GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Ordinanza ingiunzione nei confronti di Iliad Italia S.p.A. - 9 luglio 2020 [9435807]

VEDI ANCHE Comunicato del 13 luglio 2020

[doc. web n. 9435807]

Ordinanza ingiunzione nei confronti di Iliad Italia S.p.A. - 9 luglio 2020

Registro dei provvedimenti
n. 138 del 9 luglio

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il dott. Antonello Soro, presidente, la dott.ssa Giovanna Bianchi Clerici e la prof.ssa Licia Califano, componenti, e il dott. Giuseppe Busia, 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 Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), come modificato dal d.lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al citato Regolamento (di seguito “Codice”);

VISTI i reclami e le segnalazioni pervenuti al Garante, con riguardo a vari trattamenti di dati personali effettuati da parte di Iliad Italia S.p.A. (di seguito indicata anche come: “Iliad” o “la Società”);

VISTI gli esiti degli accertamenti ispettivi effettuati nei giorni 27, 28 e 29 maggio 2019 presso la sede legale della Iliad Italia S.p.A. in Milano;

VISTA la documentazione in atti;

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

RELATORE il dott. Antonello Soro;

PREMESSO

1. L’ATTIVITÀ ISTRUTTORIA SVOLTA

A partire dalla fine del 2018 sono pervenuti al Garante alcuni reclami e segnalazioni riferiti a diverse modalità di trattamento dei dati personali poste in essere da Iliad.

In particolare, le questioni portate all’attenzione dell’Autorità hanno riguardato il trattamento dei dati della clientela per l’attivazione di sim card e la relativa modalità di acquisizione di dati di pagamento, il trattamento per finalità promozionali proprie e di terzi e le misure adottate per la conservazione dei dati nell’area personale dei clienti.

Data la natura e l'eterogeneità delle questioni rappresentate ed in considerazione del fatto che la Società, in quanto nuovo operatore di comunicazioni elettroniche, non era mai stata oggetto di interlocuzioni con il Garante, si è ritenuto opportuno effettuare una valutazione complessiva nell'ambito di un unico accertamento ispettivo che è stato condotto nei giorni 27, 28 e 29 maggio 2019.

2. ESITI DELL'ISTRUTTORIA

Nel corso di tale accertamento sono state effettuate verifiche che, a partire dalle singole segnalazioni e seguendo la prassi dell'Ufficio per la conduzione degli accertamenti in loco, hanno permesso di valutare anche in via più generale le modalità con cui vengono effettuati i trattamenti e le misure tecniche e organizzative adottate dalla Società.

All'esito di tale attività sono emerse violazioni delle norme in materia di protezione dei dati personali e sono stati altresì rilevati alcuni trattamenti che avrebbero potuto verosimilmente violare tali norme. Pertanto, in data 11 ottobre 2019, è stato notificato alla Società l'avvio del procedimento ai sensi dell'art. 166, comma 5, del Codice per la contestazione delle violazioni del Codice e del Regolamento.

La Società ha fatto pervenire le proprie osservazioni in replica con nota dell'8 novembre 2019 e con un'audizione tenuta il successivo 10 dicembre.

2.1. Accettazione contestuale delle condizioni contrattuali e dell'informativa privacy.

Al fine di verificare in via generale i processi aziendali più strettamente connessi al trattamento dei dati personali degli utenti, le operazioni sono iniziate con la verifica delle attività necessarie ad attivare una nuova utenza mediante accesso al sito web www.iliad.it.

In tale contesto è stato verificato che la procedura che conduceva alla conferma dell'ordine prevedeva, una volta inseriti tutti i dati, l'obbligatoria spunta di una casella con la quale il soggetto dichiarava di "aver preso visione e accettato le condizioni generali, la carta dei servizi, la brochure dei prezzi e l'informativa privacy di Iliad sul trattamento dei dati personali" (cfr. pag. 3 del verbale del 27 maggio). I documenti ivi richiamati, compresa l'informativa, erano facilmente raggiungibili mediante apposito link.

Si rileva, tuttavia, che i trattamenti elencati nell'informativa pubblicata sul sito web sono sia di natura facoltativa che obbligatoria e, in alcuni casi (trattamenti per finalità di marketing e profilazione) sono subordinati all'acquisizione di uno specifico consenso.

Tuttavia, la formulazione della dichiarazione sopra menzionata, contemplando contestualmente la "presa visione" e la "accettazione" dell'informativa, poteva indurre il dubbio che la raccolta del consenso per finalità di marketing – che pure è prevista in maniera specifica in una delle schermate precedenti - avvenisse in tale ultima sede proprio con la spunta "per accettazione".

Pur risultando corretta la presentazione dell'informativa al momento della raccolta dei dati, come previsto dall'art. 13 del Regolamento, e tenuto conto che il titolare del trattamento deve poter dimostrare, documentandone la presa visione, di aver reso tali informazioni, appare superflua la contestuale menzione anche dell'accettazione dell'informativa dal momento che a tale dizione non si può attribuire altro significato che quello di mera conferma di lettura; in caso contrario, infatti, procedendo alla spunta della casella, il soggetto si troverebbe ad esprimere un consenso al trattamento che non sarebbe né libero, perché la spunta è obbligatoria e unica per l'accettazione anche delle clausole contrattuali, né specifico perché riguardante tutti i trattamenti menzionati nell'informativa. A tal proposito si richiama quanto contenuto nei considerando 42 e 43 del Regolamento in merito alla consapevolezza del soggetto che esprime un consenso nel contesto di una dichiarazione scritta che contempli anche altre questioni.

Pertanto, l'Ufficio, con nota dell'11 ottobre 2019, ha contestato alla Società che tale trattamento - tenuto conto che, nei termini descritti, l'intenzione del titolare non pareva essere quella di ottenere un consenso al trattamento, ma solo di dimostrare di aver ottemperato agli obblighi informativi – non aveva il carattere della chiarezza e dell'intelligibilità e, dunque, si sarebbe potuto porre in contrasto, in particolare, con i principi di correttezza e trasparenza espressi dall'art. 5, par. 1, lett. a) del Regolamento.

Con la memoria difensiva dell'8 novembre 2019, la Società ha dichiarato che, pur ritenendo "che l'approccio sino ad ora seguito sia conforme ai principi di liceità e trasparenza […], nell'ottica di migliorare sempre i servizi ai propri utenti, Iliad ha rimosso il riferimento all'informativa sul trattamento dei dati personali dalla frase contestata". La stessa ha inoltre allegato la nuova schermata

nella quale, al termine della procedura di attivazione utenza, viene richiesto di selezionare la presa visione e accettazione di Condizioni generali, Carta dei servizi e Brochure prezzi mentre, in un separato spazio viene mostrato il seguente avviso: “I tuoi dati personali saranno trattati in conformità con Informativa Privacy di Iliad sul trattamento dei dati personali”.

2.2. Richiesta del consenso per finalità di marketing.

Durante l’accertamento ispettivo è stata esaminata la procedura di registrazione presente sul sito www.iliad.it, volta alla richiesta di una nuova utenza, ed è stato riscontrato che, in calce alla pagina di inserimento dei dati anagrafici, era presente una casella da spuntare per prestare il consenso al trattamento dei dati personali per finalità promozionali della stessa Iliad. La mancata spunta della casella consentiva comunque di andare avanti nella sottoscrizione del contratto. Ciò in conformità all’informativa privacy dove, al punto 4 lett. i), era contemplato il trattamento per finalità di marketing previo espresso consenso dell’interessato.

A tal proposito, con dichiarazioni rese a verbale (cfr. pag. 2 verbale del 28 maggio) la Società ha chiarito che “la spunta della checkbox, relativa alla richiesta del consenso per finalità promozionali, vista nella procedura di attivazione online, non comporta la registrazione di tale manifestazione del consenso nei sistemi informativi di Iliad, in quanto la Società non svolge attività di marketing diretto”.

L’Ufficio, pertanto, con la menzionata nota dell’11 ottobre, ha evidenziato che, in assenza di un trattamento per finalità promozionali risultava inconferente sia la sua menzione nell’informativa, sia la richiesta di uno specifico consenso; di contro, qualora la società avesse inteso invece effettuare tale tipo di trattamento, non avrebbe potuto dimostrare la corretta acquisizione dei consensi degli interessati, non avendoli registrati. Analogamente è stato messo in evidenza che al punto 4, lett. j) dell’informativa, era prevista la possibilità di utilizzare i dati forniti dall’interessato “per l’invio di comunicazioni di marketing focalizzate sugli interessi e sulle esigenze dell’utente”. Anche in questo caso risulta non pertinente il riferimento ad un trattamento, la profilazione finalizzata al marketing, che in realtà non viene effettuato (e per il quale, in questo caso, non è neanche prevista la richiesta dello specifico consenso).

Con la memoria difensiva dell’8 novembre 2019, la Società ha innanzitutto precisato che “a differenza di altri operatori del mercato delle telecomunicazioni, Iliad non svolge alcuna attività di marketing, telemarketing o profilazione degli utenti […] e svolge attività promozionali principalmente tramite il canale televisivo e digitale che non comporta il trattamento dei dati personali degli utenti”. Poi, con specifico riguardo al punto contestato, ha dichiarato che “Iliad ha intenzione di svolgere un trattamento dei dati personali dei propri utenti per finalità promozionali e, per questa ragione, Iliad ha inserito tale finalità di trattamento nella propria informativa sul trattamento dei dati personali ed ha predisposto un sistema di raccolta dei consensi […]. Tuttavia, detta attività è stata fino ad ora posticipata proprio perché – a causa di un problema tecnico – la società non ha potuto registrare i consensi”. La stessa ha, infatti, aggiunto che il sistema di raccolta dei consensi, già predisposto, era risultato affetto da un bug di progettazione che impediva di identificare l’utente, la data e l’ora in cui veniva effettuata la spunta della checkbox relativa al consenso. La Società ha pertanto corretto l’errore e da luglio 2019 tutti i consensi vengono registrati a sistema; ciò consente agli utenti di esprimere la propria volontà di conferimento o di revoca del consenso anche attraverso l’apposita funzione presente nell’area personale.

Inoltre, si dà atto che la Società ha dichiarato di non aver previsto tra le sue procedure la cessione dei dati dei clienti a terzi per finalità promozionali (cfr. verbale del 28 maggio 2019) e pertanto non trova diretto fondamento quanto lamentato in alcune segnalazioni in merito alla ricezione di chiamate promozionali dopo aver attivato un’utenza Iliad.

2.3 Idoneità delle Simbox a garantire la riservatezza degli interessati.

Nel corso dell’accertamento ispettivo è stato richiesto alla Società di descrivere le modalità di assegnazione delle sim ai clienti. Iliad ha chiarito che le nuove utenze possono essere richieste tramite il sito web o recandosi presso i canali di vendita fisici (punti vendita a marchio Iliad o appositi spazi, detti “corner”, allestiti in luoghi aperti al pubblico). In tutti i casi la società ha predisposto apposite procedure per identificare i soggetti che richiedono l’attivazione di una utenza telefonica, in conformità a quanto disposto dalle vigenti norme in materia di contrasto al terrorismo (legge 31 luglio 2005, n. 155).

Nel caso dell’attivazione via web l’utente può scegliere se procedere subito all’identificazione tramite il sito oppure rimandare tale fase al momento della consegna della sim tramite corriere. Nel primo caso, viene richiesto, al termine della procedura, di allegare la copia del documento di riconoscimento registrando un breve video nel quale si dichiara di voler sottoscrivere il contratto; nel secondo caso, invece, l’identificazione dell’intestatario della sim viene fatta direttamente dal corriere, nominato responsabile del

trattamento e appositamente istruito per tale procedura.

Se invece l'attivazione di una nuova sim viene effettuata tramite i canali fisici, la società ha predisposto delle apposite macchine, denominate "Simbox", con le quali i clienti possono effettuare l'acquisto in autonomia, inserendo i propri dati e terminando la procedura con la scansione del documento e la registrazione di un videomessaggio di assenso alla conclusione del contratto. Il personale presente nei negozi ha solo funzione di assistenza ai clienti e non viene coinvolto nella procedura di attivazione dell'utenza.

Le videoregistrazioni così effettuate sono visionate da operatori di back office che, effettuato un confronto con il documento caricato, concludono la procedura consentendo l'attivazione dell'utenza.

Durante l'accertamento svolto dall'Autorità è stata simulata la modalità di attivazione di un'utenza mediante utilizzo di una Simbox installata presso un punto vendita. Durante tale attività, documentata mediante riprese fotografiche (cfr. all. 5 al verbale del 28 maggio) è stato possibile verificare che all'interno del negozio erano presenti diverse macchine pubblicamente accessibili per effettuare in autonomia la procedura.

È stato contestato ad Iliad che la telecamera installata sulla Simbox è in grado di effettuare una ripresa con un angolo di circa 180 gradi; come si evince anche dalla documentazione agli atti tale modalità potrebbe consentire di registrare l'immagine pure delle persone che si trovino a passare dietro o di lato al soggetto che sta effettuando l'operazione; le registrazioni fotografiche, di cui all'allegato 5 del verbale del 28 maggio, mostrano infatti che l'inquadratura della telecamera non riprende solo il viso della persona che effettua la registrazione ma anche le persone dietro di essa. Allo stesso tempo, l'assenza di misure idonee a garantire la riservatezza dei clienti durante le operazioni, potrebbe consentire a chiunque si trovi nei locali di visualizzare i dati digitati sullo schermo della Simbox e di ascoltare il contenuto del videomessaggio (durante il quale l'utente deve pronunciare il proprio nome e cognome).

Occorre, inoltre, tenere conto che tali macchine sono installate, non solo nei negozi Iliad, ma anche (e prevalentemente) presso appositi spazi allestiti presso stazioni ferroviarie e centri commerciali e anche in questo caso non sono previste particolari misure volte a tutelare la riservatezza dei clienti, considerato in particolare che si tratta di luoghi caratterizzati, in generale, da una notevole affluenza di persone (cfr. all. 2 al verbale del 27 maggio dove è presente la foto di due Simbox posizionate all'interno di un centro commerciale).

Del resto, anche nel contratto di appalto di servizi sottoscritto con la società che si occupa della gestione operativa delle aree poste nei centri commerciali, non vi è alcun richiamo in merito a particolari accorgimenti da osservare nel posizionamento delle Simbox per il rispetto di canoni di riservatezza (cfr. all. 2 al verbale del 27 maggio).

Nel fornire proprie osservazioni in replica, Iliad ha rappresentato che la telecamera della Simbox si attiva solo per il breve lasso di tempo (massimo 10 secondi) necessario ad effettuare la registrazione e non consente di inquadrare nitidamente i soggetti che passano in prossimità della macchina. Inoltre, con riguardo alla possibilità, contestata dal Garante, di esporre i dati personali digitati dagli utenti alla vista di soggetti terzi, la Società ha affermato che le dimensioni dello schermo e il suo posizionamento non dovrebbero consentire a terzi di leggere il testo digitato dal momento che la visuale sarebbe coperta dalla persona che effettua l'operazione e tenuto conto che il carattere di inserimento è di colore grigio.

Ciò precisato, pur continuando a ritenere che le misure adottate siano già conformi alle norme, la società ha comunque introdotto le seguenti soluzioni correttive:

- nella schermata che appare all'utente all'avvio della procedura di registrazione, viene mostrato il seguente avviso: "assicurati di non registrare immagini di terzi, di essere solo, di fronte e posizionato in modo che l'intero viso sia visibile e identificabile";

- le registrazioni raccolte, non appena validate dagli operatori del customer care, sono rese visibili solo ai manager della funzione customer care e, trascorsi sei mesi, sono accessibili solo alla funzione JAS (Judicial Authority Services) per la durata del contratto.

Inoltre, nel corso dell'audizione tenuta il 10 dicembre 2019, Iliad ha aggiunto che la registrazione video non viene conservata nelle Simbox, ma viene memorizzata direttamente nel database centrale; inoltre, i video contenenti immagini di terzi sono

immediatamente cancellati dagli operatori addetti alla procedura di identificazione con contestuale interruzione del processo e richiesta al cliente di effettuare una nuova registrazione. La Società ha inoltre precisato che l'operatore addetto all'identificazione e l'assistente presente nei punti vendita non possono effettuare copie dei documenti forniti dai clienti o delle registrazioni effettuate.

2.4. Rispetto delle norme in materia di accesso e conservazione dei dati di traffico telefonico e telematico.

Nel corso dell'accertamento condotto il 28 maggio 2019, è stato fatto accesso al sistema CRM della società, sia con profilo di operatore sia con profilo di amministratore, per verificarne il contenuto. È stato così rilevato, e riportato a verbale, che il profilo "amministratore del reparto di customer care" poteva visualizzare i dati di traffico telefonico degli utenti in chiaro accedendo al sistema mediante digitazione di userid e password. Inoltre, i dati accessibili erano relativi al traffico effettuato da agosto 2018.

È stato pertanto contestato alla società che tale procedura non poteva considerarsi conforme alle norme in materia di conservazione dei dati di traffico telefonico e telematico di cui agli art. 123, 132 e 132-ter del Codice e sulla base di quanto prescritto dal Garante con provvedimento generale del 17 gennaio 2018 (in www.garanteprivacy.it doc web n. 1482111). Ciò in quanto:

1. l'incaricato con profilo di amministratore – che, essendo addetto alla funzione customer care, avrebbe potuto avere accesso solo ai dati conservati per finalità di fatturazione, poteva invece visualizzare dati conservati per un periodo superiore ai sei mesi consentiti dall'art. 123 del Codice (sono risultati presenti dati di traffico di agosto 2018 alla data di maggio 2019);

2. lo stesso ha avuto accesso al sistema contenente i dati di traffico digitando unicamente username e password, senza pertanto utilizzare tecniche di strong authentication al momento dell'accertamento;

Inoltre, in conseguenza di quanto accertato sopra, non risultava attuata la prescrizione di conservare le diverse tipologie di dati in sistemi informatici separati, dal momento che l'operatore, accedendo al sistema CRM, poteva visualizzare anche dati generati in un periodo eccedente i sei mesi.

Con nota dell'8 novembre 2019, Iliad ha ritenuto non fondate le contestazioni ricevute dal Garante sulla base del fatto che le informazioni contenute nello screenshot di cui all'allegato 6 al verbale di accertamento del 28 maggio 2019, "non permettono di ricostruire i flussi di comunicazione degli utenti a cui si riferiscono e non possono pertanto considerarsi dati di traffico". A tal proposito occorre evidenziare che il contenuto cui si riferisce la società (allegato 6), essendo riferito all'accesso fatto con profilo di operatore, non è mai stato oggetto di contestazione da parte dell'Autorità e pertanto risulta impropriamente citato. La contestazione, invece, si è basata sull'accesso effettuato con profilo di amministratore che, come riportato nel verbale del 28 maggio 2019 sottoscritto dalla parte, "può visualizzare ulteriori informazioni quali i dati del traffico telefonico uscente in chiaro a decorrere, per la scheda dell'utente visualizzato, da agosto 2018". Su tale punto non sono pervenute altre osservazioni da parte di Iliad né con la menzionata memoria difensiva, né durante la successiva audizione.

Inoltre, con riguardo al contestato accesso effettuato senza adottare tecniche di strong authentication, la Società, nella propria memoria difensiva ha dichiarato che "con riferimento al gestionale Mobo oggetto di ispezione nello specifico ma in generale relativamente a tutti i sistemi aziendali, Iliad ha adottato una duplice tecnologia di autenticazione. Infatti, oltre all'inserimento della username e password dell'utente che accede al sistema, vi è una forma di autenticazione automatica determinata dalla connessione esclusivamente dei devices aziendali alla rete Iliad. Al momento dell'accesso alla rete Iliad tramite il device aziendale, infatti, il sistema effettua un primo riconoscimento del dipendente Iliad e un secondo riconoscimento avviene al momento dell'accesso al gestionale Mobo". La stessa, tuttavia, non ha allegato alcuna documentazione comprovante quanto dichiarato e occorre evidenziare che tale giustificazione non è stata fatta presente al momento dell'accertamento.

Con la nota dell'8 novembre 2019, la Società ha fornito proprie osservazioni anche riguardo al fatto che, al momento dell'accertamento, i dati di traffico telefonico generati oltre i sei mesi sono risultati presenti nel sistema gestionale del customer care, in difformità da quanto prescritto dal Garante in merito alla necessità, trascorsi i primi sei mesi, di operare una separazione dei sistemi informatici deputati alla conservazione dei dati per le diverse finalità. A tal proposito la società ha dichiarato di aver "creato un unico database con misure di sicurezza e livelli di accesso differenziati (CRM i.e. gestionale Mobo e JAS) a seconda delle finalità del trattamento e del relativo termine di conservazione. Tale sistema ha quindi una separazione di carattere logico invece che fisico".

3. VALUTAZIONI DI ORDINE GIURIDICO

Con riferimento ai profili fattuali sopra evidenziati, anche in base alle dichiarazioni della Società di cui si risponde ai sensi dell'art. 168 Codice, si formulano le seguenti valutazioni in relazione ai profili riguardanti la disciplina in materia di protezione dei dati personali.

3.1 Accettazione contestuale delle condizioni contrattuali e dell'informativa privacy.

Il trattamento descritto al punto 2.1., le cui motivazioni si richiamano interamente, per come posto in essere prima delle modifiche apportate dalla Società, non risultava pienamente conforme ai principi espressi dal Regolamento. Ciò in quanto la formulazione proposta nella schermata di conclusione del contratto risultava inconferente richiedendo la "accettazione" dell'informativa e non solo la sua presa visione e tale richiesta era, per di più, formulata insieme alle conferme di carattere contrattuale. Come noto, l'informativa redatta dal titolare ha la funzione di rendere noto all'interessato ogni aspetto del trattamento dei dati personali; tale natura meramente esplicativa fa sì che il titolare, pur potendo pretendere dall'interessato di confermarne la presa visione, non possa tuttavia richiedere anche di esprimere, attraverso una generica e generale accettazione, una volontà che risulterebbe di fatto analoga ad un consenso.

L'Ufficio pertanto, pur avendo compreso che, nei termini descritti, l'intenzione del titolare non pareva essere quella di ottenere un consenso al trattamento ma solo quella di dimostrare di aver ottemperato agli obblighi informativi, ha ritenuto necessario contestare la mancanza dei requisiti della chiarezza e dell'intelligibilità con la conseguenza di un possibile trattamento in contrasto, in particolare, con i principi di correttezza e trasparenza espressi dall'art. 5, par. 1, lett. a) del Regolamento.

Le misure correttive adottate dalla Società, a seguito della contestazione ricevuta, risultano sufficienti a separare gli obblighi informativi dalla raccolta del consenso, restituendo a tale fase del trattamento la necessaria chiarezza.

Su tale aspetto, dunque, non si ritiene di adottare specifiche misure correttive, ad eccezione di quanto indicato al punto 4.1 del presente provvedimento.

3.2. Richiesta del consenso per finalità di marketing.

Con riguardo al trattamento descritto al punto 2.2., si evidenzia che la Società, sulla base delle dichiarazioni rese, fino al luglio 2019 ha richiesto agli interessati di prestare il proprio consenso al trattamento per finalità promozionali senza tuttavia tenere traccia di tale volontà. Ciò sarebbe avvenuto perché, come in un primo momento dichiarato a verbale, la Società non effettuava (e risulterebbe non effettuare tuttora) attività di marketing diretto ma anche, come successivamente sostenuto nella memoria difensiva, a causa di un bug presente nel sistema preposto alla registrazione dei consensi.

Sulla base delle dichiarazioni rese, si deve pertanto ritenere che, come già contestato, la richiesta di un consenso per finalità promozionali, specificamente menzionate nell'informativa, senza che tale trattamento esista o sia previsto, risulti in contrasto con il principio di correttezza e trasparenza di cui all'art. 5, par. 1, lett. a), del Regolamento.

Tuttavia, preso atto dell'intenzione della Società, non menzionata nel corso dell'accertamento ispettivo, ma resa nota in sede difensiva, di voler effettivamente porre in essere un trattamento per finalità promozionali, tenuto conto degli interventi correttivi apportati, e del fatto che la Società ha dichiarato di considerare come negato il consenso dei soggetti registrati prima di luglio 2019, si ritiene che, anche su tale punto, non sussistano i presupposti per adottare specifiche misure correttive, ad eccezione di quanto indicato al punto 4.1 del presente provvedimento.

3.3 Idoneità delle Simbox a garantire la riservatezza.

Le verifiche effettuate simulando la sottoscrizione di un contratto tramite Simbox, hanno suscitato alcune perplessità in ordine alla riservatezza della procedura. Pertanto è stato contestato alla Società che un simile trattamento può esporre gli interessati al rischio di accessi non autorizzati violando il principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. f) del Regolamento.

Le misure correttive introdotte dalla Società (descritte al punto 2.3) possono ritenersi idonee a contenere il rischio, ma potrebbero non essere sufficienti, soprattutto nel caso di totem posizionati in luoghi aperti al pubblico (non solo i punti vendita Iliad ma anche i corner) che sono, in generale, caratterizzati da maggiore affluenza di persone.

Inoltre, tenuto conto del complessivo trattamento effettuato anche prima dell'adozione delle misure correttive, si ritiene integrata la violazione dell'art. 5, par. 1, lett. f) del Regolamento con riguardo alla mancata adeguatezza delle misure adottate per garantire la riservatezza dei dati personali.

Ciò premesso, ai sensi dell'art. 58, par. 2, lett. a), si ritiene di dover rivolgere alla Iliad un ammonimento in merito alle rilevate violazioni della riservatezza mediante l'uso della Simbox e di dover, di conseguenza, ingiungere alla stessa, ai sensi dell'art. 58, par. 2, lett. d), di adottare misure correttive idonee a garantire maggiore riservatezza agli interessati al momento dell'effettuazione della registrazione del video adottando specifici accorgimenti per il posizionamento delle macchine, collocandole in maniera tale da non poter consentire accessi indebiti alle informazioni (ad esempio in prossimità di una parete) o inserendo dei pannelli posteriori, ovvero prevedendo, distanze di cortesia ed integrando conseguentemente le istruzioni al personale addetto all'assistenza.

3.4. Rispetto delle norme in materia di accesso e conservazione dei dati di traffico telefonico e telematico.

Come ricostruito al punto 2.4., nel corso dell'attività ispettiva è stato accertato che l'incaricato addetto al customer care con profilo di amministratore poteva visualizzare dati di traffico telefonico in chiaro, generati da più di sei mesi, accedendo al sistema, denominato "Mobo", preposto alla gestione del customer care.

La condotta della Società è stata valutata alla luce delle disposizioni di cui agli art. 123, 132 e 132-ter del Codice che dettano specifiche indicazioni in merito alle misure da adottare nella conservazione dei dati di traffico. In particolare, l'art. 132-ter impone ai fornitori di servizi di comunicazione elettronica di avvalersi, ai sensi dell'art. 32 del Regolamento, di misure tecniche e organizzative adeguate al rischio esistente. Tali misure, da considerarsi, allo stato dell'arte, quale requisito minimo di sicurezza generalmente utilizzato dagli operatori presenti sul mercato, sono in concreto identificabili con quanto prescritto dal Garante, in materia di conservazione dei dati di traffico, con provvedimento generale del 17 gennaio 2008 (in www.garanteprivacy.it doc web n. 1482111, come modificato dal successivo provvedimento del 24 luglio 2008, doc. web n. 1538224), in base al quale:

- il trattamento dei dati di traffico telefonico e telematico da parte dei fornitori deve essere consentito solo ad incaricati specificamente autorizzati e unicamente sulla base del preventivo utilizzo di specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione; per i dati di traffico conservati per esclusive finalità di accertamento e repressione dei reati (e generati da più di sei mesi), una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato;

- i sistemi informatici utilizzati per i trattamenti di dati di traffico conservati per esclusiva finalità di giustizia devono essere differenti da quelli utilizzati anche per altre funzioni aziendali (come fatturazione, marketing, antifrode); è tuttavia ammissibile un primo periodo, di 6 mesi dalla generazione, durante il quale i dati possono essere trattati con sistemi informatici non esclusivamente riservati alle finalità di giustizia;

- il fornitore deve definire e attribuire agli incaricati specifici profili di autorizzazione differenziando le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati.

All'esito dell'attività istruttoria condotta, l'Ufficio ha ritenuto che gli elementi acquisiti potessero configurare delle violazioni ad ha pertanto avviato il procedimento di cui all'art. 166, comma 5 del Codice. A fronte delle puntuali contestazioni ricevute, la Società – che pure ha presentato una memoria di 22 pagine ed è stata ascoltata in una successiva audizione - ha risposto sul punto in maniera non esaustiva e talvolta equivoca.

Nello specifico caso relativo alla conservazione dei dati di traffico, Iliad ha replicato che le contestazioni ricevute erano da considerarsi infondate in quanto, a suo parere, vi sarebbero state tre questioni da considerare:

1) i livelli di accesso ai dati personali;

2) la verifica che attraverso il gestionale Mobo fosse possibile visionare i dati di traffico;

3) il termine di conservazione dei dati personali.

Con riguardo al primo punto, Iliad ha dichiarato di aver adottato livelli di accesso ai sistemi differenziati in base al ruolo dei dipendenti e, anche nel caso in esame, l'accesso al sistema Mobo consente livelli di visibilità delle informazioni differenti a seconda

del profilo (operatore/ amministratore). In merito a ciò, deve osservarsi che tale aspetto non è mai stato oggetto di contestazione da parte dell'Ufficio che, invece, ha contestato il fatto che l'incaricato, in quanto addetto al customer care (ancorché con il profilo di amministratore) ha potuto visualizzare dati conservati per un periodo superiore ai sei mesi, termine oltre il quale non dovrebbe più essere consentito al personale addetto a verificare la correttezza della fatturazione (quale è l'amministratore di customer care) e dovrebbe, invece, essere riservato alle sole figure autorizzate ad accedere ai dati di traffico conservati per finalità di giustizia.

Relativamente al secondo punto, come già descritto al paragrafo 2.4, la Società ha osservato che lo screenshot inserito nell'allegato 6 al verbale del 28 maggio 2019 non contiene dati di traffico e, per tale motivo, la contestazione non sarebbe fondata. Come già ricordato, l'allegato cui fa riferimento la Società è quello relativo all'accesso effettuato con profilo di operatore che non è mai stato oggetto di contestazione da parte dell'Ufficio. L'accesso effettuato con il profilo di amministratore di sistema è invece riportato nell'allegato 7, che mostra come l'incaricato abbia fatto accesso al sistema digitando userid e password e che la piattaforma di customer care tiene traccia delle operazioni effettuate dall'amministratore; inoltre, il risultato complessivo di tale accesso, in cui si dà atto della presenza di "dati del traffico telefonico uscente in chiaro a decorrere, per la scheda dell'utente visualizzato, da agosto 2018" è stato riportato nel verbale che la parte ha sottoscritto e non ha mai successivamente contestato.

Inoltre, la Società, nella menzionata memoria, proseguendo in merito alla asserita infondatezza della contestazione (terzo punto dell'elenco di cui sopra), ha aggiunto che "in ogni caso Iliad conferma che l'accessibilità ai dati di traffico nel sistema Mobo è attualmente limitata ad un periodo di sei mesi dalla loro registrazione". È pertanto da considerarsi indubbia, in quanto confermata dalla stessa Iliad, la presenza di dati di traffico nel sistema di customer care (Mobo) e, come sottolineato dall'avverbio "attualmente", i tempi di conservazione sono ora limitati a sei mesi potendo così dedurre che tale termine di conservazione fosse prima diverso e che, verosimilmente, la Società abbia posto in essere un intervento correttivo (che tuttavia non ha menzionato né tantomeno documentato).

La contestazione rivolta ad Iliad ha riguardato anche l'aspetto connesso alla conformità del procedimento di autenticazione. Come riportato nel verbale del 28 maggio 2019, l'incaricato con profilo di amministratore ha effettuato l'accesso al sistema di customer care inserendo una user-id e una password (come riportato nell'allegato 7 al verbale). È stato pertanto contestato che, al momento dell'accertamento, non è stata utilizzata la misura dell'autenticazione a due fattori che, come prescritto nel provvedimento del Garante, è necessaria per garantire la riservatezza dei dati di traffico anche se conservati solo per finalità di fatturazione.

Come descritto al punto 2.4, la società, nella propria memoria difensiva ha dichiarato che l'autenticazione a due fattori è data in automatico "dalla connessione esclusivamente dei devices aziendali alla rete Iliad. Al momento dell'accesso alla rete Iliad tramite il device aziendale, infatti, il sistema effettua un primo riconoscimento del dipendente Iliad e un secondo riconoscimento avviene al momento dell'accesso al gestionale Mobo". Sul punto si richiama il menzionato provvedimento del Garante che ammette che «tale fase di autenticazione può essere realizzata con procedure strettamente integrate alle applicazioni informatiche con cui il fornitore tratta i dati di traffico, oppure con procedure per la protezione delle singole postazioni di lavoro che si integrino alle funzioni di autenticazione proprie dei sistemi operativi utilizzati. Nel secondo caso, il fornitore deve assicurare che non esistano modalità di accesso alle applicazioni informatiche da parte dei propri incaricati di trattamento che consentano di eludere le procedure di strong authentication predisposte per l'accesso alla postazione di lavoro». Pertanto, pur considerando che la giustificazione addotta dalla Società potrebbe essere in linea di principio accettabile con riguardo solo ai dati generati entro i sei mesi, essa appare tuttavia tardiva e dunque non più verificabile, in quanto fatta presente solo dopo aver ricevuto la contestazione e non durante l'accertamento ispettivo; la stessa è, altresì, non documentata dal momento che la Società si è limitata ad affermare che una prima fase di autenticazione è superata con l'accesso al device aziendale senza tuttavia comprovare, né durante l'accertamento ispettivo, né successivamente, che lo strumento utilizzato dall'incaricato possedeva le caratteristiche necessarie ad identificare l'utilizzatore in maniera univoca. Si deve, peraltro, ricordare che per l'accesso ai dati generati da più di sei mesi, è in ogni caso richiesto che una delle tecnologie di autenticazione sia basata su caratteristiche biometriche dell'incaricato.

Infine, i rilievi mossi nei confronti della Società, hanno riguardato più in generale le modalità di conservazione dei dati di traffico che, sulla base delle risultanze istruttorie, destavano perplessità anche in ordine alla conservazione separata in funzione della finalità (fatturazione o giustizia). Infatti, la presenza di dati di traffico generati da più di sei mesi nel sistema dedicato alla gestione dei clienti, ha comportato la contestazione alla Società del mancato rispetto della prescrizione di conservare in sistemi informatici separati le diverse tipologie di dati.

In relazione a tale specifica contestazione, la Società ha replicato soltanto che "Iliad ha creato un unico database con misure di sicurezza e livelli di accesso differenziati (CRM i.e. gestionale Mobo e JAS) a seconda della finalità del trattamento e del relativo

termine di conservazione. Tale sistema ha quindi una separazione di carattere logico invece che fisico [...] Iliad non ha deciso di procedere ad una duplicazione fisica dei database a seconda della finalità del trattamento". Dalla laconica risposta della Società, che pure ha ricevuto puntuali contestazioni e ha avuto ampiamente modo di articolare la propria difesa, si può solo evincere che è presente un unico sistema, separato logicamente mediante accessi differenziati in base alle finalità e ai tempi di conservazione. La Società, tuttavia, non ha fornito alcuna spiegazione in merito al contestato accesso ai dati generati da oltre sei mesi da parte dell'incaricato dell'area customer care che, per la funzione svolta, non avrebbe dovuto accedere a tali dati tenuto conto che, stando a quanto dichiarato, la separazione logica in base alle finalità avrebbe dovuto comunque impedire tale accesso.

Pertanto, la risposta sopra riportata, conferma quanto già contestato in merito alla mancata separazione dei sistemi deputati alla conservazione dei dati di traffico.

Il citato provvedimento del Garante, infatti, prescrive che i dati conservati per esclusive finalità di giustizia siano conservati in sistemi informatici distinti fisicamente – e non logicamente - da tutti gli altri sistemi aziendali e a tali sistemi siano applicate misure dedicate quali, tra le altre, l'accesso solo a personale autorizzato con sistemi di riconoscimento a due fattori (di cui uno biometrico) e la cifratura dei dati. Lo stesso provvedimento ammette anche che, a scelta del titolare, i dati generati fino a sei mesi, possano essere conservati in un unico sistema per poter essere trattati anche per finalità di giustizia, senza necessità di ricorrere ad alcuna separazione; tale facoltà, tuttavia, è applicabile, come detto, solo entro i sei mesi dalla generazione e pertanto, in presenza di dati generati da più di sei mesi, non può considerarsi applicabile al caso in esame.

Pertanto, le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria, della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice, non consentono, in ogni caso, di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, e non risultano idonee ad escludere la responsabilità della parte in ordine a quanto contestato non avendo esse contribuito a dimostrare che le misure adottate dalla società possano ritenersi rispondenti alle misure di sicurezza - allo stato dell'arte disponibili e adottate in via generale dagli operatori di comunicazione elettronica - descritte nel provvedimento del Garante in materia di conservazione dei dati di traffico.

Alla luce del nuovo quadro normativo costituito dal Regolamento e dal Codice, si deve infatti ritenere che le specifiche prescrizioni del provvedimento del Garante del 17 gennaio 2008 siano da considerare alla stregua delle basilari misure di sicurezza del trattamento applicabili ai fornitori di servizi di comunicazione elettronica. Il mancato rispetto di tali prescrizioni deve considerarsi equivalente alla mancanza di misure tecniche e organizzative adeguate al rischio esistente e, di conseguenza, integra la violazione dell'art. 132-ter del Codice.

