con un operatore, destinati allo svolgimento di tali attività. Non vi era da parte del Comune alcuna difficoltà ad assegnare più credenziali nel caso in cui un opt avesse fatto richiesta in tal senso", non è in grado di superare la criticità connessa alla circostanza di aver comunque assegnato, inizialmente, una sola coppia di credenziali di accesso per ciascun OpT e di aver, comunque, dato istruzioni in merito alla possibilità di un utilizzo condiviso tra gli operatori delle credenziali medesime (cfr email del XX);

b) i file di log registravano le sole operazioni che "hanno prodotto effetti diretti sulla procedura, quali tutti quelli relativi al caricamento delle dichiarazioni e dei documenti richiesti per perfezionare l'istanza" escludendo le operazioni di mera consultazione effettuate eventualmente anche in assenza di autorizzazione degli interessati. Il Comune ha confermato, in sede di audizione, di aver previsto, solo dopo la "notifica di violazione da parte del Garante", "la registrazione nei file di log anche delle operazioni di visualizzazione, comprensive del dettaglio dei dati visualizzati da parte degli operatori", unitamente alla scelta di limitare le possibilità di accesso ai soli operatori comunali: tali misure, idonee a ridurre i rischi di accessi non autorizzati ai dati personali degli interessati, non erano però presenti all'atto dei trattamenti nel periodo considerato (aprile-giugno 2020);

c) la funzione di ricerca degli interessati richiedeva l'inserimento dei soli primi tre caratteri del codice fiscale. Pur prendendo atto dei "frequenti errori di inserimento delle generalità", che hanno spinto il Comune a tale scelta (come dichiarato dal medesimo negli scritti difensivi e in audizione), si rileva che tale modalità rendeva estremamente facile, per un operatore autorizzato, verificare la condizione di richiedente del buono alimentare di qualsiasi interessato, anche in assenza di una esplicita autorizzazione di quest'ultimo, vista la semplice reperibilità dei tre elementi iniziali del codice fiscale. La presenza di ulteriori informazioni che assicurassero la sussistenza di un'autorizzazione da parte dell'interessato (quali, a esempio, il codice associato alla domanda o il numero di protocollo della pratica) avrebbe potuto rappresentare una misura idonea sia a consentire una più agevole individuazione degli interessati, sia a ridurre il rischio di accessi indebiti;

d) era possibile, per gli operatori degli OpT, consultare anche le pratiche già concluse, ancorché non oltre il termine in cui è avvenuta la disabilitazione dell'accesso (in base a quanto dichiarato, giugno 2020), rendendo possibile la consultazione anche a distanza di tempo e, di conseguenza, la conoscenza della circostanza dell'effettiva percezione del buono alimentare da parte di un richiedente. Infatti, sia quanto riportato nell'atto di designazione a responsabile del

trattamento (secondo cui gli OpT erano stati specificamente designati per l'attività di “assistenza agli utenti nella compilazione della richiesta per l'erogazione dei buoni spesa per l'emergenza epidemiologica da Covid-19”) che quanto dichiarato in sede di audizione (“la maggior parte dell'utenza aveva la necessità di contattare più volte gli opt, per le seguenti ragioni: errori nella compilazione; incompletezza della documentazione presentata; difficoltà legate alla tipologia di utenza, distribuita su tutte le fasce sociali, compresi gli stranieri, anche non regolari; assenza di dispositivi e di competenze informatiche”) giustificano l'accesso alla piattaforma limitatamente al momento in cui la pratica di erogazione era in corso di istruttoria, al fine di fornire informazioni all'interessato circa l'avanzamento dello stato della pratica, ma non lo giustificano invece con riferimento alle pratiche già definite, per cui il richiedente era già a conoscenza dell'esito.

Inoltre, si ritiene inconfidente quanto dichiarato dal Comune, negli scritti difensivi, circa le “esimenti ad esclusione della pena, e soprattutto scriminanti che escludono il reato e l'antigiuridicità di una condotta di per sé illecita”, in quanto si tratta di valutazioni che concernono l'applicazione della legge penale e che non sono oggetto del presente procedimento, non rientrando tra i profili di competenza del Garante.

Analogamente, non risulta fondata l'osservazione secondo cui “Le stesse norme sulla protezione dei dati personali ammettono deroghe in caso di emergenza sanitaria e fino al termine dell'emergenza sanitaria”; si tratta di un riferimento generico e non corretto, considerato che l'art. 17-bis del d.l. 17 marzo 2020, n. 18, pur prevedendo che i soggetti individuati dalla norma possano effettuare trattamenti di dati personali che risultino necessari all'espletamento delle funzioni ad essi attribuite nell'ambito dell'emergenza determinata dal diffondersi del Covid-19, fa salva la necessità che tali trattamenti debbano essere effettuati adottando misure appropriate a tutela dei diritti e delle libertà degli interessati e nel rispetto dei principi di cui all'art. 5 del Regolamento, tra cui il principio di minimizzazione dei dati, secondo cui i dati devono essere “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati” (art. 5, par. 1, lett. c), del Regolamento). D'altro canto, il particolare contesto in cui il trattamento in questione è stato effettuato, pur potendo essere tenuto in considerazione in sede di quantificazione della sanzione amministrativa, ai sensi dell'art. 83, par. 2, del Regolamento (cfr. infra), comunque non è idoneo ad escludere la sussistenza delle illecità riscontrate.

