

NEWSLETTER

COMPLIANCE & TECHNOLOGY

SETTEMBRE/DICEMBRE 2018

Indice

LEGISLAZIONE E ATTI DI INDIRIZZO	3
E-commerce: verso il mercato unico digitale con l'entrata in vigore del Regolamento sul "geoblocking"	3
Pubbligate le Linee guida dell'AGCOM sulle modalità di dismissione e trasferimento dell'utenza nei contratti per adesione	3
Online le modifiche al Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e relative procedure attuative	3
Il Garante Privacy pubblica l'elenco dei trattamenti da sottoporre, ai sensi dell'art. 35 par. 4 del GDPR, a valutazione di impatto (DPIA)	4
Il Garante Privacy rilascia il proprio parere sullo schema di disegno di legge sugli "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"	4
Pubbligate le FAQ sulla tenuta del registro delle attività del trattamento	5
Pubbligate le FAQ sulla definizione agevolata delle violazioni pendenti in materia di protezione dei dati personali	5

Il Garante Privacy fornisce indicazioni sull'interpretazione delle istanze comprese nell'ambito degli "affari pregressi" di cui all'articolo 19 del D.Lgs. 10 agosto 2018, n. 101.	6
Publicata l'opinione dell'EDPB sull'elenco del Garante italiano per definire i trattamenti per cui è necessaria una DPIA	6
GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA UE	6
Il titolare di una connessione internet privata è responsabile dell'illecito download di contenuti protetti dal diritto d'autore	6
Non acquista automaticamente la qualifica di "professionista" il soggetto che pubblica annunci di vendita su Internet	6
Accesso consentito ai dati conservati dai fornitori dei servizi di comunicazione elettronica anche per il perseguimento di reati non gravi	7
GIURISPRUDENZA	7
Privacy: rimessa alle Sezioni Unite la questione sul bilanciamento tra diritto all'oblio e diritto di cronaca	7
La certificazione ISO/IEC 27001 non può costituire requisito per il conferimento dell'incarico di DPO	8
PROVVEDIMENTI DELLE AUTORITÀ DI REGOLAZIONE	8
Consumatori: l'AGCM sanziona Facebook per uso dei dati degli utenti a fini commerciali	8
Apple e Samsung multate dall'AGCM per pratiche commerciali scorrette in relazione al rilascio degli aggiornamenti dei sistemi operativi IOS e Android	8
Privacy: secondo il Garante, il sistema di fatturazione elettronica ipotizzato dall'Agenzia delle Entrate sarebbe in contrasto con la normativa in materia di protezione dei dati personali	9

LEGISLAZIONE E ATTI DI INDIRIZZO

Regolamento Europeo: verso il mercato unico digitale con l'entrata in vigore del Regolamento sul "geoblocking"

Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio del 28 febbraio 2018

Il 3 dicembre 2018 è entrato definitivamente in vigore il "*Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE*" (c.d. "**Regolamento Geoblocking**").

L'Unione Europea aggiunge così un ulteriore tassello alla creazione di un mercato unico digitale, vietando alle imprese attive nella rete e sui canali online l'imposizione di restrizioni ai consumatori sulla base della loro nazionalità, del luogo di residenza o della loro temporanea ubicazione.

L'obiettivo primario dalla nuova normativa che abolisce i blocchi geografici nel commercio online è quello di rendere il mercato unico digitale sempre più competitivo e integrato. Grazie a detto Regolamento, infatti, i consumatori europei potranno fare acquisti online su tutti i siti di e-commerce dei paesi dell'Unione Europea senza essere discriminati a seconda dell'ubicazione geografica. A tal fine, le imprese operanti nel settore dovranno fare attenzione a verificare la *compliance* delle proprie condizioni generali di vendita su Internet.

[Leggi qui](#)

AGCOM: Pubblicate le Linee Guida sulle modalità di dismissione e trasferimento dell'utenza nei contratti per adesione

Delibera del 16 ottobre 2018, n. 487/18/CONS

L'Autorità per le Garanzie nelle Comunicazioni ("AGCOM") ha adottato le Linee guida volte a regolare i comportamenti degli operatori dei servizi di telefonia, televisivi e di comunicazione elettronica in fase di dismissione e trasferimento dell'utenza ad altro operatore, ai fini della corretta applicazione dalla c.d. Legge Bersani (D.L. 31 gennaio 2007, n. 7).