Per quanto sopra riportato, inoltre, deve ritenersi altresì, integrata la violazione dell'art. 123 del Codice, con riguardo alla conservazione eccedente i sei mesi nei sistemi adibiti a finalità di fatturazione.

Sulla base degli elementi sopra esposti, rilevate le violazioni indicate al presente paragrafo, si rende necessario ai sensi dell'art. 58, par. 2, lett. d), del Regolamento ingiungere ad Iliad di adeguare le misure di sicurezza poste a tutela dei dati di traffico conformandole a quanto prescritto dal Garante con il provvedimento del 17 gennaio 2008 come modificato dal provvedimento del 24 luglio 2008. Inoltre, tenuto conto che le contestazioni rivolte alla Società non si sono dimostrate sufficienti a sollecitare un intervento correttivo da parte di quest'ultima, si ritiene di dover adottare nei confronti della stessa Società un'ordinanza ingiunzione, ai sensi degli artt. 58, par. 2, lett. i), del Regolamento, 166, comma 7, del Codice e 18 della legge n. 689/1981, per l'applicazione delle sanzioni amministrative pecuniarie previste dall'art. 83, parr. 4 e 5, del Regolamento.

4. ORDINANZA INGIUNZIONE PER L'APPLICAZIONE DELLA SANZIONE AMMINISTRATIVA PECUNIARIA

4.1. Informativa e consenso.

Le condotte accertate ai punti 3.1. e 3.2. della presente decisione integrano rispettivamente la violazione dell'art. 5, par. 1, lett. a), del Regolamento.

Tuttavia, tenuto conto:

- delle intenzioni del titolare che, sulla base di quanto acquisito in atti, non paiono volte a realizzare consapevolmente gli effetti delle condotte contestate e sono piuttosto riconducibili ad un'applicazione negligente delle norme;

- della presumibile mancanza di conseguenze in capo agli interessati dal momento che la finalità promozionale del trattamento non sarebbe stata ancora realizzata;

- delle misure adottate e volte a risolvere le criticità sopra indicate,

si ritiene che esse possano essere qualificate come violazioni “di grado minore” alla luce dell’art. 83, par. 2 e del considerando 148 del Regolamento e che, pertanto, possa essere sufficiente al riguardo ammonire Iliad, ai sensi dell’art. 58, par. 2 lett. b) del Regolamento per la mancata osservanza dell’ art. 5, par. 1, lett. a) del Regolamento, nonché dei principi di cui all’art. 25 del Regolamento, significando, altresì, che in difetto si rende applicabile la sanzione di cui all’art. 83, par. 5 lett. a) del Regolamento.

4.2. Simbox e misure di sicurezza.

Le condotte accertate al punto 3.3 della presente decisione sono idonee ad esporre gli interessati al rischio di accessi non autorizzati ai dati personali e dunque sono suscettibili di integrare la violazione del principio di integrità e riservatezza di cui all’art. 5, par. 1, lett. f) del Regolamento.

Tuttavia tenuto conto delle misure correttive introdotte dalla Società idonee a contenere tale rischio, nonché degli accorgimenti adottati con riferimento ad eventuali video contenenti immagini di terzi, si ritiene che anche tale violazione possa essere qualificata “di grado minore” alla luce dell’art. 83, par. 2 e del considerando 148 del Regolamento. Pertanto si ritiene sufficiente al riguardo ammonire Iliad, ai sensi dell’art. 58, par. 2, lett. a), del Regolamento in merito alle rilevate violazioni della riservatezza mediante l’uso della Simbox e, contestualmente, ingiungere alla stessa, ai sensi dell’art. 58, par. 2, lett. d) del medesimo Regolamento, di adottare misure correttive idonee a garantire maggiore riservatezza agli interessati al momento dell’effettuazione della registrazione del video adottando gli specifici accorgimenti indicati al punto 3.3 della presente decisione.

4.3. Misure di sicurezza applicate alla conservazione dei dati di traffico.

Le condotte accertate al punto 3.4 della presente decisione integrano le violazioni degli artt. 132-ter e 123, comma 2 del Codice, soggette rispettivamente alla sanzione di cui all’art. 83, par. 4 e par. 5 del Regolamento.

4.4. Quantificazione della sanzione amministrativa pecuniaria.

In ragione di quanto sopra prospettato, risulta applicabile l'art. 83, par. 3, del Regolamento, in base al quale, se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento viola, con dolo o colpa, varie disposizioni del Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave con conseguenziale applicazione della sola sanzione prevista dall’art. 83, par. 5 del Regolamento.

In particolare, ai fini della quantificazione della sanzione amministrativa, per le violazioni di cui al precedente punto 4.3, il citato art. 83, par. 5, nel fissare il massimo edittale nella somma di 20 milioni di euro ovvero, per le imprese, nel 4% del fatturato mondiale annuo dell’esercizio precedente ove superiore, specifica le modalità di quantificazione della predetta sanzione, che deve “in ogni caso [essere] effettiva, proporzionata e dissuasiva” (art. 83, par. 1 del Regolamento (UE) 2016/679), individuando, a tal fine, una serie di elementi, elencati al par. 2, da valutare all’atto di quantificarne il relativo importo.

In adempimento di tale previsione, nel caso di specie, devono essere considerate le seguenti circostanze:

1. l’ampia portata dei trattamenti riguardanti la conservazione dei dati di traffico) che, sulla base degli elementi forniti e in mancanza di altre specificazioni in merito, si possono ritenere di carattere sistemico e dunque estesi alla generalità dei clienti del servizio di telefonia mobile di Iliad relativi a circa 3 milioni di utenze alla data dell’accertamento ispettivo, come dalla stessa dichiarato (art. 83, par. 2, lett. a) del Regolamento);

2. la gravità delle violazioni rilevate, in ragione del fatto che, per l’inadeguatezza delle misure di sicurezza, sono stati esposti a violazione una tipologia di dati personali (i dati di traffico telefonico) per i quali il legislatore, in considerazione dell’elevato pregiudizio derivante dal trattamento, ha predisposto delle norme di carattere speciale a tutela della conservazione (art. 83, par. 2, lett. a) del Regolamento);