In altri termini, anche nel complesso quadro emergenziale, spetta al titolare del trattamento adottare le misure necessarie a garantire che i dati degli interessati siano adeguatamente protetti, evitando così che, per ricevere un doveroso sostegno dall'ente pubblico, possano derivare loro conseguenze pregiudizievoli.

In conclusione, si ritiene, invece, di non dover sollevare rilievi in relazione alla possibilità, per gli OpT, di accedere “a tutte le pratiche del data-base classificate allo stadio di dichiarazione integrativa presente e non convalidata dall'OPT”, senza quindi una limitazione degli accessi a un sottoinsieme delle domande presentate in base a criteri predeterminati (come, ad esempio, la vicinanza o competenza territoriale), al fine di consentire ai richiedenti “di rivolgersi all'OPT più facilmente accessibile in relazione alla dimora o agli spostamenti abituali”. Infatti, nel particolare contesto emergenziale venutosi a creare a livello sanitario e delle conseguenti azioni di contrasto alla diffusione dell'epidemia da COVID-19, si ritiene che tale scelta potesse risultare uno strumento di semplificazione nella presentazione della domanda di buono alimentare.

Pertanto, a questo proposito si è tenuto anche conto che, in sede difensiva, il Comune ha affermato che “Inizialmente l'accesso degli opt è stato limitato alle persone del proprio bacino di utenza, proprio per limitare le possibilità di accesso. Poi, visto l'andamento dell'utenza che si presentava di fatto presso opt diversi anche perché la residenza anagrafica non sempre corrisponde con il domicilio reale, si è reso necessario estendere l'accesso a tutte le istanze e consentire all'utenza di presentarsi presso l'opt che risultava essere il più confacente al suo domicilio e ai suoi spostamenti”, denotando come, su questo profilo, fossero state originariamente applicate delle soluzioni ispirate ai principi di data protection by design e by default.

7. Conclusioni

Per tutto quanto sopra descritto, le circostanze evidenziate negli scritti difensivi e in sede di audizione, esaminate nel loro complesso, sicuramente meritevoli di considerazione ai fini della valutazione della condotta, non risultano sufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo alcuna delle ipotesi previste dall'art. 11 del Regolamento del Garante n. 1/2019.

In tale quadro, si confermano pertanto le valutazioni preliminari dell'Ufficio con la nota del XX (prot. n. XX), e si rileva l'illiceità del trattamento di dati personali effettuato dal Comune di Palermo, in quanto il trattamento di dati personali, effettuato tramite la piattaforma “Centrale Unica Aiuti Alimentari” nel periodo considerato (aprile-giugno 2020) e con le modalità precedentemente descritte, è stato effettuato:

a) in violazione del principio di “integrità e riservatezza”, di cui all'art. 5, par. 1, lett. f), del Regolamento, in quanto non è stata assicurata un'adeguata sicurezza dei dati personali, avendo consentito accessi non autorizzati;

b) in violazione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, di cui all'art. 25 del Regolamento, in quanto, al momento di determinare i mezzi del trattamento, non sono state messe in atto adeguate misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, nonché a garantire che non siano resi accessibili dati personali a un numero indefinito di persone fisiche;

c) in assenza di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, in violazione dell'art. 32 del Regolamento, in quanto non si è tenuto in adeguato conto dei rischi di accessi non autorizzati.

Considerato tuttavia che, in base a quanto dichiarato negli scritti difensivi e in sede di audizione, il Comune di Palermo ha affermato di aver adottato una serie di misure volte ad elevare le misure di sicurezza contro accessi non autorizzati ai dati contenuti nella citata piattaforma (limitazione dell'accesso a un numero circoscritto di operatori della sola amministrazione comunale, riduzione dei profili di autorizzazione, registrazione dei file di log anche in caso di mera consultazione, obbligo di motivazione in relazione alle richieste di consultazione), fermo restando quanto si dirà sull'applicazione della sanzione amministrativa pecuniaria, non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento.

8. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria (artt. 58, par. 2, lett. i), e 83 del Regolamento)

Al riguardo, l'art. 83, par. 3, del Regolamento, prevede che «Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave».

Nel caso di specie, la violazione delle disposizioni citate è soggetta all'applicazione della stessa sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento, che si applica pertanto al caso di specie.

