GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Parere sullo schema di “Linee guida per l’erogazione del servizio pubblico Wi-Fi free” predisposto da AgID - 29 ottobre 2020 [9487928]

VEDI ANCHE NEWSLETTER DEL 1° dicembre 2020

[doc. web n. 9487928]

Parere sullo schema di “Linee guida per l’erogazione del servizio pubblico Wi-Fi free” predisposto da AgID - 29 ottobre 2020

Registro dei provvedimenti
n. 201 del 29 ottobre 2020

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 dott. Claudio Filippi, vice 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 decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del 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”, di seguito Codice;

Visti gli artt. 14-bis e 71 del decreto legislativo 7 marzo 2005, n. 82, recante il “Codice dell’amministrazione digitale” (di seguito CAD) e la determinazione dell’Agenzia per l’Italia digitale (AgID) n. 160 del 2019, recante il “Regolamento per l’adozione di linee guida per l’attuazione del Codice dell’Amministrazione Digitale”, che disciplinano le procedure per l’adozione di linee guida contenenti le regole tecniche e di indirizzo, previa consultazione pubblica e sentiti l’amministrazione interessata e il Garante per la protezione dei dati personali, nonché l’acquisizione del parere della Conferenza unificata;

Vista la richiesta di parere di AgID;

Vista la documentazione in atti;

Viste le osservazioni formulate dal vice segretario generale ai sensi dell’art. 15 del regolamento del Garante n. 1/2000;

Relatore la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

L’AgID ha inoltrato al Garante la richiesta di parere sullo schema di “Linee guida per l’erogazione del servizio pubblico Wi-Fi free”,

già sottoposto a consultazione pubblica, adottato, ai sensi dell'art. 71 del CAD, in attuazione dell'art. 8-bis del CAD, rubricato "Connettività alla rete Internet negli uffici e luoghi pubblici", in base al quale le amministrazioni, i gestori di servizi pubblici e le società a controllo pubblico favoriscono la disponibilità di connettività alla rete Internet presso gli uffici pubblici e altri luoghi pubblici (in particolare, nei settori scolastico, sanitario e di interesse turistico), anche mettendo a disposizione degli utenti la porzione di banda trasmissiva non utilizzata dagli stessi uffici.

In generale, dunque, lo schema è volto a fornire alle amministrazioni locali e nazionali, che intendono mettere a disposizione della cittadinanza un servizio di accesso ad Internet tramite access point (di seguito anche "AP") Wi-Fi, un quadro di riferimento "normativo e tecnologico entro il quale armonizzare le iniziative in essere, con le strategie governative nazionali ed europee".

Lo schema di Linee guida, che sarà oggetto di aggiornamento nel tempo, si applica ai soggetti di cui all'art. 2, comma 2 del CAD (di seguito, in alcuni casi, anche semplicemente "le amministrazioni") e intende fornire indicazioni circa le modalità attraverso le quali può essere resa disponibile la banda destinata al wireless gratuito, anche attraverso il richiamo alla normativa tecnica di settore (famiglia di standard IEEE 802.11x), nonché i criteri di sicurezza che devono essere adottati, in termini di: configurazione della rete interna e modalità di trasporto sulla rete geografica; sicurezza delle comunicazioni; identificazione degli utenti del servizio; prevenzione di potenziali attacchi; monitoraggio del servizio.

Lo schema richiama, tra gli obblighi per i predetti soggetti, quelli di:

- garantire la segregazione degli AP rispetto alla rete interna, attraverso la separazione fisica delle reti o attraverso una separazione logica basata sulla creazione di reti locali virtuali (VLAN) a "livello 2" o "livello 3" dell'architettura di riferimento ISO/OSI;

- dedicare al servizio Wi-Fi free la sola banda non utilizzata, al fine di non compromettere la disponibilità di banda per il funzionamento dei servizi propri dell'amministrazione.

E', inoltre, raccomandato alle amministrazioni di provvedere all'identificazione degli utenti, al fine di poter rintracciare eventuali comportamenti malevoli perpetrati attraverso la propria rete di AP, valutando anche la possibilità di interoperare con le strutture alberghiere per offrire il servizio ai turisti.

RILEVATO

Considerata la delicatezza dei profili coinvolti, si rileva la necessità di apportare integrazioni allo schema in esame, al fine di renderlo pienamente conforme ai principi e alle garanzie in materia di protezione dei dati personali, con specifico riferimento agli aspetti di seguito evidenziati.

1. La progettazione del servizio Wi-Fi free

In primo luogo, si rappresenta che l'attività di erogazione del servizio di Wi-Fi free comporta, da parte dei soggetti di cui all'art. 2, comma 2 del CAD e, in particolare, delle amministrazioni, il trattamento dei dati personali degli utenti che intendono usufruire del predetto servizio, nell'ambito delle varie fasi dell'utilizzo dello stesso, che presentano differenti caratteristiche, anche in ragione dei diversi apparati e servizi di rete impiegati (es. firewall, proxy server, DNS server). In tal senso, occorre, infatti, distinguere i trattamenti di dati personali relativi alla preliminare attività di identificazione degli utenti, in fase di autenticazione all'atto dell'accesso al servizio, da quelli relativi alla successiva fase di utilizzo della rete da parte dell'utente.

Conseguentemente, appare opportuno integrare lo schema al fine di rendere adeguatamente consapevoli le predette amministrazioni, in qualità di titolari, dei rischi che il connesso trattamento di dati personali comporta per le libertà e i diritti degli interessati.

In primo luogo, sarebbe necessario inserire un richiamo di carattere generale - eventualmente nell'ambito del Capitolo 3 rubricato "Framework normativo" - agli obblighi che gravano in capo al titolare, per garantire la conformità al Regolamento, anche assicurando la protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 del Regolamento).

In particolare, è opportuno evidenziare che, nel configurare il predetto servizio (a partire dall'eventuale bando di gara), il titolare deve integrare, in ciascuna fase del trattamento, come sopra descritta, le garanzie volte ad attuare in modo efficace i principi di

protezione dati, con particolare riferimento a:

a) liceità, correttezza e trasparenza del trattamento (art. 5, par. 1 lett. a));

b) limitazione della finalità e minimizzazione dei dati (artt. 5, par. 1, lett. b) e c));

c) limitazione della conservazione (art. 5, par. 1, lett. e));

d)integrità e riservatezza dei dati, adottando misure tecniche ed organizzative per garantire un livello di sicurezza adeguato (artt. 5, par. 1, lett. f), e 32).

2. Trattamento dei dati personali degli utenti

2.1. Identificazione degli utenti e conservazione dei dati

Preliminarmente, si ritiene necessario osservare che, al fine di rispettare il principio di liceità, correttezza e trasparenza nei confronti degli utenti, occorre precisare, che gli obblighi che gravano in capo alle amministrazioni (cc.dd. service provider) sono distinti da quelli che sono imposti dalla legge a carico dei fornitori di servizi di comunicazione elettronica (cc.dd. resource provider).

Pertanto, nello specifico, sarebbe opportuno evidenziare più chiaramente - anche nell'ambito del Capitolo 3, al paragrafo rubricato "Identificazione degli utenti" - che gli obblighi di identificazione degli utenti e di conservazione dei dati di traffico telematico gravano, secondo la normativa di riferimento, esclusivamente in capo agli operatori di telecomunicazione e non, in generale, ai soggetti di cui all'art. 2, comma 2, del CAD considerato che, anche quando offrono il servizio Wi-Fi free, questi ultimi non sono equiparabili ai "fornitori di servizi di comunicazione elettronica".

Nello schema viene, invece, raccomandato alle amministrazioni di dotarsi "di sistemi di identificazione (e autenticazione) dell'utente, ovvero consentano l'accesso attraverso dispositivi personali il cui rilascio prevede l'identificazione"; ciò al fine di consentire di risalire all'autore di un'eventuale condotta illecita, perpetrata attraverso l'uso del servizio Wi-Fi free (sul punto, si evidenzia, peraltro, la non pertinenza del richiamo al provvedimento del Garante n. 106 del 30 aprile 2019 - cfr. nota n. 6 dello schema - considerato che, nel caso specifico, l'AP attraverso cui è stato effettuato l'accesso fraudolento alla rete faceva parte della rete intranet di una società).

Al riguardo, considerato che i soggetti che forniscono accesso ad Internet, tramite Wi-Fi free, non sono in ogni caso legittimati a implementare sistemi di tracciamento che comportano la conservazione dei dati relativi al traffico telematico, effettuato dagli utenti tramite i propri AP Wi-Fi, si osserva che nello schema in esame non si forniscono indicazioni sugli eventuali trattamenti di dati personali che, conseguentemente, le amministrazioni dovrebbero porre in essere per consentire di individuare, a posteriori, i responsabili di eventuali condotte illecite, nel rispetto dei principi di proporzionalità e minimizzazione (ad es. conservando i dati relativi alla connessione e disconnessione degli utenti e non i dati relativi al traffico telematico).

Al fine di disciplinare adeguatamente il trattamento dei dati personali degli utenti, posto in essere dai soggetti di cui all'art. 2, comma 2, del CAD, per l'esecuzione del compito di interesse pubblico consistente nell'offerta del servizio Wi-Fi free, ai sensi dell'art. 8-bis del CAD, con particolare riferimento alla fase di identificazione degli utenti e alla conservazione dei dati, occorre che lo schema in esame sia integrato fornendo indicazioni alle amministrazioni in relazione a:

a) l'individuazione dei dati personali degli utenti da raccogliere e conservare nell'ambito del predetto processo di identificazione, nel rispetto del principio di minimizzazione (art. 5, par. 1 lett. c) del Regolamento);

b) se del caso, la minimizzazione dei dati di cui è consentita la conservazione al solo fine di individuare, a posteriori, i responsabili di eventuali condotte illecite, senza effettuare tracciamenti, non necessari, relativi al traffico telematico riferito agli utenti (art. 5, par. 1, lett. b) e c) del Regolamento);

c) le modalità che, eventualmente, si intendono utilizzare per impedire l'accesso a determinate tipologie di siti o servizi in rete, configurando i sistemi e gli apparati, a tal fine utilizzati, evitando di conservare i dati al traffico telematico effettuato dagli utenti (art. 5, par. 1, lett. c), del Regolamento);

d) l’individuazione, per ciascuna delle tipologie di dati trattati, di adeguati tempi di conservazione dei dati, nel rispetto del principio di limitazione della conservazione (art. 5, par. 1, lett. e), del Regolamento);

e) le misure adottate per assicurare il rispetto del principio di trasparenza nei confronti degli interessati, con l’indicazione puntuale della finalità perseguita, delle tipologie di dati oggetto di trattamento e dei tempi di conservazione dei dati (art. 5, par. 1, lett. a) del Regolamento).

2.2. Interoperabilità con strutture alberghiere

Per quanto concerne l’identificazione dei “turisti” (par. 5.1.8), lo schema prevede che le amministrazioni possano “interoperare con le strutture alberghiere al fine di poter assegnare credenziali per l’utilizzo della Wi-Fi gratuita per il periodo di permanenza in Italia”.

In generale, si rappresenta che tale modalità di interoperabilità può essere attuata con più scenari d’uso, esemplificati nello schema in esame, che comportano diverse conseguenze in termini di trattamento dei dati personali degli utenti, in relazione ai quali occorre precisare i ruoli assunti dai vari soggetti coinvolti, nell’ambito del trattamento, e le diverse misure che devono essere adottate a garanzia degli interessati.

In ogni caso, deve essere chiarito che la predetta interoperabilità non deve automaticamente prevedere la comunicazione alle amministrazioni dei dati dei clienti delle strutture alberghiere aderenti all’iniziativa, e il turista deve poter decidere autonomamente se aderire al servizio di Wi-Fi free in interoperabilità o utilizzare la sola connettività alberghiera.

3. Sicurezza dei dati e dei sistemi

Nell’ambito delle attività poste in essere per offrire il servizio di Wi-Fi free intervengono soggetti diversi che possono trattare i dati personali degli utenti quali, in particolare, il service provider, ossia la pubblica amministrazione, e il resource provider, ovvero il fornitore di servizi di comunicazione elettronica.

Nel richiamare quanto già indicato con riferimento al processo di identificazione da parte degli albergatori, si rappresenta, in generale, la necessità che siano configurati correttamente i ruoli e i compiti assunti nel trattamento dei dati personali dai diversi soggetti coinvolti nell’erogazione del predetto servizio, anche con specifico riferimento agli obblighi di sicurezza che ricadono in capo ai predetti soggetti (art. 32 del Regolamento e art. 132-ter del Codice), già nell’ambito delle clausole contrattuali del contratto di fornitura del servizio di comunicazione elettronica.

Sul tema della sicurezza, in generale, occorre assicurare una corretta applicazione del Regolamento e, conseguentemente, integrare lo schema (anche nell’ambito del Capitolo 5 rubricato “Criteri di implementazione del servizio per le PA”), tenendo conto degli obblighi previsti in materia di sicurezza dei dati e dei sistemi dal Regolamento, in ragione dei rischi che possono derivare agli utenti connessi ad una rete Wi-Fi non adeguatamente protetta.

Al fine di promuovere una corretta applicazione del Regolamento da parte delle amministrazioni e dei loro fornitori, si ritiene che il riferimento alle misure “minime di sicurezza” di cui al par. 5.1.5, non sia conforme ai più ampi obblighi di sicurezza previsti dal Regolamento. Come più volte ribadito da questa Autorità (cfr. da ultimo, il provvedimento n. 32 del 13 febbraio 2020), il concetto di misure minime non è di per sé sufficiente ad assicurare la conformità al Regolamento, a norma del quale, occorre invece valutare, in concreto, i rischi che possono derivare, in particolare, dalla divulgazione non autorizzata o dall’accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Le misure tecniche ed organizzative che, infatti, il titolare e il responsabile del trattamento sono tenuti ad adottare, devono essere tali da garantire un livello di sicurezza adeguato al rischio, che presenta il 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” (art. 32 del Regolamento).

Considerato quanto sopra, si rappresenta dunque la necessità che sia introdotto un richiamo specifico agli obblighi di sicurezza previsti dal citato art. 32 del Regolamento, volto ad esplicitare l’obbligo di adottare misure tecniche e organizzative adeguate, per assicurare la disponibilità e l’integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti, nonché di adottare procedure per la gestione delle violazioni di dati personali (artt. 33 e 34 del Regolamento), nonché, per quanto riguarda l’attività svolta dal resource provider, all’art. 132-ter del Codice relativo alla sicurezza del trattamento nella fornitura dei servizi di comunicazione elettronica.

In particolare, si ritiene, inoltre, opportuno integrare lo schema (anche eventualmente nell'ambito del paragrafo "Sicurezza e prevenzione di potenziali attacchi") con indicazioni più puntuali rivolte alle amministrazioni, relative ai livelli di sicurezza, affinché i trattamenti dei dati vengano posti in essere in modo conforme alle garanzie previste in materia di protezione dei dati personali, con specifico riferimento alla necessità di:

- adottare misure di sicurezza volte ad impedire che, tramite il servizio pubblico Wi-Fi free, sia possibile accedere a risorse di rete interne (es. postazioni di lavoro, portale intranet o altri servizi interni) o ad altre risorse esposte su rete SPC;

- individuare specifiche cautele nel caso in cui il servizio pubblico Wi-Fi free sia utilizzato anche dai dipendenti della pubblica amministrazione che fornisce il servizio;

- prevedere il divieto esplicito di trattamento dei dati relativi ai dispositivi degli utenti, a fini di tracciamento dell'ubicazione o degli spostamenti, mediante tecniche di Wi-Fi location tracking.

Da ultimo, anche alla luce di quanto statuito dalla Corte di giustizia nella recente sentenza relativa al caso cd. Schrems II (16 luglio 2020, causa C-311/18), è opportuno evidenziare che con riferimento alla possibile migrazione del controller fisico in un'infrastruttura cloud (prevista nell'ambito del Capitolo 6 rubricato "Possibili evoluzioni tecnologiche del servizio"), l'eventuale scelta del fornitore, qualora esterno all'amministrazione, deve rispondere a tutte le garanzie previste dal Regolamento in relazione ai trattamenti effettuati al di fuori dell'Unione europea.

RITENUTO

Considerato quanto sopra si ritiene che lo schema in esame debba essere opportunamente integrato, come rilevato ai precedenti paragrafi 1, 2 e 3, al fine di assicurare la conformità ai principi e alle garanzie previsti dal Regolamento e dal Codice nel trattamento di dati personali effettuato dai soggetti che erogano servizi Wi-Fi free, ai sensi dell'art. 8- bis del CAD.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 36, par. 4, e 57, comma 1, lett. c), del Regolamento, esprime parere nei termini di cui in motivazione sullo schema di "Linee guida per l'erogazione del servizio pubblico Wi-Fi free", predisposto da AgID, ai sensi dell'art. 14-bis e art. 71 del decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale.

Roma, 29 ottobre 2020

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL VICE SEGRETARIO GENERALE
Filippi