L'Autorità fornisce chiare indicazioni sulla (i) determinazione dei c.d. *switching cost* applicati dagli operatori in caso di recesso anticipato dell'utente e sulla (ii) corretta applicazione degli obblighi informativi e di comunicazione, nonché (iii) circa il limite di durata dei contratti che prevedono offerte promozionali.

[Leggi qui](#)

AGCOM: Online le modifiche al Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e relative procedure attuative

Modifiche al Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70, di cui alla delibera n. 680/13/CONS

Delibera del 16 ottobre 2018, n. 490

Il 18 ottobre 2018 sono state approvate le modifiche al Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica.

Il Regolamento indica quali procedure adottare ai fini dell'accertamento e dell'inoltro delle richieste finalizzate ad ottenere la cessazione delle violazioni del diritto d'autore e dei connessi diritti di privativa.

Le nuove norme disciplinano l'esercizio dei poteri che l'art. 2 della Legge europea 2017 ha attribuito all'AGCOM per consentirle di contrastare le violazioni più gravi mediante la previsione di misure cautelari finalizzate ad evitare la reiterazione delle violazioni.

L'Autorità, inoltre, potrà imporre ai *provider* di adottare le misure più idonee per evitare la reiterazione di violazioni già accertate e contrastare le iniziative volte ad eludere l'applicazione dei propri provvedimenti.

In linea con i più recenti orientamenti della giurisprudenza nazionale ed europea, l'Autorità aggiornerà, entro tre giorni dall'istanza, l'elenco dei siti oggetto di inibizione che si rigenerano mediante la sola modificazione del nome a dominio. Specifiche e ulteriori misure possono consistere anche nel c.d. "*notice and stay down*" e, quindi, nell'impedire il caricamento di contenuti già rimossi.

[Leggi qui](#)

Per il testo aggiornato del Regolamento

[Leggi qui](#)

Garante Privacy: pubblicato l'elenco dei trattamenti da sottoporre, ai sensi dell'art. 35 par. 4 del GDPR, a valutazione di impatto (DPIA)

Provvedimento dell'11 ottobre 2018, n. 467 [doc. web 9058979]

Il Garante Privacy, in ossequio al meccanismo di coerenza previsto dal Regolamento (UE) 2016/679 e recependo i rilievi formulati dall'EDPB, ha approvato la lista delle operazioni di trattamento transazionali soggette a DPIA ex art. 35 par. 4.

[Leggi qui](#)

Garante Privacy: l'Autorità rilascia il proprio parere sullo schema di disegno di legge sugli "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"

Provvedimento dell'11 ottobre 2018, n. 464 [doc. web n. 9051774]

Il Garante Privacy ha espresso parere favorevole allo schema di disegno di legge recante misure per il contrasto all'assenteismo dei dipendenti pubblici, fornendo, tuttavia, alcune osservazioni in relazione all'introduzione di sistemi di identificazione biometrica e videosorveglianza in sostituzione degli attuali sistemi di rilevazione automatica delle presenze.

Con specifico riguardo all'impiego simultaneo e obbligatorio di tali sistemi, il Garante ha evidenziato la necessità di limitare la scelta ad un unico sistema di verifica, il quale dovrà essere implementato nel rispetto del principio di gradualità, evitandone l'utilizzo laddove gli stessi non appaiano idonei agli scopi perseguiti. In ogni caso, l'Autorità suggerisce di ancorare l'impiego di tali strumenti alla sussistenza di specifici fattori di rischio o di

determinati presupposti (ad esempio, la dimensione dell'ente, il numero dei dipendenti coinvolti, ecc.).

Di particolare interesse le osservazioni tecniche sull'adeguatezza del termine "identificazione biometrica". Il Garante chiarisce che per "sistema di identificazione biometrica" si intende un sistema che opera verifiche "one-to-many", consentendo di rilevare in tempo reale il dato biometrico di un soggetto sconosciuto e di confrontarlo con i dati biometrici presenti in un database, i quali sono poi a loro volta associati a determinati soggetti.

Ai fini della rilevazione delle presenze, al contrario, i dipendenti che effettuano l'accesso sono già stati identificati e, pertanto, è sufficiente una verifica "one-to-one", da effettuarsi mediante sistemi da definirsi più correttamente quali "sistemi di verifica biometrica dell'identità".

[Leggi qui](#)

Garante Privacy: pubblicate le FAQ sulla tenuta del registro delle attività del trattamento

Comunicato stampa del 10 ottobre 2018 [doc. web 9047529]

Sul sito del Garante della Privacy sono state pubblicate le FAQ sul registro delle attività di trattamento previsto all'art. 30 del Regolamento (UE) 2016/679.

Le FAQ forniscono indicazioni precise sulle modalità di predisposizione, tenuta e aggiornamento di detto registro, nonché sui soggetti a ciò obbligati, i quali vengono individuati: (i) nelle imprese od organizzazioni con almeno 250 dipendenti; (ii) in qualunque altro titolare o responsabile che effettui trattamenti che possano presentare rischi, anche non elevati, per i diritti e le libertà delle persone o effettuino trattamenti non occasionali di dati oppure trattamenti di particolari categorie di dati (quali dati biometrici, dati genetici, dati sulla salute, sulle convinzioni religiose, sull'origine etnica ecc.) o relativi a condanne penali e a reati.

Inoltre, il Garante Privacy, in un'ottica di semplificazione, ha allegato alle FAQ un modello di "registro semplificato" per i titolari e i responsabili delle PMI.

[Leggi qui](#)

Garante Privacy: pubblicate le FAQ sulla definizione agevolata delle violazioni pendenti in materia di protezione dei dati personali

Comunicato stampa dell'1 ottobre 2018 [doc. web 9045581]

Sul sito del Garante della Privacy sono state pubblicate le FAQ per la definizione agevolata dei procedimenti pendenti e avviati entro il 25 maggio 2018.

Le FAQ forniscono utili indicazioni agli operatori per l'utilizzo del meccanismo di definizione agevolata dei processi pendenti introdotto dall'art. 18 del D.lgs. del 10 agosto 2018, n. 101, il quale attribuisce ai contravventori la possibilità di richiedere ed effettuare il pagamento dei 2/5 del minimo edittale della sanzione irrogatagli dal Garante entro e non oltre il 18 dicembre 2018.

[Leggi qui](#)

Garante Privacy: l'Autorità fornisce indicazioni sull'interpretazione delle istanze comprese nell'ambito degli “affari progressi” di cui all'articolo 19 del D.Lgs. 10 agosto 2018, n. 101.

Delibera del 27 settembre 2018, n. 455 [doc. web n. 9047256]

Il Garante della Privacy ha chiarito che, dal 4 ottobre 2018 e per i successivi 60 giorni, gli interessati o comunque chi vi abbia interesse possono presentare al Garante motivata richiesta di trattazione di reclami, segnalazioni e richieste di verifica preliminare inviati dagli stessi al Garante entro il 25 maggio 2018.

L'Autorità, inoltre, chiarisce che la richiesta non deve riguardare reclami e segnalazioni già esaminati, ovvero di cui la stessa Autorità ha già inviato all'istante comunicazione di avvio del procedimento, richiesta di informazioni, esibizione di documenti a terze parti o di altro atto recettizio.

[Leggi qui](#)

EDPB: pubblicata l'opinione dell'Autorità sull'elenco del Garante italiano per definire i trattamenti per cui è necessaria una DPIA

Opinion del 25 settembre 2018, n. 12

Il 25 settembre, il Comitato europeo per la protezione dei dati (EDPB) ha pubblicato l'Opinion sull'elenco dei trattamenti dei dati personali che, secondo il Garante della Privacy, richiederebbero una “Valutazione di Impatto sulla Protezione dei Dati” (DPIA).

[Leggi qui](#)

GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA UE

Il titolare di una connessione internet privata è responsabile dell'illecito download di contenuti protetti dal diritto d'autore

Corte di Giustizia UE, sentenza del 18 ottobre 2018, C-149/17

La Corte di Giustizia Europea, con la Sentenza nella causa C-149/17 si è pronunciata sull'interpretazione delle disposizioni in materia di tutela del diritto di proprietà intellettuale.

La CGUE, in particolare, ha stabilito che il detentore di una connessione Internet, attraverso la quale siano stati condivisi file protetti da diritto d'autore in modalità *peer-to-peer*, non può esonerarsi dalla propria responsabilità nei confronti del titolare dei diritti di proprietà intellettuale indicando semplicemente che un suo familiare aveva la possibilità di accedere alla suddetta connessione.

[Leggi qui](#)

Non acquista automaticamente la qualifica di “professionista” il soggetto che pubblica annunci di vendita su Internet

Corte di Giustizia UE; Sentenza del 4 ottobre 2018, C-105/17

Alla Corte di Giustizia UE è stata sottoposta questione pregiudiziale sulla possibilità di qualificare, ai sensi della normativa consumeristica, come “professionista” il soggetto che pubblichi annunci di vendita su diversi siti internet.

La Corte suggerisce un approccio interpretativo “caso per caso”, in virtù del quale il giudice è chiamato a valutare, *in primis*, se il soggetto agisce avvalendosi di un contesto organizzato per lo svolgimento dell’attività di vendita.

Secondo la Corte, ai sensi della Direttiva sulle pratiche commerciali sleali e la Direttiva 2011/83/UE (c.d. “*Consumer Rights*”), la persona fisica che pubblica contemporaneamente su Internet un certo numero di annunci per la vendita di beni nuovi e d’occasione può qualificarsi come “professionista” e la relativa condotta può costituire “pratica commerciale” solo nella misura in cui il soggetto in questione abbia agito in un contesto organizzato e nell’ambito dello svolgimento di un’attività commerciale, industriale, artigianale o professionale.

[Leggi qui](#)

Accesso consentito ai dati conservati dai fornitori dei servizi di comunicazione elettronica anche per il perseguimento di reati non gravi

Corte di Giustizia UE, Sentenza del 2 ottobre 2018, C-207/16

La Corte di Giustizia, nell’ambito delle indagini su una rapina con sottrazione di un telefono cellulare, è stata chiamata a verificare la legittimità dell’accesso ai dati personali conservati dai fornitori di servizi di comunicazione elettronica da parte delle autorità nazionali competenti per l’accertamento di reati anche “non gravi” (ossia con pena inferiore ai 5 anni).

La Corte, effettuata un attento bilanciamento degli interessi in gioco, ha sostenuto che l’accesso delle autorità pubbliche a dati di natura meramente identificativa non costituisce un’ingerenza grave nei diritti fondamentali degli interessati, poiché trova giustificazione nelle generali esigenze di prevenzione, accertamento e perseguimento di reati, a prescindere dalla loro gravità.

[Leggi qui](#)

GIURISPRUDENZA NAZIONALE

Rimessa alle Sezioni Unite la questione sul bilanciamento tra diritto all’oblio e diritto di cronaca

Cassazione Civile, Sez. III, Ordinanza del 5 novembre 2018, n. 28084

La Cassazione, con ordinanza del 5 novembre 2018, n. 28084, ha rimesso gli atti al Primo Presidente per la eventuale assegnazione alle Sezioni Unite della questione sul corretto bilanciamento tra diritto all’oblio e diritto di cronaca.

La questione scaturisce dalla difficoltà di individuare correttamente i presupposti per l’esercizio, da parte del singolo, del diritto all’oblio in caso di ripubblicazione, a distanza di molti anni, di una notizia risalente nel tempo che lo riguarda.

[Leggi qui](#)

La certificazione ISO/IEC 27001 non può costituire requisito per il conferimento dell'incarico di DPO

TAR Friuli Venezia Giulia, Sez. I, Sentenza 13 settembre 2018, n. 287

È illegittimo richiedere il possesso della certificazione ISO/IEC 27001 quale requisito di ammissione ad una procedura selettiva per il conferimento dell'incarico di Data Protection Officer ("DPO").

Il TAR ha chiarito che il nucleo essenziale della funzione di garanzia propria del DPO è rappresentato dalla tutela del diritto fondamentale alla protezione dei dati personali e non dalla predisposizione di meccanismi volti a incrementare i livelli di efficienza e sicurezza nella gestione delle informazioni.

[Leggi qui](#)

PROVVEDIMENTI DELLE AUTORITÀ DI REGOLAZIONE

AGCM: l'Autorità sanziona Facebook per uso dei dati degli utenti a fini commerciali

Provvedimento del 29 novembre 2018

Con provvedimento del 29 novembre 2018, l'Autorità Garante della Concorrenza e del Mercato (di seguito "AGCM") ha concluso l'istruttoria avviata nell'aprile 2018 nei confronti di Facebook Ireland Ltd. e della sua controllante Facebook Inc. (di seguito "Facebook") per presunte violazioni del Codice del Consumo.

L'AGCM ha accertato che Facebook non ha informato adeguatamente e immediatamente i consumatori, in fase di attivazione dell'account, delle finalità connesse all'attività di raccolta dei dati forniti da questi ultimi, inducendoli ingannevolmente a registrarsi sulla omonima piattaforma enfatizzandone la gratuità del servizio.

Inoltre, secondo l'AGCM Facebook avrebbe attuato una pratica aggressiva esercitando un indebito condizionamento nei confronti dei consumatori registrati che, attraverso la pre-selezione della funzione "Piattaforma attiva", subiscono la trasmissione dei loro dati a siti web/app di terzi per finalità commerciali, con numerosi ostacoli alla fruibilità del social network in caso di revoca del consenso.

L'AGCM ha, quindi, irrogato una sanzione amministrativa pecuniaria dall'ammontare complessivo pari a 10 milioni di euro nei confronti di Facebook, nonché, ai sensi dell'art. 27, comma 8, del Codice del Consumo, gli ha imposto l'obbligo di pubblicare una dichiarazione rettificativa sul sito internet e sull'app per informare i consumatori.

[Leggi qui](#)

AGCM: Apple e Samsung multate per pratiche commerciali scorrette in relazione al rilascio degli aggiornamenti dei sistemi operativi IOS e Android

AGCM Provvedimenti del 24 ottobre 2018, nn. 27363 e 27365

Ad esito di due complesse istruttorie, con due distinti Provvedimenti, l'AGCM ha accertato la violazione degli artt. 20, 21, 22 e 24 del Codice del Consumo da parte delle società del gruppo Apple e Samsung.

In particolare, è stato rilevato che entrambe le società hanno posto in essere pratiche commerciali scorrette in relazione al rilascio di alcuni aggiornamenti del firmware dei loro smartphones (iPhone 6/6 Plus/6s/6s Plus e Galaxy Note 4) provocando gravi disfunzioni e riducendo in modo significativo le prestazioni degli stessi, accelerando così il loro processo di sostituzione (c.d. “obsolescenza programmata”).

Secondo l’Autorità, le società, al fine di perseguire una più ampia politica industriale, avrebbero indotto i consumatori, mediante insistenti richieste, ad effettuare il download e a installare gli aggiornamenti dei software IOS e Android su dispositivi non in grado di supportarli tecnicamente senza fornirgli preventivamente adeguate informazioni circa l’impatto di tale scelta sulle prestazioni dei prodotti dagli stessi acquistati.

Oltretutto, a seguito delle richieste pervenute dai consumatori, le società non avrebbero offerto un’adeguata gestione delle richieste di assistenza rivolte dai consumatori, né avrebbero offerto a questi ultimi la possibilità di ripristinare l’originaria funzionalità degli apparecchi in caso di sperimentata diminuzione delle prestazioni dovuta agli aggiornamenti dagli stessi installati (c.d. “downgrading”).

Per Provvedimento Apple

[Leggi qui](#)

Per Provvedimento Samsung

[Leggi qui](#)

Garante Privacy: secondo l’Autorità, il sistema di fatturazione elettronica ipotizzato dall’Agenzia delle Entrate sarebbe in contrasto con la normativa in materia di protezione dei dati personali

Provvedimento del 15 novembre 2018, n. 481

Con Provvedimento del 15 novembre 2018, il Garante Privacy, esercitando per la prima volta il potere correttivo di avvertimento attribuito dall’art. 58, par. 2, lett. a) del GDPR nei confronti dell’Agenzia delle entrate, ha sottolineato l’incompatibilità del nuovo sistema connesso all’obbligo di fatturazione elettronica con la normativa in materia di protezione dei dati personali.

Nel provvedimento si rileva come una preventiva consultazione dell’Autorità, peraltro stabilita dal previgente Codice privacy, avrebbe potuto assicurare, fin dalla progettazione, l’avvio del nuovo obbligo con modalità e garanzie *privacy compliant*, introducendo misure tecnico-organizzative adeguate in tutta la filiera del trattamento dei dati personali utilizzati per la fatturazione elettronica. Detto sistema presenta, secondo il Garante, un rischio elevato per i diritti e le libertà degli interessati poiché comporta un trattamento sistematico, generalizzato e di dettaglio di dati personali su larga scala, potenzialmente relativo ad ogni aspetto della vita quotidiana dei cittadini.

In particolare, sempre secondo l’Autorità, tale trattamento sarebbe sproporzionato rispetto all’obiettivo di interesse pubblico perseguito.

[Leggi qui](#)

* * *

Il presente documento non ha carattere di esaustività e ha finalità meramente informativa.