Il Garante, ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere correttivo di «infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso». In tale quadro, «il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice» (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

La predetta sanzione amministrativa pecuniaria, inflitta in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare, tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

In relazione ai predetti elementi, è stato considerato che il trattamento ha presumibilmente avuto a oggetto i dati personali di almeno 18.000 persone, e quindi di un numero elevato di interessati, avendo il Comune dichiarato che sono state trattate «circa 53.000 domande tra aprile e maggio, di cui solo 18.000 evase positivamente», e che la violazione si è protratta per circa due mesi, avendo il Comune dichiarato che, con riferimento al caso di specie, «Dette funzioni sono state disabilitate in data XX alle ore XX la prima ed in data XX alle ore XX la seconda». Inoltre, è stato tenuto conto della particolare gravità della condotta, visto che sono stati raccolti dati sulla salute, in quanto il modulo di acquisizione dei dati degli interessati richiedeva se «all'interno del nucleo familiare sono presenti persone con disabilità».

Di contro, si è tenuto favorevolmente conto del fatto che le soluzioni inizialmente adottate dal Comune, per quanto inadatte a offrire un'adeguata tutela dei diritti e delle libertà degli interessati, sono comunque il frutto di una ponderazione del contesto, degli interessi in campo, delle necessità emerse nell'operatività e della tipologia di interessati: ciò emerge chiaramente laddove il Comune ha dichiarato, ad esempio, che «Le informazioni richieste all'utente sono state ridotte al minimo [...] al fine di rispettare il principio di minimizzazione dei dati personali sancito dall'art. 5 comma c del GDPR» e che «Inizialmente l'accesso degli opt è stato limitato alle persone del proprio bacino di utenza, proprio per limitare le possibilità di accesso». Ciò consente di qualificare una colpa di tipo lieve e una responsabilità di livello basso in capo al titolare. Inoltre, si è tenuto conto del fatto che il Comune, nel corso del procedimento, ha dichiarato di aver adottato le misure ritenute idonee a superare le criticità evidenziate nel corso dell'istruttoria, cooperando pienamente con l'Ufficio e affermando che «il servizio in questione è stato cautelativamente sospeso non appena il Comune è venuto a conoscenza delle criticità evidenziate nella notifica di violazione da parte del Garante. Attualmente è stato riattivato, dopo che sono stati apportati gli adeguamenti necessari a superare le predette criticità».

In ogni caso, e in termini più generali, ai fini della quantificazione della sanzione pecuniaria, si è tenuto in particolare considerazione il contesto emergenziale in cui il trattamento è avvenuto e la necessità di provvedere con urgenza per fronteggiare il profondo disagio socioeconomico causato dalla pandemia da Covid-19, avendo il Comune dichiarato che «nei mesi di marzo/aprile, la chiusura improvvisa e assoluta di tutte le attività ha messo la popolazione nell'impossibilità di provvedere a se stessa. [...] La situazione rischiava di diventare insostenibile, per ripetuti episodi in varie città italiane tra cui anche Palermo di

attacchi ai supermercati ed istigazione alla rivolta per la fame che cominciava a serpeggiare tra la popolazione più colpita. Anche la Prefettura ha convocato il Comitato per l'Ordine e la Sicurezza Pubblica chiedendo al Comune misure tempestive”

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di dover determinare, ai sensi dell'art. 83, parr. 2 e 3, del Regolamento, l'ammontare della sanzione pecuniaria, prevista dall'art. 83, par. 5, del Regolamento, nella misura di euro 40.000,00 (quarantamila) per la violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta effettiva, proporzionata e dissuasiva sensi dell'art. 83, par. 1, del medesimo Regolamento.

In relazione alle specifiche circostanze del presente caso, in ragione del fatto che il trattamento oggetto di esame sia stato effettuato mediante una banca dati contenente dati personali di una vasta platea di soggetti che si sono trovati (anche solo temporaneamente) in uno stato di disagio economico, si ritiene altresì che debba essere applicata la sanzione accessoria della pubblicazione del presente provvedimento sul sito web del Garante, prevista dall'art. 166, comma 7, del Codice e dall'art. 16, comma 1, del Regolamento del Garante n. 1/2019.

Si ritiene, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento del Garante n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

rilevata l'illiceità del trattamento effettuato dal Comune di Palermo, nei termini indicati in motivazione, ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento

ORDINA

al Comune di Palermo, in persona del legale rappresentante pro-tempore, con sede legale in Piazza Pretoria, 1 - Palazzo Delle Aquile - 90133 Palermo (PA) - C.F. 80016350821, di pagare la somma di € 40.000,00 (quarantamila) a titolo di sanzione amministrativa pecuniaria per le violazioni di cui in motivazione;

INGIUNGE

al medesimo Comune di pagare la somma di euro € 40.000,00 (quarantamila), secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. 689/1981.

Si ricorda che resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato – di un importo pari alla metà della sanzione irrogata, entro il termine di cui all'art. 10, comma 3, del d. lgs. 1° settembre 2011, n. 150 previsto per la proposizione del ricorso come sotto indicato (art. 166, comma 8, del Codice).

DISPONE

- la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice e dall'art. 16, comma 1, del Regolamento del Garante n. 1/2019;

- l'annotazione nel registro interno dell'Autorità delle violazioni e delle misure adottate, ai sensi dell'art. 58, par. 2, del Regolamento, con il presente provvedimento, come previsto dall'art. 17 del Regolamento del Garante n. 1/2019.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 15 aprile 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei
