CONFERENZA DELLE REGIONI
E DELLE PROVINCE AUTONOME

19/55/CR8b/C14

Posizione sullo Schema di "Linee guida per l'erogazione del servizio pubblico wi-fi free"

Introduzione

Va chiarito fin da subito che molte Regioni, autonomamente o attraverso accordi o convenzioni con altri Enti Pubblici, offrono il servizio di accesso pubblico alla Rete attraverso wifi, lo fanno secondo il principio che ritiene l'accesso ad Internet un diritto che andrebbe garantito a tutti i cittadini in quanto sempre più l'esercizio della propria appartenenza ad una comunità, le attività di vita e lavoro, la socialità e la fruizione, da ultimo ma non ultima, di servizi pubblici passa dal Web. Il servizio di wifi è offerto sempre gratuitamente, si prediligono spazi pubblici che risultano maggiormente frequentati e ove possibile si spinge per creare tale opportunità anche in aree decentrate, isolate o marginali di città e territori nella convinzione che l'accesso alla Rete non debba diventare una discriminante e non debba produrre nuove marginalizzazioni. Le esperienze pubbliche e private di reti wifi ad accesso pubblico hanno evidenziato due punti particolarmente critici: 1) il processo di registrazione/autenticazione/identificazione che spesso se complesso scoraggia gli utenti all'uso del servizio; 2) la qualità dell'esperienza utente, in termini di velocità di navigazione, che in molti casi è limitata o deludente. Le Regioni nelle loro esperienze hanno tentato di intervenire su questi aspetti e quindi hanno maturato un'elevata esperienza, identificato e messo in atto soluzioni, misurato impatto in termini di utilizzo del servizio. Per queste ragioni si propongono di seguito alcune considerazioni e una descrizione di esperienze in essere al fine che siano tenute in considerazione nel processo di integrazione e revisione delle Linee Guida AgID successivo alla fase di consultazione avvenuta nel corso del mese di febbraio e primi giorni di marzo.

Posizione delle Regioni e Province Autonome

Nelle Linee Guida (LG), dove in linea generale i requisiti funzionali sono condivisibili, si osserva in primo luogo come l'**introduzione di una identificazione obbligatoria** ridurrebbe significativamente la capacità e potenzialità di sviluppo e diffusione del wifi gratuito ed introdurrebbe un fardello poco efficace opposto alla necessità, fatta propria dalle amministrazioni pubbliche, di garantire una sempre più capillare diffusione della rete e della fruizione di servizi ad essa connessi.

Peraltro, sfugge alle LG, la sostanziale differenza tra **autenticazione** e **identificazione**. In tal senso, AGID[1], nella sezione del proprio sito istituzionale dedicata al regolamento EIDAS, assume che "***L'identificazione*** *elettronica è un processo in cui si usano i dati di autenticazione personale in forma elettronica per identificare*

[1] https://www.agid.gov.it/it/piattaforme/eidas/identificazione-autenticazione-elettroniche

univocamente: una persona fisica e una persona giuridica. ***L'autenticazione*** *elettronica è il processo che permette di assicurare il riconoscimento dell'utente elettronico.".*

Va tenuto inoltre in considerazione lo stato attuale di alcune amministrazioni Regionali che hanno adottato soluzioni per garantire l'accesso alle reti wifi senza autenticazione (adottando anche regolamenti specifici per esempio per ospiti all'interno di alcuni edifici, oppure applicando la norma generale e destinando tale servizio a tutti gli utenti). Infatti si ricorda che l'attività di una pubblica amministrazione non ha come scopo prevalente quello di erogare ed offrire servizi di accesso ad Internet. Quindi si ritiene sarebbe indispensabile prevedere, all'interno delle LG, anche l'opzione della non identificazione "personale degli utilizzatori" se, come previsto dalla norma, i provider infrastrutturali sono le pubbliche amministrazioni (vedi art. 10 del decreto del <<Fare>>, giustamente citato all'interno delle LG e l'allegato al presente documento "Considerazione di carattere normativo").

Inoltre si osserva che nella realtà di alcune piccole amministrazioni, alcuni requisiti funzionali indicati all'interno delle LG potrebbero non essere al momento soddisfatti e ciò comporta anche un impatto oneroso economicamente per l'adeguamento tecnologico/operativo non dovuto a norma di legge. In linea generale le LG dovrebbero quindi indicare quali "**opzioni**" e non requisiti per l'erogazione del servizio.

Osservazioni e proposte di integrazione

Nel caso di accesso con registrazione/autenticazione/identificazione:

- potrebbe aver senso definire regole comuni e di sistemi di verifica per l'accesso da parte dei **minori d'età** qualora si voglia considerare l'accesso anche per questa tipologia di utenti;
- rispetto alle **misure minime di sicurezza**, non si ritiene necessario un sistema di Data Loss Prevention, se le reti di accesso per il wifi pubblico sono separate e segregate. Il DLP necessita di agent a bordo dei client e, oltre a non essere applicabile nello scenario previsto, non sarebbe neanche attuabile su utenze ospiti (non potendo installare agent sui loro client). Si ritiene invece più opportuno che l'erogatore del servizio disponga di un sistema di "intrusion detection and prevention" in grado di monitorare costantemente la rete per verificare e bloccare tentativi di intrusione fraudolenta.

In tutti i casi:

- si ritiene utile condividere politiche di **URL Filtering** tra tutte le Amministrazioni che intendono erogare il servizio per uniformare l'esperienza di accesso dell'utente; si precisa però che non è detto che tutte le Amministrazioni siano già pronte per l'adozione di tali meccanismi oltre al fatto che l'Unione Europea nella sua iniziativa WiFi4EU richiede, quale condizione al finanziamento dei punti WiFi, che sia garantito il principio di neutralità e non siano applicati filtri alla navigazione;
- si ritiene utile condividere politiche in caso di **infringement** (incidenti di sicurezza, violazioni di copyright, ecc.) relativamente alla gestione degli utenti coinvolti o agli indici di compromissione;
- alcuni requisiti espressi rispetto ai **criteri di implementazione del servizio** da parte delle pubbliche amministrazioni come, ad esempio, la necessità che tutti gli Access Point siano collegati alla **rete cablata** non possono trovare applicazione in alcune zone del territorio (alcune amministrazioni hanno fatto uso di collegamenti in ponte radio per aree particolarmente disagiate), seppure il principio sia largamente condiviso e l'obiettivo debba essere quello di ricercare e offrire la migliore esperienza utente possibile.

Rispetto poi alle **modalità di federazione**, la consultazione riporta il seguente capoverso:
"…Le modalità tecnologiche di realizzazione delle federazioni sono diverse, ad esempio:

- *si possono utilizzare le stesse credenziali su reti afferenti a diversi Service Provider, che propaghino reciprocamente le credenziali e gli SSID delle infrastrutture federate;*
- *l'accesso utente con la stessa password su due reti identificate da diversi SSID; in tale scenario le Amministrazioni dovranno sincronizzare i database degli utenti. …."*

In merito a questo passaggio si evidenzia che le credenziali non devono essere propagate sulle infrastrutture federate; esistono invece meccanismi di federazione che consentono di verificare l'identità degli utenti di rete diverse (quali meccanismi tipo Proxy Radius o basati su SAML, come avviene ad esempio con SPID). Anche il secondo punto non si ritiene applicabile per il medesimo motivo: in una federazione non si devono "sincronizzare" i database degli utenti. Ogni utente, con i propri dati identificativi, esiste unicamente nel DB dell'amministrazione in cui è stato registrato: è la federazione che consente, mediante la verifica dell'identità remota, l'accesso ad una rete che non ha nei propri DB l'utenza, non la replica dei dati. Tale scenario andrebbe quindi rivisto.

Le maggiori esperienze della Wi-Fi pubblica nella PA

Quali ulteriori esempi che potrebbero essere presi in considerazione ed inseriti nelle linee guida possiamo citare quelli presenti sul territorio della Regione Piemonte, della Regione Emilia-Romagna e della Regione Liguria (di seguito descritti) ma non sono da dimenticare anche esperienze come quella della Provincia Autonoma di Trento (TrentinoWiFi), quella della Regione Friulia Venezia Giulia (FVG WiFi), Regione Lazio (Free Lazio WiFi), ecc… Sono infine da ricordare le numerose e molto spesso storiche esperienze di grandi e piccole città come solo a titolo di esempio Firenze, Genova, Venezia, ecc….

Piemonte

In Piemonte sono attualmente erogate **tre tipologie di servizio wifi free**, legate a indirizzi diversi da parte degli Enti promotori.

1. Città di Torino, il servizio FreeTorinoWiFi, aderente alla maggiore federazione nazionale FreeItaliaWiFi[2] (non menzionata nelle LG e sostanzialmente già in grado di erogare i servizi come delineati nella documentazione oggetto di discussione) e dai cui eredita le principali regole tecniche:
    a. Navigazione con autenticazione;
    b. Credenziali d'accesso:
        i. Servizio di registrazione in self provisioning, con credenziali spendibili su tutte le reti wifi aderenti alla Federazione FreeItaliaWiFi (attualmente 7.000 host spot attivi, 90 reti federate, 2.700.000 utenti)
        ii. SPID e, in dismissione, credenziali TorinoFacile (accesso ai servizi on line della Città con credenziali locali)
        iii. Carta di Credito, con transazione a zero costi per l'utente (per chi non può accedere con le modalità precedenti: turisti e stranieri, ad esempio)
    c. Navigazione senza filtri d'accesso, puntando alla responsabilizzazione dell'utente e limitata nei volumi o nella durata (700 Mb o 8 ore al giorno)
    d. Divieto di tracking e profilazione utenze, divieto di veicolazione di contenuti commerciali

[2] http://freeitaliawifi.it/

2. Diversi Enti locali (Città di Cuneo, Vercelli, Alba, Pinerolo, ecc.), hanno aderito al Servizio FreePiemonteWiFi, simile al precedente ma privo di alcune personalizzazioni richieste dalla Città di Torino. Anche per questo servizio è previsto l'accesso in autoregistrazione o con SPID e, in dismissione, l'accesso con credenziali SistemaPiemonte (accesso ai servizi on line della Regione Piemonte con credenziali locali).

Le credenziali di queste due reti sono mutualmente riconosciute, secondo i principi base della federazione, alla pari di tutte quelle rilasciate all'interno del circuito FreeItaliaWiFi.
Ad oggi, i due servizi piemontesi sono utilizzati da oltre 170.000 utenti registrati, a cui vanno aggiunti i cittadini in possesso di credenziali TorinoFacile o SistemaPiemonte, gli utenti che accedono con SPID e gli stranieri che accedono con Carta di Credito; gli accessi unici giornalieri sono circa 1.500.
Come esempio di terzo servizio erogato si cita un servizio di accesso WiFi limitato agli edifici della Regione Piemonte che, in forza di una specifica Legge Regionale (n.5/2011), consente l'accesso degli utenti ospiti senza autenticazione ma con navigazione degli utenti soggetta ad url filtering controllo dei contenuti malevoli.
L'accesso a queste tre tipologie di servizio è garantito in modo da salvaguardare la separazione e la segregazione del traffico rispetto a quello delle reti dove insistono i servizi interni delle Pubbliche Amministrazioni aderenti come richiesto dalle LG proposte.

Emilia-Romagna

"EmiliaRomagnaWiFi" è il SSID diffuso da più di 6700 access points (a febbraio 2019) situati in luoghi pubblici del territorio regionale (piazze, aree commerciali, zone turistiche, giardini pubblici, biblioteche, ospedali, impianti sportivi, teatri etc.). La rete WiFi regionale è messa a disposizione gratuitamente tramite Lepida ScpA, la società in house della Regione e di oltre 400 enti soci. La rete ha implementato e sostituito le reti esistenti (dei Comuni, delle ASL, delle biblioteche, ecc...).
Lepida ScpA agisce in qualità di controllata - ricordiamo che ai sensi dell'art. 6, comma 1 del Codice delle Comunicazioni Elettroniche "lo Stato, le Regioni e enti locali , o loro associazioni, non possono fornire reti o servizi di comunicazione elettronica accessibili al pubblico, se non attraverso società controllate o collegate" - ed è dotata di autorizzazione generale ex art. 25 del d.lgs. n. 259/2003 per le reti e i servizi di comunicazione elettronica. Tali funzioni vengono attribuite a Lepida mediante la Legge Regionale n. 11/2004,

Le caratteristiche principali del servizio EmiliaRomagnaWiFi, definite dalla Delibera di Giunta Regionale n. 137/2017, sono:

- **unico SSID "EmiliaRomagnaWiFi"** per tutto il territorio regionale;
- **velocità di connessione a banda ultra larga**: gli access point sono connessi direttamente in fibra ottica alla rete Lepida (la rete di proprietà degli enti pubblici regionali nata per fornire cablaggi in fibra ottica a municipi, ospedali, scuole ed altri edifici pubblici della regione);
- **assenza di autenticazione**: per rendere il meccanismo di aggancio alla rete semplice e immediato, in modo particolare ai non residenti (es. turisti, lavoratori di passaggio);
- **libertà e gratuità del servizio**.

È opportuno evidenziare il percorso che ha portato alla scelta di non richiedere l'autenticazione degli utenti.

Fino all'inizio del 2017 la rete degli access point regionale irradiava un solo SSID ("Wisper") con richiesta di registrazione e autenticazione degli utenti.
In più occasioni la necessità di registrazione si è rivelata un ostacolo alla fruizione semplice e immediata del servizio. A seguito della abrogazione dei commi del decreto Pisanu, che prevedevano gli obblighi di monitoraggio e preventiva identificazione degli utenti, Regione Emilia-Romagna ha deciso di affiancare all'SSID con autenticazione "Wisper" il nuovo SSID "EmiliaRomagnaWiFi" che non richiede autenticazione.
Oggi stimiamo che il servizio EmiliaRomagnaWiFi (caratterizzato da Banda Ultra Larga, pubblico, libero, senza autenticazione e gratuito) sia utilizzato da oltre 1.5 milioni di utenti unici su base semestrale, a fronte di circa 10.0 utenti registrati per il servizio di WiFi con autenticazione. Inoltre anche il confronto fra i dati di utilizzo di banda dei due servizi http://bit.ly/2IVyJPb confermano un importante aumento dell'uso del servizio WiFi pubblico a seguito dell'introduzione di EmiliaRomagnaWiFi senza autenticazione.

Liguria

Regione Liguria mediante il progetto LiguriaWIFi ha realizzato un sistema di wi-fi pubblico e gratuito diffuso sul territorio regionale in 200 comuni su 234. La registrazione avviene, una volta rilevata la rete LiguriaWIFI, attraverso un captive portal nel quale devono essere inseriti "una tantum" i dati richiesti, numero di telefono del cellulare, nome e cognome dell'utente e data di nascita e indirizzo e-mail. A fronte dell'inserimento dei dati viene inviato un SMS al numero di cellulare indicato, contenente un codice di accesso e un link che rimanda alla pagina di accesso al servizio. Dopo il primo accesso alla rete ogni qual volta l'utente si trovi in un'area coperta dal servizio sarà "agganciato" automaticamente alla rete e potrà iniziare ad utilizzare la connessione. La registrazione è valida su tutto il territorio ligure.
Qualora non si disponga di un dispositivo dotato di scheda SIM, è possibile effettuare la registrazione utilizzando il numero di carta di credito, l'operazione è ovviamente a costo 0 per l'utenza. Questa modalità è valida anche per gli utenti stranieri appartenenti a paesi il cui prefisso internazionale non è elencato tra quelli selezionabili nella pagina di registrazione, laddove non c'è certezza che il proprietario della SIM sia stato identificato.
Per la realizzazione delle aree WiFi, Regione Liguria fornisce ai comuni aderenti l'hardware costituito da gateway e access point, i servizi di installazione, configurazione e manutenzione, nonché "l'aggancio" alla piattaforma centrale di autenticazione, manutenuta da Gugliegmo per conto di Regione Liguria.
Al Comune aderente è richiesto di mettere a disposizione una connettività ADSL adeguata e l'energia elettrica per alimentare gli apparati sopra citati.

Alcuni dati sull'utilizzo della rete riferiti all'anno 2018:

- Numero connessioni: 10.800.000
- Numero Utenti: 5.000.000
- Traffico in download: 222,4 Terabyte di traffico in download
- Traffico in upload: 24 Terabyte

Circa il tema della sicurezza, sui gateway forniti ai Comuni, nel caso in cui la connettività sia condivisa con gli stessi uffici comunali, è possibile attivare e configurare un sistema firewall con il fine di separare il traffico WiFi pubblico da quello interno. La sicurezza a livello locale (comunale) è demandata ai singoli Comuni.

LiguriaWiFi è dotato di un sistema di monitoraggio centralizzato della rete, che agisce in proattività, fornendo ai Comuni e a Regione Liguria le informazioni in tempo reale circa il funzionamento o meno degli apparati installati sul territorio. In questo modo i Comuni sono immediatamente avvisati di possibili malfunzionamenti dei sistemi e invitati a eseguire delle semplici operazioni di ripristino, in modo da garantire la disponibilità del servizio.
Viene considerato un punto di forza del sistema il servizio di assistenza a disposizione sia degli utenti che dei Comuni aderenti, attraverso l'attivazione di due canali di comunicazione, un numero verde e una casella e-mail. Attraverso tali canali si possono inoltrare richieste di assistenza sia per problematiche tipicamente legate agli utenti (registrazione, account) sia legate al funzionamento del servizio stesso.

WIFI.italia.it

Per quanto riguarda il progetto, citato nel paragrafo delle maggiori esperienze, **WIFI.italia.it**, si presenta come lo strumento per la realizzazione di un sistema di accesso unico e semplificato per i cittadini italiani e per i turisti, in grado di favorire riuso e razionalizzazione di spesa per quanto riguarda le soluzioni tecnologiche adottate dalle PA, tuttavia presenta vincoli tutt'altro che insignificanti: la registrazione e l'accesso alla rete può avvenire solo attraverso l'utilizzo di apposita App (e installazione di un eseguibile software), inoltre il servizio non è fruibile su Pc, ma solo su smartphone e tablet. L'adesione di altre reti wifi al sistema non sembra porsi in termini di federazione, ma piuttosto come una implementazione in parallelo, con l'erogazione di un nuovo SSID sugli hotspot della rete "aderente". Non è chiaro quindi cosa si intenda per "reti federate" quando si dice che *"il sistema wifi.italia raccoglie e gestisce i dati di registrazione degli utenti e di quelli relativi alle loro autenticazioni sulle reti federate, anonimizzandoli e solo per i fini dell'esecuzione del servizio"*. Forse sarebbe più corretto parlare di infrastrutture ospitanti. Proponendo altresì alle *"amministrazioni di dismettere i sistemi di autenticazione e la gestione delle identità degli utenti per utilizzare l'accesso a wifi.italia"*, non si tiene conto degli investimenti pregressi fatti dalle amministrazioni per la creazione della propria piattaforma. Di contro, anche dalla documentazione presente sul sito, non risultano i livelli di servizio forniti dal gestore della piattaforma wifi.italia, ad esempio in termini di assistenza all'utente.

Considerazioni di carattere normativo
Nella parte relativa al framework normativo si rilevano alcune contraddizioni che riportiamo di seguito in forma sintetica e, in allegato, la forma estesa.

In primo luogo, si ritiene discriminante e inefficace disciplinare in maniera difforme la somministrazione dei servizi wifi da parte di soggetti pubblici e privati. La limitazione del perimetro delle linee guida ai soli soggetti di cui all'art. 2 comma 2 del CAD produce l'effetto distorsivo di un'arbitraria rigidità per i soggetti pubblici e di un esercizio di libero arbitrio - nelle valutazioni delle responsabilità che da tale servizio discendono - per i soggetti privati. Le esigenze di sicurezza non sembrano risolte con la richiesta di autenticazione degli utenti, considerato anche che il D.L. 21 giugno 2013, n. 98, art. 10 ha liberalizzato l'accesso alla rete internet tramite tecnologia Wi-Fi, escludendo qualsiasi obbligo di preventiva autenticazione da parte degli utilizzatori.

Per quanto riguarda gli specifici obblighi di sicurezza in capo al provider del servizio, sussistono, d'altra parte, notevoli criticità per gli Enti pubblici in ordine all'effettuazione di trattamenti di dati personali che il legislatore ha già valutato come non necessari (art. 10 D.L. 98/2013). Per di più, sussiste una platea ampia di soggetti privati, che possono ricoprire sostanzialmente il ruolo di provider, che non ricadono nell'ambito di applicazione materiale del GDPR (c.f.r art. 2 par. 2 lett. c) dello stesso GDPR). E', invece, evidente come la somministrazione di un servizio wi-fi senza autenticazione abbia un impatto, in termini di protezione dei dati personali, certamente meno critico, in ragione del fatto che, richiedendo l'autenticazione agli utenti, devono essere trattati i dati relativi a username e password degli stessi, oltre eventualmente a numero di telefono, estremi della carta di credito ecc.
In termini di responsabilità civile del provider in caso di fatto illecito di terzi, le linee guida non tengono in debito conto gli approdi giurisprudenziali dell'Unione Europea e dei tribunali internazionali sul tema, anche con riferimento alla significativa omogeneità di indirizzo interpretativo teso ad escludere la sussistenza di oneri di registrazione degli accessi da parte dei provider che forniscono connettività wifi. Ad es. nel noto caso Tobias McFadden c. Sony Music Entertainment Germany GMBH, la Corte di Giustizia Europa, con sentenza del 15.09.2016, causa C-484/14, ha stabilito che il provider del servizio wi-fi non può essere ritenuto responsabile delle informazioni trasmesse dai destinatari di tale servizio a condizione che non dia origine esso stesso alla trasmissione, non selezioni il destinatario della trasmissione e non selezioni né modifichi le informazioni trasmesse (art. 12, paragrafo 1, della direttiva 2000/31/CE). Infine si rileva come l'autenticazione elettronica priva di un comprovante sistema di identificazione non consente l'acquisizione di informazioni nodali ai fini della detonazione di illeciti. Pertanto, la conseguenza sarebbe quella di subordinare l'accesso al wifi non solo a sistemi di autenticazione tout court, ma a sistemi di autenticazione basati su sistemi di identificazione certa.
Se l'obiettivo che devono porsi le Amministrazioni consiste nell'assecondare l'esercizio di un diritto fondamentale dei cittadini di accesso alla rete ed ai servizi ad essa connessi, è evidente come l'autenticazione costituisca un fardello inutile e poco efficace rispetto alle esigenze di sicurezza conclamate nelle Linee guida.