3. il grado di responsabilità del titolare del trattamento, tenuto conto che le misure tecniche e organizzative descritte non

sono risultate adeguate allo stato dell'arte, nonostante le prescrizioni del Garante siano da considerarsi ormai ampiamente note fra gli operatori dei servizi di comunicazione elettronica, in quanto impartite con un provvedimento generale del 2008, più volte oggetto di specifici provvedimenti applicativi;

4. il generale approccio tenuto da Iliad nel trattamento dei dati personali (art. 83, par. 2, lett. d) del Regolamento), considerato che, oltre quanto evidenziato al punto precedente, pure le violazioni descritte ai punti 3.1, 3.2. e 3.3, pur se considerate di carattere minore, hanno comunque mostrato un quadro complessivamente negligente nell'applicazione, sin dalla progettazione, di misure di tutela degli interessati che, date le costanti e numerose pronunce del Garante, sono ormai da considerarsi comunemente note ai titolari del trattamento (si vedano, anche qui, i numerosi provvedimenti in merito alla correttezza dell'informativa e alla raccolta del consenso e, con riguardo al rispetto di misure idonee ad evitare accessi non autorizzati, mediante, ad es. l'istituzione di distanze "di cortesia", i numerosi interventi chiarificatori del Garante, tra i quali, ad es. la nota del 30.3.1998, doc. web n. 39464);

5. il grado di cooperazione con l'Autorità di controllo, dal momento che la Società si è limitata a ritenere infondate le violazioni contestate, sostenendo le proprie ragioni con argomentazioni spesso non pertinenti con quanto accertato a verbale, e tenuto conto che, a fronte delle contestazioni ricevute in materia di conservazione dei dati di traffico, la stessa, diversamente da quanto fatto con gli altri rilievi ricevuti, non ha ritenuto di dover intervenire in alcun modo per adeguare le proprie misure di sicurezza, limitandosi solo a confermare l'attuale presenza nel sistema Mobo di dati di traffico generati da non più di sei mesi (art. 83, par. 2, lett. f) del Regolamento);

6. la maniera in cui l'Autorità di controllo ha preso conoscenza della violazione, emersa nel corso di un'attività ispettiva (art. 83, par. 2, lett. h) del Regolamento).

Quali elementi attenuanti, si ritiene di dover tener conto:

1. delle misure adottate da Iliad che, ancorché non sufficienti, appaiono comunque utili ad attenuare parte delle conseguenze pregiudizievoli delle violazioni riscontrate;

2. della rilevante perdita registrata nel 2018, superiore al valore della produzione (art. 83, par. 2, lett. k) del Regolamento).

In una complessiva ottica di necessario bilanciamento fra diritti degli interessati e libertà di impresa, tenuto conto che la Società, anche in ragione della recente presenza sul mercato italiano, non ha avuto precedenti procedimenti sanzionatori, e in via di prima applicazione delle sanzioni amministrative pecuniarie previste dal Regolamento, occorre valutare prudentemente i suindicati criteri, anche al fine di limitare l'impatto economico della sanzione sulle esigenze organizzative, funzionali ed occupazionali della Società.

Pertanto si ritiene che - in base al complesso degli elementi sopra indicati, debba applicarsi alla Iliad la sanzione amministrativa del pagamento di una somma pari al 4% della sanzione edittale massima di 20 milioni di euro, corrispondente a euro 800.000,00 (ottocentomila). La sanzione edittale massima è individuata con riferimento al disposto dell'art. 83, comma 5, tenuto conto che il 4% del fatturato di Iliad Italia S.p.A. risulta inferiore ai 20 milioni di euro.

Si rileva che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

In tale quadro, si ritiene altresì – in considerazione della delicatezza dei trattamenti di cui è stata accertata l'illiceità alla luce dei diritti fondamentali degli interessati e dell'elevato numero degli stessi- che, ai sensi dell'art. 166, comma 7, del Codice, e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente provvedimento sul sito web del Garante, a titolo di sanzione accessoria.

Si ricorda che in caso di inosservanza del presente provvedimento, è applicata in sede amministrativa la sanzione di cui all'art. 83, par. 5, lett. e), del Regolamento.

TUTTO CIÒ PREMESSO IL GARANTE

nei confronti di Iliad Italia S.p.A., con sede legale in viale Francesco Restelli, 1/A, Milano, C.F. 13970161009,

a) con riguardo alle violazioni riscontrate relativamente alle corrette modalità di somministrazione dell'informativa e del consenso degli interessati (punti 3.1. e 3.2 in premessa), ammonisce Iliad, ai sensi dell'art. 58, par. 2 lett. b) del Regolamento per la mancata osservanza dell'art. 5, par. 1, lett. a), del Regolamento, nonché dei principi di cui al successivo art. 25 del Regolamento;

b) con riguardo alle violazioni riscontrate relativamente alle videoregistrazioni effettuate mediante Simbox (punto 3.3. in premessa): ai sensi dell'art. 58, par. 2, lett. a), del Regolamento ammonisce Iliad in merito alle rilevate violazioni della riservatezza e, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, ingiunge alla stessa di adottare, entro 120 giorni dal ricevimento del presente provvedimento, le misure correttive indicate in premessa, idonee a garantire maggiore riservatezza agli interessati durante l'utilizzo di dette apparecchiature;

c) con riguardo alle violazioni riscontrate relativamente alla conservazione dei dati di traffico telefonico (punto 3.4. in premessa), ai sensi dell'art. 58, par. 2, lett. d), ingiunge di adottare, entro 120 giorni dal ricevimento del presente provvedimento, tutte le misure necessarie a rendere il trattamento conforme al provvedimento del Garante del 17 gennaio 2008 come modificato dal provvedimento del 24 luglio 2008;

d) ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante;

e) ai sensi dell'art. 157 del Codice, richiede di comunicare, entro i successivi 30 giorni, quali iniziative siano state intraprese al fine di dare attuazione a quanto prescritto, con un riscontro adeguatamente documentato; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. e) del Regolamento;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i), del Regolamento, alla predetta Iliad Italia S.p.A., in persona del suo legale rappresentante, di pagare la somma di euro 800.000,00 (ottocentomila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

alla predetta Società, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 800.000,00 (ottocentomila), secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981;

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante.

Ai sensi dell'art. 78 del Regolamento (UE) 2016/679, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati personali, o, in alternativa, al tribunale del luogo di residenza dell'interessato, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 9 luglio 2020

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia