TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI

Segnalazioni giuridiche a cura del Servizio Centrale Legale

N. 4 Anno XXIV
Aprile 2019

INDICE:

portale dei servizi telematici gestito dal Ministero della Giustizia.
Quanto alla procedura, la domanda per l'azione di classe potrà essere proposta con ricorso esclusivamente davanti alla sezione specializzata del Tribunale in materia di imprese competente per il luogo ove ha sede la parte resistente. Il procedimento sarà regolato dal rito sommario di cognizione *ex* art. 702-*bis* ss., senza che possa essere disposto il mutamento del rito. Una disciplina *ad hoc* è anche prevista per gli accordi transattivi tra le parti, spettando al Tribunale, "*ove possibile*" (qualunque cosa questo significhi), formulare una proposta transattiva o conciliativa. Inoltre, tra le spese del procedimento è stato inserito un apposito compenso che, in caso di condanna, il resistente dovrà corrispondere al rappresentante comune della "classe". È altresì prevista la possibilità di esperire l'esecuzione forzata in forma collettiva, promossa dal rappresentante comune degli aderenti.
È infine specificamente disciplinata l'azione inibitoria collettiva rispetto ad atti e comportamenti posti in essere in pregiudizio di una pluralità di individui o enti, che può essere proposta da chiunque abbia interesse ad ottenere la cessazione o il divieto di reiterazione di tale condotta.
La nuova disciplina in materia di class action, che indubbiamente ne estende il campo di applicazione promuovendo il ricorso a tale rimedio, entrerà in vigore decorsi 12 mesi dalla data di pubblicazione in Gazzetta Ufficiale e si applicherà alle condotte illecite poste in essere successivamente alla data di entrata in vigore. Alle condotte illecite poste in essere precedentemente continueranno ad applicarsi le disposizioni al momento vigenti.

Avv. Martina Bischetti
Freshfields Bruckhaus Deringer

IL PARLAMENTO APPROVA LE DIRETTIVE A TUTELA DEGLI ACQUISTI DI BENI E SERVIZI ONLINE ED OFFLINE DA PARTE DEI CONSUMATORI

Direttiva sui contenuti digitali - Direttiva sulle vendite dei beni

Il Parlamento Europeo ha approvato lo scorso 26 marzo un pacchetto di norme volte a r**afforzare la tutela dei consumatori negli acquisti sia online che tramite i canali tradizionali**.
Le due direttive sui contenuti digitali e sulla vendita di beni fanno parte della strategia per il mercato unico digitale, che mira a garantire un migliore accesso dei consumatori e delle imprese ai beni e ai servizi online in tutta Europa.
Le nuove leggi armonizzano i principali diritti contrattuali, quali i mezzi e le modalità di ricorso e di rimborso a disposizione dei consumatori.
Le norme sui contenuti digitali mirano a garantire che chi acquista o scarica musica, app, giochi o utilizza servizi cloud o piattaforme di social media sarà finalmente protetto qualora l'operatore non fornisca il contenuto digitale o ne fornisca uno difettoso.
Il testo prevede che **qualora il contenuto digitale difettoso non sia correggibile o sostituibile in un tempo ragionevole, il consumatore avrà diritto ad una riduzione di prezzo o al rimborso integrale entro 14 giorni**. E' prevista la presunzione che il difetto sussista già se il difetto si manifesta entro un anno dalla fornitura, senza che il consumatore ne debba fornire la prova.
Il diritto di garanzia anche per gli acquisti di contenuti digitali non può essere inferiore a due anni.
In considerazione del sempre maggiore valore economico che stanno assumendo i dati personali, particolarmente interessante è la previsione che riconosce pari diritti a quei consumatori che forniscono i propri dati personali in cambio di contenuti o servizi digitali; il rilascio dei propri dati personali viene di fatto riconosciuto, qual è in effetti, come una controprestazione equivalente al pagamento e conseguentemente all'utente vengono riconosciute le medesime tutele.
La direttiva sulla vendita di beni si applica ai prodotti o servizi acquistati sia on line che in un negozio tradizionale.
Il commerciante sarà in ogni caso, qualunque sia il canale di vendita, responsabile qualora il difetto del prodotto si manifesti entro 2 anni dal momento in cui il consumatore ha ricevuto il prodotto.
La nuova normativa prevede che i consumatori che acquistano beni con elementi digitali avranno il diritto di ricevere gli aggiornamenti necessari durante tutto "il periodo di tempo che il consumatore può ragionevolmente attendersi" in base alla tipologia e alla destinazione dei beni e agli elementi digitali.
Entrambe le direttive dovranno essere sottoposte all'approvazione formale del Consiglio dei Ministri dell'UE, entreranno in vigore 20 giorni dopo la pubblicazione sulla GUCE e dovranno essere attuate dagli Stati membri entro 2 anni; conoscerne il contenuto in anticipo però è fondamentale per i professionisti al fine di pianificare le proprie strategie commerciali.

Avv. Eleonora Lenzi
Studio Legale Stefanelli

PRIVACY

SITI INTERNET: IL PROBLEMA DELLA GESTIONE DEI COOKIE ATTRAVERSO RECENTI PROVVEDIMENTI EUROPEI

I cookie sono piccoli file di testo che vengono inviati al browser durante la navigazione sul web e sono fonte di preoccupazione per molti utenti, ma anche per molti proprietari di siti internet in quanto la loro non corretta "gestione" può comportare sanzioni sgradevoli e non è sempre facile individuarne i corretti adempimenti.
La materia è stata disciplinata dalla direttiva comunitaria 2009/136/CE che ha modificato la direttiva 2002/58/CE (E-Privacy), imponendo al gestore del sito web di informare l'utente del fatto che fa uso dei cookie sul sito, e in determinati casi a ottenere il consenso preventivo all'uso degli stessi.
La direttiva europea del 2009 si limitava a creare un quadro normativo all'interno del quale erano, eventualmente, i singoli Garanti nazionali a definire una regolamentazione di dettaglio. La normativa in materia di cookie, di cui alle direttive europee, è stata recepita in Italia con la nuova formulazione dell'art. 122 D. Lgs 196/2003 ad oggi ancora in vigore in quanto il Regolamento ePrivacy che dovrebbe sostituire la Direttiva 2009/136/CE è in fase di approvazione. Nel frattempo, tuttavia, il nuovo Regolamento europeo in materia di protezione dei dati personali (GDPR) 2016/679 non può dirsi del tutto estraneo alla materia, vista anche l'inclusione dei Cookie all'applicazione del GDPR nel Considerando 30.
Si ricorda, poi che il rapporto tra GDPR e Regolamento ePrivacy è già stato esaminato dall'European Data Protection Board (si veda articolo "Il digital marketing tra la disciplina del GDPR e la "normativa ePrivacy") ma il tema dei cookie resta di grande interesse, come dimostrato dai Provvedimenti emanati di recente.

Si riportano di seguito alcuni interessanti Provvedimenti di Autorità e Corti Europee che hanno trattato la tematica fornendo utili suggerimenti.

Il 7 marzo 2019, l'Autorità di controllo per la protezione dei dati personali olandese ha emesso una guida sull'utilizzo dei cookie nei siti web. La guida in questione ha ritenuto illegittimo l'impiego dei cosiddetti **"cookie wall", cioè di quei banner che informano l'utente dell'utilizzo dei cookie che consentono di accedere al contenuto del sito solo a seguito dell'accettazione degli stessi**.
L'unico modo che hanno i fruitori del sito stesso per accedere ai contenuti della pagina web è quello di accettare i cookie in questione.
L'Autorità olandese ha motivato la propria posizione ritenendo che il cookie wall non permette di ottenere validamente il consenso degli utenti. Infatti, ai sensi dell'articolo 4, n. 11) del Regolamento (UE) 2016/679, il consenso dell'interessato si definisce come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".
Secondo l'Autorità i problema è il requisito della "libertà del consenso", che sarebbe pregiudicato nel caso in cui all'interessato non fosse data la possibilità di rifiutare l'installazione dei cookie, in particolare quelli di profilazione, quantomeno senza incorrere in conseguenze negative, quali l'impossibilità di utilizzare il sito.
In altri termini: il gestore del sito, nel proporre il banner, deve effettuare una distinzione tra i cookie tecnici e quelli di profilazione, dando la possibilità di accedere ai contenuti anche a coloro che dovessero rifiutare i secondi.

La posizione del Garante Olandese, peraltro è in linea con l'approccio già adottato dall'Autorità per la protezione dei dati personali austriaca (decisione del 30 novembre 2018) dove è stata sanzionata la modalità di acquisizione del consenso al "cookie di marketing" che non era realmente volontario in conformità con i principi del GDPR.
In materia di cookie un'altra interessante sentenza è stata emessa dal Consiglio di Stato francese il 6 giugno 2018.
Nel caso specifico il CNIL, cioè l'Autorità Garante francese, aveva imposto alla società Editions Croque Future di rispettare le norme in materia di protezione dei dati personali nell'utilizzo di cookie. La società in questione, infatti, depositava i cookie sui terminali degli utenti senza informarli preventivamente. La suddetta società impugna il provvedimento del Garante, ma il Consiglio di Stato da ragione al Garante francese.
In particolare, il Consiglio di Stato conferma che **i cookie che hanno finalità pubblicitaria non possono essere ritenuti "strettamente necessari"**, e quindi sono soggetti a consenso preventivo. Anche se tali cookie sono necessari per la redditività economica del sito, nel senso che il sito dipende letteralmente dai guadagni pubblicitari per mantenersi, i cookie in questione devono comunque essere preventivamente autorizzati dagli utenti, consentendo loro anche di esercitare il diritto di opposizione. In tal senso la base

giuridica per i cookie pubblicitari può essere solo il consenso dell'utente e non l'interesse legittimo.

Si segnala un interessante elemento trattato dal Consiglio francese: la problematica dei cookie di terze parti. In particolare il Consiglio evidenzia che l'"editore" di un sito (cioè il gestore materiale) è comunque "responsabile" (nel senso che ne risponde) dei cookie anche se questi sono di "terze parti" (es. Facebook), in quanto ne autorizza il trattamento. In tal senso è "titolare" (controller) del trattamento, anche se le finalità dei cookie sono effettivamente stabilite dalla terza parte.
In tal senso il titolare del trattamento, cioè il gestore del sito, deve anche garantire i tempi di conservazione del cookie, che devono essere proporzionati alla finalità, e quindi fissati dal CNIL in un massimo di 13 mesi.
Si segnalano, infine, due casi in attesa del giudizio della Corte di Giustizia.
Il prima relativo alla Causa Fashion ID (C-40/17) riguardante una società La Fashion ID GmbH & Co. KG che commercializza articoli di moda online. Essa ha inserito un plugin nel suo sito Internet: il pulsante «Like» di Facebook. Di conseguenza, quando un utente entra nel sito Internet della Fashion ID, le informazioni relative all'indirizzo IP e alla stringa del browser di tale utente sono trasferite a Facebook. Detto trasferimento avviene automaticamente quando si apre il sito Internet della Fashion ID, indipendentemente dal fatto che l'utente abbia cliccato o meno il pulsante «Like» e abbia o meno un account Facebook.
L'associazione tedesca per la tutela dei consumatori riteneva che l'uso di tale plugin comporta la violazione della normativa sulla protezione dei dati. Il Caso arriva davanti al Tribunale tedesco che richiede alla Corte di Giustizia chiarimenti sull'interpretazione di varie disposizioni della direttiva 95/46/CE. Tra le questioni poste riguardanti il trattamento dati, alcune riguardano il dovere di Fashion ID di informare e raccogliere il consenso dagli interessati.

Il secondo Giudizio atteso dalla Corte di Giustizia (C-673/2017) ha origine da caso pendente davanti alla Corte federale di giustizia tedesca che riguarda un gioco a premi organizzato dalla "Planet49", il cui sito richiedeva agli utenti il consenso installazione di cookie mediante una casella di spunta preselezionata. In sostanza viene richiesto alla Corte di chiarire se, alla luce del diritto Ue, il consenso all'istallazione di cookie possa essere validamente ottenuto nei modi sopra descritti, e quali informazioni debbano essere fornite all'utente riguardo all'uso dei cookie affinché si possa ritenere che il consenso espresso sia "informato". Particolarmente interessante di tale ultimo caso è che nelle Conclusioni dell'Avvocato Generali viene interpretato il caso alla luce non solo da Direttiva 95/46/CE, ma anche del Regolamento 2016/679.

Avv. Alessandra Delli Ponti
Studio Legale Stefanelli

DIECI BUONE PRATICHE PER UNA REGISTRAZIONE EFFICACE DELLE VIOLAZIONI DI DATI

Proseguiamo in questo articolo l'approfondimento sul Data Breach, prendendo spunto da alcune importanti indicazioni fornite dal Garante per la Protezione dei Dati Personali dei Paesi Bassi (**Autoriteit Persoongegevens – di seguito indicato come AP**). L'AP, infatti, in data 17 marzo ha comunicato che solo il 60% dei registri delle violazioni, esaminati in un recente studio esplorativo, presenta adeguatamente gli elementi richiesti dalla normativa.
Ricordiamo che l'art. 33 del Regolamento UE 2016/679, riporta che "**Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".** La violazione di tale disposizione è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000€, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Questo articolo richiede quindi di documentare le violazioni di dati personali, sebbene non si specifichi come tale operazione vada svolta. In supporto ai titolari del trattamento, il WP250 rev. 01 "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679", adottate il 3 ottobre 2017 - Versione emendata e adottata in data 6 febbraio 2018, consiglia di utilizzare un "Registro delle violazioni" che includa quelle non notificate al Garante.

La corretta predisposizione di un Registro delle violazioni è pertanto un'azione fondamentale, per comprovare che tutte le azioni richieste al titolare per la gestione dei Data Breach siano state osservate, ma anche per fare valutazioni di azioni preventive in merito a incidenti informatici. Sarebbe infatti un errore focalizzarsi unicamente sulle conseguenze sanzionatorie di un eventuale illecito: al contrario, per lavorare in

un'ottica di prevenzione degli incidenti e considerare i vantaggi che possono derivare da una corretta organizzazione delle procedure di gestione del Registro dei Data Breach, risultano interessanti i seguenti 10 suggerimenti del Garante olandese.

1. **Descrivere in maniera chiara e completa gli incidenti**
   Il Registro dei Data Breach dovrebbe descrivere in maniera dettagliata l'incidente di sicurezza. Data e ora dell'episodio, momento in cui si è venuto a conoscenza dello stesso, fonte di segnalazione potrebbero essere utili elementi da tracciare.
   Tutto ciò offrirà l'opportunità di monitorare l'efficienza del sistema di rilevazione degli incidenti, elemento spesso sottovalutato nei sistemi di gestione dei dati, e a cui invece si legano sia importanti aspetti tecnici (in particolare per incidenti di natura informatica), sia aspetti organizzativi e di sensibilizzazione del personale.
2. **Distinguere misure preventive e misure correttive**
   Si ricorda che mentre le Azioni correttive hanno lo scopo di eliminare la causa di una non violazione ai dati personali, le Azioni preventive hanno l'obiettivo di eliminare la causa potenziale della violazione per evitare che si ripresenti.
   Entrambe le misure dovranno essere inserite nel Registro, indicando infine anche le misure che dovrebbero essere implementate in futuro.
3. **Evitare di frammentare le registrazioni degli incidenti**
   La documentazione raccolta sui Data Breach è funzionale quando organizzata come una panoramica sul sistema di gestione del dato. Evitare differenze nel livello di dettaglio degli eventi registrati e regolare la gestione di tutte le violazioni attraverso un'unica procedura (messa a disposizione di tutto il personale), permetterà di raccogliere le informazioni in modo uniforme e consentirà all'organizzazione di effettuare delle valutazioni d'insieme. L'organizzazione potrà pertanto sfruttare meglio le esperienze passate per evitare o prevenire ulteriori incidenti futuri.
4. **Riportare se e come il DPO è stato coinvolto negli eventi e nella registrazione degli stessi**
   Tra i suoi compiti del DPO vi sono quelli di cooperare con l'autorità di controllo e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento. Conviene pertanto considerare sempre un suo coinvolgimento nella gestione della violazione dei dati personali e nella compilazione del Registro delle violazioni. Non è da escludere il completo affidamento del compito di compilazione del Registro allo stesso DPO.
5. **Riportare le segnalazioni all'Autorità di controllo e ai soggetti coinvolti**
   In fase di gestione delle violazioni, non tutti i Data Breach verranno notificati all'Autorità di controllo, e non tutti i Data Breach notificati dovranno essere necessariamente comunicati agli interessati. La scelta di effettuare tali comunicazioni dovrà dipendere dalla valutazione sulla presenza di rischio per i diritti e le libertà degli interessati, e sull'entità dello stesso. È quindi fondamentale documentare tali scelte, le ragioni che le hanno determinate, e stabilire preventivamente i criteri di valutazione del rischio (ad es. tramite il tool della CNIL https://www.cnil.fr/sites/default/files/typo/document/Notifications-AutoEvaluation.xls).
6. **Agire con trasparenza nei confronti delle persone interessate**
   Nello svolgimento di un'eventuale comunicazione agli interessati, i titolari del trattamento devono tenere in considerazione il modo migliore per effettuare tale comunicazione, l'urgenza e la sicurezza dei possibili metodi. Si suggerisce perciò di indicare nel Registro delle violazioni le motivazioni che hanno guidato le scelte sulla modalità di comunicazione, allegando ad ogni episodio le prove di tali comunicazioni, che dovranno essere sempre archiviate e conservate.
7. **Preparare un manuale e formare il personale incaricato della registrazione della violazione dei dati**
   Come già evidenziato in altri punti, la predisposizione di una procedura o di un manuale che guidi le operazioni di gestione del Data Breach e di compilazione del Registro delle violazioni è il modo migliore per assicurarsi di rispettare tutti gli adempimenti. Inutile sottolineare che, agendo d'anticipo, si potrà evitare (o, almeno, ridurre) il panico tipico delle situazioni d'urgenza: avendo già designato le attività da svolgere, il rispetto dele termine di 72 ore verrà facilitato.
8. **Riportare quali altre organizzazioni sono state coinvolte in una violazione**
   Sempre in un'ottica di miglioramento e prevenzione, tenere traccia degli altri eventuali soggetti (Titolari, Responsabili o sub-Responsabili del trattamento) che sono stati coinvolti nella violazione di dati personali, nonché del livello di coinvolgimento degli stessi, risulterà utile per definire anche gli aspetti da trattare in fase di stipula o rinnovo di contratti.

9. **Classificare le violazioni dei dati**
   Una classificazione dei tipi di violazione di dati, in relazione alla natura dell'incidente, alle sue conseguenze, alle parti interessate e alle misure attivate, può essere d'aiuto per monitorare gli sviluppi nel tempo del proprio sistema di sicurezza. Inoltre, l'organizzazione potrà basarsi su queste informazioni per stabilire i successivi interventi di implementazione consentendo una programmazione delle risorse da coinvolgere.
10. **Discutere regolarmente la registrazione della violazione dei dati al livello giusto all'interno dell'organizzazione come parte di un ciclo di pianificazione-controllo / apprendimento.**
    Le informazioni raccolte nel Registro dovrebbero essere regolarmente discusse al corretto livello di gestione tra le funzioni aziendali coinvolte, e diventare parte integrante di un ciclo di pianificazione-esecuzione-controllo-azione finalizzato allo sfruttamento degli incidenti come opportunità di apprendimento e miglioramento continuo.

Avv. Fabio Marinello
Studio Legale Stefanelli

DIRETTORE RESPONSABILE
Maria Antonietta Portaluri

REDAZIONE
Alessandra Toncelli – Mirella Cignoni – Mattia Ciribifera

LA REDAZIONE RINGRAZIA PER LA COLLABORAZIONE

Prof. Avv. Fabio Bortolotti e Avv. Silvia Bortolotti, BBM Partners, Buffa, Bortolotti & Mathis - Avv. Martina Bischetti, Avv. Luca Feltrin e Avv. Roberta Laghi, Freshfields Bruckhaus Deringer (Milano) - *Avv. Alessandra Delli Ponti, Avv. Eleonora Lenzi e Avv. Fabio Marinello,* Studio Legale Stefanelli (Bologna).

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

***Te*Lex Anie**

Pubblicazione a cura di:
Servizio Centrale Legale
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.246
e-mail legale@anie.it
Diffusione via web www.anie.it