Proposta di percorso di adeguamento alle Linee Guida

Si richiede pertanto di voler dare corso ad una revisione delle suddette LG anche in collaborazione con una rappresentanza delle Regioni e Province Autonome che possa portare il punto di vista di diverse PA che sul tema hanno sviluppato esperienze e competenze da mettere a fattor comune.

ALLEGATO - Considerazioni di carattere normativo

Con riferimento a quanto specificatamente prescritto al par. 4.1 per i provider del servizio di wi-fi, il primo cahier de doleance è riferito all'ambito di applicazione delle linee guida.

L'assunto logico e lapalissiano è che solo l'omogeneità di regolamentazione delle modalità di usufruizione dei servizi di wi-fi consente di assolvere alle asserite esigenze di sicurezza rappresentate nel documento in consultazione.

La limitazione del perimetro delle linee guida ai soli soggetti di cui all'art. 2 comma 2 del CAD produce l'effetto distorsivo di un'arbitraria rigidità per i soggetti pubblici e di un esercizio di libero arbitrio - nelle valutazioni delle responsabilità che da tale servizio discendono - per i soggetti privati. Si tratta di una misura che ha nel suo ambito di applicazione uno dei suoi principali vulnus, in nome di esigenze di sicurezza che la richiesta autenticazione degli utenti certamente non risolve.

Esigenze, si noti, non fatte proprie dal legislatore, che, come pure riportato da Agid, con l'adozione D.L. 21 giugno 2013, n. 98, art. 10 ha liberalizzato l'accesso alla rete internet tramite tecnologia Wi-Fi, escludendo qualsiasi obbligo di preventiva autenticazione da parte degli utilizzatori, disponendo che "1. L'offerta di accesso alla rete internet al pubblico tramite tecnologia WIFI non richiede l'identificazione personale degli utilizzatori. Quando l'offerta di accesso non costituisce l'attività commerciale prevalente del gestore del servizio, non trovano applicazione l'articolo 25 del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, e successive modificazioni, e l'articolo 7 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, e successive modificazioni".

E postulando la perfezione del nostro ordinamento giuridico, se non come approdo di certo come anelito, sarebbe inammissibile la presenza di una norma del CAD in contraddizione la disposizione di legge sopra richiamata (ed infatti siffatta disposizione è assente nel Codice).

Tale inammissibilità appare ancora più manifesta nell'eventualità, nostro malgrado verificatasi, che fossero proprio le linee guida, che pure devono limitarsi a fornire "le regole tecniche e di indirizzo per l'attuazione del presente Codice [dell'Amministrazione digitale]" a produrre tale contrapposizione incoerente con la norma primaria citata. I saggi, cui è riconosciuta la perentorietà della sintesi, avrebbero sostenuto "Absurda sunt vivanda".

Peraltro, dal punto di vista sistematico, nel documento l'autenticazione degli utenti viene incardinata negli oneri di gestione della sicurezza della rete, fissando alcuni punti che in nessuna misura colgono nel segno.

Infatti, l'entrata in vigore del Regolamento UE 2016/679 non ha imposto nuovi vincoli di sicurezza, in soluzione di continuità rispetto alla precedente normativa.

Agid sostiene che "secondo le normative sulla privacy in vigore sia a livello nazionale che europeo, con particolare riferimento al Regolamento Ue 2016/679, il cosiddetto GDPR, chi effettui trattamento di dati personali di utenti deve avvalersi di misure tecnicamente in grado di assicurare la protezione di suddetti dati, rendendoli sicuri da intrusioni esterne o interne alla rete".

Si osserva, in prima battuta, che far discendere l'obbligazione generale di sicurezza delle reti wifi dalla normativa in materia di protezione dei dati personali comporta un'ontologica disomogeneità di attuazione, in ragione dell'ambito di applicazione materiale del GDPR che all'art. 2 par. 2 lett. c) prevede l'esclusione dei

trattamenti di dati personali "effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico".
Si osserva inoltre che, ai fini della connettività, si renderebbe necessario il trattamento di un insieme limitato di dati (ad es. mac-address) dei dispositivi e non delle credenziali di identificazione/ e/o di autenticazione degli utenti, del loro numero di cellulare o del numero di carta di credito ecc. Emerge, in tutta evidenza, che la gestione degli accessi alle reti wi-fi ha un impatto, in termini di protezione dei dati personali, connotato da un indice di rischio elevatissimo, che un accesso senza autenticazione, d'altra parte, non presenta.
Si sostiene nelle Linee Guida, nel citato par. 4.1, che

- "rendere disponibile agli utenti la connettività Internet implica responsabilità secondo il Codice Civile e secondo i principi della responsabilità oggettiva, dei danni causati da eventuali attività non lecite commesse da parte degli utenti, a meno di non aver messo in pratica tutte le misure necessarie a controllare il servizio e a impedire che gli atti illeciti potessero essere commessi" e che
- "è tuttavia necessario dotarsi di sistemi di gestione della connettività e dell'autenticazione che permettano all'operatore di poter tracciare il traffico telematico degli utenti per poter rispondere ai suddetti obblighi".

Postulare la responsabilità civile, in termini di responsabilità oggettiva, del provider del servizio wi-fi è interpretazione che non tiene in debito conto gli approdi giurisprudenziali, anche europei, in materia: pronunce giudiziali che assegnano all'autenticazione una rilevanza inconsistente dal punto di vista delle responsabilità civili e penali e inefficace dal punto di vista tecnologico.
Tale indirizzo cotanto perentorio è in palese contrasto con quanto sostenuto dalla Corte di Giustizia dell'Unione Europea, ad esempio nel caso Tobias McFadden c. Sony Music Entertainment Germany GMBH, (sentenza del 15.09.2016, causa C-484/14) che ha escluso la responsabilità dei gestori di hotspot per i reati commessi dagli host. Il caso concerneva l'utilizzo da parte di un terzo della rete locale wireless gestita dal sig. McFadden, il quale veniva reso disponibile al pubblico il servizio senza procedure di autenticazione.
La Corte assume che il provider del servizio wi-fi non può essere ritenuto responsabile delle informazioni trasmesse dai destinatari di tale servizio a condizione che non dia origine esso stesso alla trasmissione, non selezioni il destinatario della trasmissione e non selezioni né modifichi le informazioni trasmesse (cfr. art. 12, paragrafo 1, della direttiva 2000/31/CE).
Ammessa, solo per un attimo, la configurabilità della responsabilità oggettiva ex art. 2051 c.c., la fattispecie in oggetto trova la sua principale direttrice nel rapporto di custodia, ovvero nel legame intercorrente tra un soggetto e una cosa, che si esplicita nell'effettivo esercizio di un potere fisico consistente nel controllo delle modalità d'uso e di conservazione della cosa stessa. Da tale legame discenderebbe un dovere di custodia, o meglio di un vincolo di vigilanza.
Nel quadro di nostro interesse, si potrebbe in via ipotetica ricondurre entro tali canoni il rapporto tra il provider della connessione wifi (che assurgerebbe a custode) e il router wireless (la cosa oggetto di custodia): l'accesso alla rete senza autenticazione -comportamento teoricamente frutto di una custodia disattesa- sarebbe equiparabile al caso della violazione di un rapporto di custodia intercorrente tra il condominio e le impalcature montate per svolgere alcuni lavori di ristrutturazione di un edificio!

E' evidente la grossolanità di una siffatta interpretazione forzatamente estesa all'esercizio da parte dei cittadini di un diritto - oramai oggetto di espliciti riconoscimenti normativi - fondamentale per lo sviluppo della società in cui viviamo e che, invece, deve essere condotta tenendo in debito conto i rischi connessi alla violazione di un rapporto di custodia e vigilanza in connessione alla strenua tutela del sopracitato diritto, cui sono connessi i corollari della libertà di espressione e informazione.
Uno sguardo comparatistico, effettuato al fine di mitigare gli effetti della penuria di arresti giurisprudenziali nazionali, regala un quadro di pronunce piuttosto omogenee nell'escludere la responsabilità del provider nei casi di commissione di fatti illeciti da parte di terzi utilizzatori della rete wifi "aperta":

- Caso Media Cat in Inghilterra (permettere ad un terzo di fruire di una connessione internet non vorrebbe necessariamente dire « autorizzarlo a commettere illeciti in rete)
- Caso AF Holdings v. Hatfield-Doenegli Stati Uniti (il giudice ha escluso la sussistenza di una presunzione di responsabilità a carico dell'intestatario di una connessione wireless non protetta, nè un generale dovere di protezione e prevenzione da fattispecie di violazione di copyright ed escluso che tra le due parti sussista un legame speciale che giustifichi la validità di un tale obbligo agendo come eccezione alla regola principale"
- Conseil Constitutionel, decisione del 10.06.2009, che ha imposto al legislatore la modifica della norma sulla tutela del diritto d'autore nella parte in cui prevedeva un obbligo di vigilanza a carico dell'abbonato ad internet affinché la stessa connessione non venisse utilizzata per attività illecite

Giova, ai fini della presente analisi, soffermarsi in ordine alla rilevanza del dato di autenticazione, ai fini dell'accertamento di eventuali responsabilità. Sul punto, la Corte di Cassazione (ad es. nella sentenza n. 6046/2009) ha osservato che l'autenticazione di un utente consente di solo di provare che il reato è stato compiuto a mezzo della rete e di un determinato supporto elettronico, ma non che tale processo di autenticazione sia rilevante ai fini dell'evitare il compimento di atti illeciti.
Peraltro, sfugge ai commentatori, e alle Linee guida, la sostanziale differenza tra autenticazione e identificazione. In tal senso, AGID , nella sezione del proprio sito istituzionale dedicata al regolamento EIDAS, assume che "L'identificazione elettronica è un processo in cui si usano i dati di autenticazione personale in forma elettronica per identificare univocamente: una persona fisica e una persona giuridica. L'autenticazione elettronica è il processo che permette di assicurare il riconoscimento dell'utente elettronico.". L'autenticazione elettronica priva di un comprovante sistema di identificazione non consente l'acquisizione di informazioni nodali ai fini della detonazione di illeciti. Pertanto, la conseguenza sarebbe quella di subordinare l'accesso al wifi non solo a sistemi di autenticazione tout court, ma a sistemi di autenticazione basati su sistemi di identificazione certa come SPID.
Peraltro, dall'esame delle pronunce giurisprudenziali italiane emerge che, l'indirizzo IP, nella sua accezione statica o dinamica, costituisce un mero dato tecnico che descrive la "traccia" della dinamica intercorsa in un dato lasso di tempo tra un utente, un terminale e la rete e, quindi, non può assurgere ad elemento inconfutabile ai fini dell'identificazione del soggetto che opera sul web. Pertanto, l'imputazione di una fattispecie di responsabilità raggiunta a mezzo dell'indirizzo IP associato ai dati di autenticazione dell'utente (senza identificazione certa), costituisce operazione non equilibrata e inconferente sul piano tecnico-giuridico.

L'autenticazione costituisce, a tutti gli effetti, un fardello poco efficace opposto alla necessità, fatta propria dalla Regione Emilia-Romagna, di garantire una sempre più capillare diffusione della rete e della fruizione di servizi ad essa connessi. L'obiettivo che si è posto l'Ente è quello di assecondare l'esercizio di un diritto fondamentale dei cittadini della società dell'informazione. Tale azione istituzionale è volta a dare corpo al pensiero di un grande dei nostri tempi, il compianto Stefano Rodotà, che, nel corso della terza edizione dell'Internet Governance Forum del 30 Novembre 2010, postulava la modifica alla Carta Costituzionale italiana con il riconoscimento in capo ad ogni cittadino del diritto all'accesso ad internet, con l'introduzione dell'art. 21-bis per cui "tutti hanno eguale diritto di accedere alla Rete Internet, in condizione di parità', con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale".

Roma, 23 marzo 2019