OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Luglio 2023

MONTHLY ROUNDUP

Luglio 2023

I principali aggiornamenti in materia di TMT & Data Protection del mese

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Provvedimenti del Garante Privacy

- App per rimborso pedaggi: il Garante multa una società per l'errata qualificazione dei ruoli privacy [Link]
- Fidelity card: il Garante multa una società per la violazione di numerose disposizioni del GDPR [Link]
- Giornalismo: il Garante sanziona un quotidiano per la pubblicazione di dati personali e dettagli di minori [Link]
- Sanità: il Garante sanziona un centro medico per aver violato il principio di esattezza e integrità mediante lo scambio delle informazioni sanitarie di due pazienti [Link]

Provvedimenti EU

- European Commission adopts new adequacy decision for safe and trusted EU-US data flows [Link]
- Questions & Answers: EU-US Data Privacy Framework [Link]
- EDPB informs stakeholders about the implications of the DPF and adopts a statement on the first review of the Japan adequacy decision [Link]
- Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases [Link]
- Cyber Resilience Act: MEPs back plan to boost digital products security [Link]

PRINCIPALI AGGIORNAMENTI

- Qualificazione dei ruoli privacy: quanto è importante e quali sono le possibili ripercussioni
- Fidelity card: come trattare i dati personali raccolti per finalità di marketing e profilazione
- L'AgCOM adotta le Linee Guida concernenti i meccanismi di reclamo da parte degli utenti

Qualificazione dei ruoli privacy: quanto è importante e quali sono le possibili ripercussioni

Lo scorso 17 luglio, l'Autorità Garante per la protezione dei dati personali (il "**Garante**" o l'"**Autorità**") ha reso noto, nella sua newsletter (disponibile **qui**), di aver emesso un provvedimento sanzionatorio pari a un milione di euro nei confronti di Autostrade per l'Italia S.p.A. ("**ASPI**") per avere trattato in modo illecito i dati di circa 100mila utenti registrati alla app per il rimborso del pedaggio, denominata *Free to X* ("**FtX**"), in violazione del Regolamento UE 679/2016 ("**GDPR**").

L'attività ispettiva era stata avviata a seguito di un reclamo presentato dall'associazione dei consumatori Assoutenti, ove la stessa aveva sollevato alcuni profili di criticità in merito alle attività di trattamento dei dati personali degli utenti attuate da ASPI e da FtX, per il tramite dell'applicazione denominata "*Free To X*", volta a consentire il rimborso, totale o parziale, del costo del biglietto autostradale per ritardi dovuti a cantieri per lavori (c.d. servizio Cashback).

La decisione del Garante

Al termine dell'istruttoria, il Garante ha accertato che l'accordo tra ASPI e FtX identificava **erroneamente** ASPI come responsabile del trattamento, anziché come titolare del trattamento. Al riguardo, il Garante ha rilevato che l'errata qualificazione dei ruoli svolti dalle due società aveva inciso sull'informativa privacy fornita agli utenti, la quale **non è stata quindi correttamente formulata**. Inoltre, il Garante ha ritenuto ASPI inadempiente rispetto all'obbligo di designare FtX quale responsabile del trattamento. Pertanto, il Garante ha concluso che ASPI ha trattato illecitamente i dati personali di circa 100.000 interessati, infliggendo alla stessa una multa pari a 1 milione di euro.

Il Garante ha irrogato la suddetta sanzione, non imponendo tuttavia ulteriori misure correttive in quanto ASPI aveva collaborato nel corso del procedimento mediante l'adozione di misure correttive, tra cui l'aggiornamento dell'informativa sulla privacy.

Considerazioni generali

Sulla base di quanto accertato dal Garante, il servizio di Cashback, fornito tramite l'app di FtX, era stato posto in essere da ASPI, in qualità di titolare del trattamento.

Secondo l'Autorità risulta necessario identificare con **precisione** i soggetti che trattano i dati personali degli interessati e definirne **chiaramente** le rispettive attribuzioni, in particolare quella di titolare e di responsabile, ai fini della corretta applicazione della normativa in materia di protezione dei dati personali rispetto alle attività di trattamento svolte.

In particolare, si ricorda che, ai sensi dell'art. 4(7) del GDPR, il titolare del trattamento è il soggetto che determina le finalità e i mezzi del trattamento di dati personali. Di contro, il responsabile del trattamento, ai sensi dell'art. 4(8) del GDPR, è il soggetto che agisce per conto del titolare ed è chiamato a seguire le istruzioni impartite da quest'ultimo per quanto concerne la finalità del trattamento e gli elementi essenziali che ne costituiscono i mezzi (cfr. "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", le "**Linee Guida**", dell'European Data Protection Authority, "**EDPB**").

Ai fini di una corretta qualificazione dei ruoli privacy, occorre effettuare una **valutazione delle circostanze concrete del trattamento**. La valutazione deve tener conto di **tutte le circostanze** di fatto pertinenti, al fine di stabilire se uno specifico soggetto eserciti un'influenza **determinante** sul trattamento dei dati personali in questione.

La necessità di una valutazione fattuale significa anche che la titolarità di un trattamento non deriva dalle caratteristiche soggettive di chi tratta i dati, ma dalle attività concretamente svolte da tale soggetto in un contesto specifico. In altre parole, uno stesso soggetto può agire contemporaneamente in qualità di titolare del trattamento per determinate operazioni di trattamento, e in qualità di responsabile del trattamento per altre operazioni. La qualifica di titolare o di responsabile del trattamento va valutata in relazione a ciascuna specifica attività di trattamento dei dati.

Nel caso di ASPI, l'Autorità ha rilevato che il meccanismo di rimborso mediante l'app di FtX era stato **individuato da ASPI**, in qualità di concessionario della costruzione e dell'esercizio della rete autostradale, e che la natura delle misure compensative, così come le modalità di adempimento delle stesse, le condizioni e i requisiti della richiesta di rimborso da parte dell'utente, erano state definite autonomamente dalla stessa ASPI.

La società, infatti, aveva ideato il meccanismo, dando a **FtX** esclusivamente l'incarico di sviluppare uno strumento informatico volto a offrire una soluzione gratuita, smart e user friendly per la gestione dei rimborsi sui ritardi significativi causati dalla presenza di cantieri di lavoro sulle tratte autostradali affidate in concessione ad ASPI, fornendo alla stessa anche criteri già puntualmente stabili.

Alla luce di quanto sopra, il Garante ha evidenziato come emerga chiaramente che, con riferimento al trattamento inerente al servizio Cashback, le finalità e i relativi mezzi sono stati determinati da ASPI e, pertanto, che la stessa rivestiva (e riveste) il ruolo di titolare. Dall'altro lato, FtX agirebbe in qualità di responsabile del relativo trattamento.

A cascata, l'errata qualificazione dei ruoli privacy ha avuto ripercussioni su tutti gli adempimenti richiesti dalla normativa in materia di protezione dei dati personali.

In particolare, il Garante ha evidenziato come l'informativa fornita agli utenti non sia stata **correttamente formulata** in quanto, con riferimento al servizio Cashback, riportava **erroneamente** quale titolare del trattamento FtX e non ASPI, effettiva titolare del trattamento, e **mancava di tutte le ulteriori informazioni** volte ad assicurare un **trattamento corretto** e **trasparente** nei confronti degli utenti. In tal modo, ASPI ha violato i principi di correttezza e trasparenza di cui all'art. 5(1)(a) del GDPR, nonché l'art. 13 del GDPR, con riferimento alle informazioni da fornire agli interessati.

Inoltre, l'errata qualificazione dei ruoli privacy ha, altresì, condotto ASPI ad una ulteriore violazione, in quanto la stessa, effettiva titolare del trattamento, non aveva designato FtX quale responsabile del trattamento, ai sensi dell'art. 28 del GDPR. Sul punto, infatti, il Garante ha evidenziato come ASPI, con riferimento al servizio Cashback, avrebbe dovuto vincolare FtX, in qualità di responsabile, ad ASPI stessa, in qualità di titolare e non viceversa.

Conclusioni

Il provvedimento del Garante porta ad alcune considerazioni sugli adempimenti che le società dovrebbero tenere in considerazione al fine di

essere conforme alla normativa in materia di protezione dei dati personali.

Secondo le Linee Guida dell'EDPB, le due condizioni fondamentali per la qualifica di responsabile del trattamento sono:

- l'essere un soggetto distinto rispetto al titolare del trattamento;
- il trattare i dati personali per conto del titolare del trattamento.

L'EDPB rammenta altresì che non tutti i fornitori di servizi che trattano dati personali nel corso della prestazione sono responsabili del trattamento, poiché il ruolo di responsabile del trattamento non scaturisce dalle caratteristiche del soggetto che tratta dati, ma dalle sue **attività concrete** in un **contesto specifico**. In altre parole, uno stesso soggetto potrebbe agire **contemporaneamente** come **titolare del trattamento** per determinate operazioni di trattamento e come **responsabile del trattamento** per altre – come avviene nel caso di ASPI e FtX.

Pertanto, ai fini di una corretta qualificazione dei ruoli privacy, nonché dei correlati adempimenti, i titolari del trattamento dovranno, a titolo esemplificativo e non esaustivo:

- effettuare una valutazione in relazione a un insieme specifico di dati o di operazioni e la natura del servizio al fine di determinare se l'attività di trattamento abbia per oggetto il trattamento di dati personali per conto del titolare;
- avvalersi di responsabili del trattamento che presentino garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate (ad esempio, sussistenza di conoscenze specialistiche, competenze tecniche in materia di misure di sicurezza e di violazione dei dati, verifica del loro grado di affidabilità e delle risorse di cui dispongono, nonché della loro adesione a un codice di condotta o a un meccanismo di certificazione riconosciuti);
- disciplinare il rapporto tra titolare e responsabile del trattamento mediante la stipula di un contratto o di un atto giuridico di altra natura, redatto per iscritto, anche in formato elettronico, con carattere di vincolatività. Il titolare e il responsabile del trattamento possono negoziare un contratto specifico, comprensivo di tutti gli elementi obbligatori, oppure basarsi, in tutto o in parte, su clausole contrattuali tipo. Il GDPR elenca gli elementi che devono figurare nell'accordo di trattamento, il quale tuttavia non dovrebbe limitarsi a ribadire le disposizioni del GDPR, ma dovrebbe disciplinare in modo più specifico e concreto come saranno soddisfatti i requisiti applicabili e quale sia il livello di sicurezza richiesto per il trattamento dei dati personali oggetto dell'accordo stesso;
- fornire agli interessati informative che contengano tutte le informazioni previste dall'art. 13 del GDPR.

* * *

Fidelity card: come trattare i dati personali raccolti per finalità di marketing e profilazione

Nella newsletter dello scorso 28 giugno, il Garante per la protezione dei dati personali (il

"**Garante**" o l'"**Autorità**"), ha reso noto il provvedimento con cui ha sanzionato una nota società tessile italiana (la "**Società**") con una multa pari a **240 mila euro**, per aver trattato per finalità di marketing e profilazione un'ampia quantità di dati personali di propri clienti ed ex clienti, in maniera illecita, in assenza di adeguate misure di sicurezza, nonché senza determinare un periodo di conservazione. La Società, nello specifico, aveva raccolto i dati dei clienti tramite l'iscrizione al servizio di *e-commerce*, ai programmi fedeltà e alle newsletter promozionali.

Prima di procedere con un'analisi del provvedimento del Garante, è utile chiarire cosa si intende per programmi fedeltà.

Programma fedeltà

I programmi di fidelizzazione sono strategie di *marketing* adottate dalle società per incoraggiare i clienti esistenti a mantenere un rapporto di lungo termine e a continuare ad effettuare acquisti. Questi programmi premiano la fedeltà dei clienti offrendo loro incentivi, vantaggi particolari, sconti o ricompense in base al loro comportamento di acquisto o all'interazione con la società.

Solitamente, un programma di fidelizzazione richiede la registrazione dei clienti presso la società o l'adesione a un programma specifico tramite l'utilizzo di una carta fedeltà o un account *online*. Attraverso il programma, i clienti possono accumulare punti, sconti, buoni regalo o altri premi in base alla frequenza degli acquisti, all'ammontare delle spese o ad altri comportamenti desiderati dall'azienda.

I programmi di fidelizzazione sono ampiamente utilizzati in vari settori, tra cui la vendita al dettaglio, la ristorazione, le compagnie aeree, gli hotel, i servizi finanziari e altro ancora. Oltre a incentivare la fedeltà dei clienti, questi programmi consentono alle società di raccogliere dati sul comportamento di acquisto e le preferenze dei clienti, consentendo loro di personalizzare le offerte e migliorare le strategie di *marketing*.

Tuttavia, poiché i programmi fedeltà comportano il trattamento dei dati personali dei clienti, le società nell'implementazione di tali programmi devono tenere in considerazione la normativa in materia di protezione dei dati personali.

Inoltre, è importante che i programmi di fidelizzazione siano trasparenti, fornendo informazioni chiare sui termini e le condizioni, inclusi i criteri per accumulare e utilizzare i premi, nonché le opzioni per l'accesso, la modifica o la cancellazione dei dati personali dei clienti.

Complessivamente, i programmi di fidelizzazione possono essere vantaggiosi sia per le società che per i clienti, creando un rapporto di fiducia e reciproco beneficio. Tuttavia, bisogna adottarli nel rispetto della normativa vigente, anche al fine di evitare di incorrere in sanzioni come è avvenuto, recentemente, alla Società sanzionata dal Garante.

Il provvedimento del Garante nei confronti della Società

Il Garante ha emesso un provvedimento nei confronti della Società comminando una sanzione pari a 240 mila euro, accertando il **trattamento illecito di un'ampia quantità di dati personali** di clienti ed ex clienti, in violazione del Regolamento UE 679/2016 ("**GDPR**"). Tra le violazioni più gravi, l'Autorità ha rilevato **l'assenza di adeguate** misure di sicurezza, in violazione dell'art. 32, par. 1, lett. b) del GDPR e la conservazione, **senza limiti temporali**, di dati personali a fini di *marketing* e profilazione, in violazione del principio di limitazione della conservazione previsto dall'art. 5, par. 1, lett. e) del GDPR.

Un'ispezione condotta dall'Autorità ha, infatti, evidenziato che la Società conservava i dati raccolti tramite le carte fedeltà, compresi i dettagli sugli acquisti effettuati dal 2015, i dettagli degli scontrini e i punti accumulati, anche degli ex clienti.

Tale mole di informazioni risultava per la Società estremamente preziosa e appetibile per le attività di *marketing* e di profilazione – pratiche ai giorni nostri sempre più diffuse e utilizzate.

Inoltre, le verifiche effettuate hanno rivelato che il database gestionale della Società, contenente i dati dei clienti, era accessibile a **tutti** i dipendenti dei negozi del gruppo aziendale presenti in **7 paesi europei**, da qualsiasi dispositivo connesso a Internet, utilizzando un'unica password e un singolo account.

Il Garante, in questo caso, evidenziava, *inter alia*, la mancanza di limitazioni particolari per i dipendenti e, quindi, la possibilità per gli stessi di effettuare addirittura *screenshot* o operazioni analoghe, la possibilità di accedere alla piattaforma da qualunque dispositivo, anche senza aver effettuato il login al sistema di cassa e l'assenza dell'obbligo di cambiare password al momento della creazione di un nuovo account.

Considerando il numero elevato di interessati coinvolti e la durata considerevole delle violazioni, il Garante ha deciso di sanzionare la Società e le ha imposto l'obbligo di adottare idonee misure tecniche e organizzative finalizzate ad assicurare che la gestione dei dati personali dei clienti, da parte del personale degli store della Società, avvenga nel rispetto della normativa in materia di protezione dei dati personali e, in particolare, dell'art. 32, par. 1, lett. b) e d) e par. 2 del GDPR.

L'Autorità inoltre ha ingiunto alla Società di:

- cancellare o anonimizzare i dati personali degli ex clienti che risalgono a oltre 10 anni fa, salvo in caso di controversie giudiziali o stragiudiziali in corso;
- adottare idonee soluzioni organizzative e tecniche finalizzate ad assicurare che la conservazione dei dati dei clienti e degli ex clienti avvenga nel rispetto dei principi di cui all'art. 5 del GDPR e, in particolare, nel rispetto dei principi di limitazione della finalità, minimizzazione dei dati e limitazione della conservazione.

In relazione alla durata decennale della conservazione dei dati, il Garante ha altresì richiamato il provvedimento generale del 24 febbraio 2005, "Fidelity card" e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione, evidenziando che tale periodo di conservazione risulta "palesemente" eccessivo rispetto alla misura di **12 mesi/24 mesi** indicata, in relazione alle finalità di marketing e profilazione, dall'Autorità stessa.

Sul punto, il Garante, infatti, aveva prescritto ai titolari del trattamento l'identificazione di termini massimi di conservazione dei dati da osservare presso banche dati sia centrali, sia locali e tale identificazione deve essere effettuata dopo aver esaminato la possibilità di raccogliere e conservare dati nei termini consentiti per ciascuna delle finalità, tenendo conto di eventuali scelte degli interessati sopravvenute.

In *primis*, il principio da osservare risulta essere quello secondo cui i dati personali dei quali **non è necessaria la conservazione** in relazione agli scopi per i quali sono stati trattati devono essere **cancellati o anonimizzati** e, in ogni caso, i dati relativi al dettaglio degli acquisti con riferimento a clienti individuabili possono essere conservati per finalità di marketing o di profilazione per un periodo **non superiore**, rispettivamente, a **12 e a 24 mesi** dalla loro registrazione, salvo che l'anonimizzazione non permetta, anche

indirettamente o collegando altre banche di dati, di identificare gli interessati.

Nel caso di eventuale ritiro, disabilitazione per mancato utilizzo entro un determinato arco temporale, scadenza o restituzione delle *fidelity card,* il titolare del trattamento può individuare un termine di conservazione dei dati personali per esclusive finalità amministrative e, quindi, non anche per finalità di *marketing* o di profilazione, non superiore ad un trimestre, salvo eventuali specifici obblighi di legge sulla conservazione di documentazione contabile. Il Garante ha altresì evidenziato l'obbligo di indicare tali informazioni nell'informativa che viene fornita agli interessati e l'obbligo di predisporre idonei meccanismi di cancellazione automatica dei dati anche da parte di terzi cui gli stessi siano stati eventualmente comunicati.

Un altro aspetto emerso durante l'attività ispettiva del Garante, il quale è stato archiviato grazie al tempestivo intervento correttivo apportato dalla Società durante il procedimento, è stato quello relativo alla gestione dei cookie. In particolare, l'Autorità aveva evidenziato diverse criticità, tra cui:

- un banner informativo relativo all'utilizzo di cookie, propri e di terze parti, con impossibilità di deselezionare le tipologie di cookie;
- la mancata menzione, nell'informativa estesa, dei cookie di profilazione utilizzati, diversamente dall'informativa breve;
- il rimando, nel banner dei cookie, ad una pagina bianca e non all'informativa estesa;
- l'assenza di informativa estesa;
- l'assenza di *form* di manifestazione di volontà per l'utilizzo dei cookie.

Sul punto, si rammenta che i cookie devono essere gestiti in conformità della normativa in materia di protezione dei dati personali. In relazione ad essi, risulta utile analizzare anche le Linee guida cookie e altri strumenti di tracciamento del 10 giugno 2021 adottate dal Garante.

Conclusioni

Questo provvedimento sanzionatorio rappresenta un importante richiamo per le società poiché sottolinea, ancora una volta, l'estrema importanza di gestire i dati personali nel rispetto della normativa in materia di protezione dei dati personali, nonché l'obbligo di adottare adeguate misure di sicurezza tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio in modo da assicurare, *inter alia*, su base permanente la riservatezza dei dati. Le violazioni della normativa in materia di protezione dei dati possono, infatti, comportare **sanzioni significative e arrecare danni alla reputazione aziendale**. Pertanto, è fondamentale che le organizzazioni considerino la protezione dei dati personali come una priorità e implementino politiche e procedure complete per garantire la privacy e la sicurezza dei dati personali degli interessati.

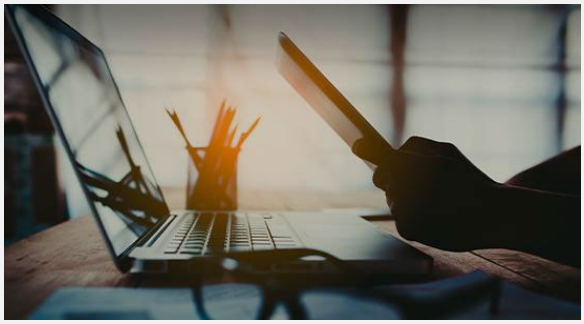
Alcuni aspetti da non dimenticare sono:

- determinare le finalità per cui vengono raccolti e trattati i dati personali;
- raccogliere e trattare i dati personali in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati i dati stessi;
- determinare un periodo di conservazione dei dati personali che non sia eccessivo rispetto alle finalità per le quali sono trattati i dati stessi, tenendo altresì in considerazione i provvedimenti e le indicazioni del Garante, nonché dell'*European Data Protection Board* ("**EDPB**"), ove presenti;

- predisporre idonee informative da fornire agli interessati che contengano tutte le informazioni previste dalla normativa in materia di protezione dei dati personali;
- adottare misure tecniche e organizzative adeguare per garantire un livello di sicurezza adeguato al rischio e aggiornarle, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

* * *

L'AgCOM adotta le Linee Guida concernenti i meccanismi di reclamo da parte degli utenti



Lo scorso 18 maggio, l'Autorità per le garanzie nelle comunicazioni ("**AgCOM**" o "**Autorità**") ha emanato, con la delibera n. 115/23/CONS, le "*Linee guida concernenti i meccanismi di reclamo predisposti dai prestatori di servizi di condivisione di contenuti online e regolamento concernente la risoluzione delle controversie tra prestatore di servizi di condivisione di contenuti online e utenti, in attuazione dell'articolo 102-decies della legge 22 aprile 1941, n. 633*" (le "**Linee Guida**") con le quali l'Autorità ha stabilito l'obbligo per i prestatori di servizi di condivisione di contenuti online di mettere a disposizione degli utenti [1] mezzi di reclamo celeri ed efficaci contro la rimozione o la disabilitazione di contenuti per violazione del diritto d'autore.
Lo schema delle Linee Guida era stato sottoposto a consultazione pubblica con la delibera n. 276/22/CONS del 19 luglio 2022 e, pertanto, nella sua adozione ha tenuto in considerazione le osservazioni e le valutazioni emerse nel corso delle audizioni con tutti i soggetti interessati.

La delibera dà esecuzione all'art. 102-decies della l. n. 633/1941[2] (c.d. legge sul diritto d'autore, di seguito, in breve, "**LdA**") e fornisce efficaci strumenti di tutela contro le decisioni delle piattaforme che, se non attentamente ponderate, possono pregiudicare la libertà di espressione degli utenti.

Le previsioni contenute nelle Linee Guida, infatti, mirano ad evitare che le piattaforme accolgano indiscriminatamente tutte le richieste di disabilitazione e rimozione, al solo fine di non incorrere in eventuali responsabilità nei confronti dei titolari dei diritti, con il rischio di andare a ledere la creatività dei *content creator*.

Prima di procedere con una disamina delle Linee Guida, giova ricordare che l'art. 102-septies della LdA prevede espressamente che i prestatori di servizi di condivisione di contenuti online (i "**Prestatori**"), considerato che quando concedono l'accesso al pubblico a opere[3] o altri materiali protetti dal diritto d'autore compiono un atto di comunicazione o messa a disposizione del pubblico di tali contenuti, devono

[1] Ai sensi dell'art. 1, par. 1, lett. i) delle Linee Guida per utente si intende ogni persona fisica o giuridica che carica opere o materiali a mezzo di un servizio della società dell'informazione così come definito dall'art. 102-*sexies* della LdA o un nuovo servizio della società dell'informazione.
[2] Gli artt. da 102-*sexies* a 102-*decies* della LdA, che dettano specifiche previsioni applicabili ai prestatori di servizi di condivisione di contenuti online, sono stati introdotti con il D.Lgs. n. 177/2021, il quale recepisce l'art. 17 della Direttiva UE n. 2019/790 (c.d. Direttiva Copyright).
3 Ai sensi dell'art. 1, par. 1, lett. d) delle Linee Guida per opera si intende qualsiasi opera, o parti di essa, di carattere sonoro, audiovisivo, fotografico, videoludico, editoriale e letterario, inclusi i programmi applicativi e i sistemi operativi per elaboratore, tutelata dalla LdA e diffusa su reti di comunicazione elettronica.

necessariamente acquisire una preventiva autorizzazione da parte dei titolari dei diritti delle opere dell'ingegno che gli utenti caricano sulla piattaforma, anche mediante la conclusione di un accordo di licenza. In assenza di tale preventiva autorizzazione, i Prestatori commetterebbero una violazione del diritto di comunicazione al pubblico.

In relazione, invece, all'art. 102-decies della LdA, la disposizione prevede che i Prestatori debbano istituire e rendere disponibili agli utenti di tali servizi dei meccanismi di reclamo **celeri** ed **efficaci**, nel caso in cui a specifiche opere o altri materiali caricati dagli stessi venga disabilitato l'accesso o vengano rimossi, a seguito di una decisione da parte del Prestatore stesso.

La disposizione, al comma 1, stabilisce che i titolari dei diritti possano chiedere al Prestatore di disabilitare l'accesso a loro specifiche opere o ad altri materiali o di rimuoverli, indicandone i motivi della richiesta.

Le Linee Guida

Le Linee Guida specificano gli elementi necessari affinché i meccanismi di reclamo rispondano ai requisiti di efficacia e celerità previsti dall'art. 102-*decies* della LdA. In particolare, il documento dell'AgCOM contiene una guida funzionale per l'implementazione del meccanismo di reclamo, nonché le modalità tecniche operative che i Prestatori possono seguire al fine di uniformarsi a quanto previsto dal legislatore europeo e nazionale.

L'AgCOM, tuttavia, specifica che quanto illustrato nelle Linee Guida ha valenza di **principio generale** e che i Prestatori possono continuare a utilizzare i sistemi di reclamo **già adottati** e/o **svilupparne di nuovi** in futuro, purché questi garantiscano i requisiti di celerità ed efficacia nell'intero processo di contestazione della decisione di disabilitazione dell'accesso o di rimozione di specifiche opere o di altri materiali caricati dagli utenti.

In concreto, le Linee Guida specificano che:

- gli utenti hanno il **diritto di contestare**, tramite reclamo, la decisione di disabilitazione dell'accesso o rimozione di contenuti assunta dal Prestatore;
- il Prestatore **non può limitare** la possibilità dell'utente di esercitare il proprio diritto di reclamo e il reclamo deve essere gratuito;
- i termini per esercitare il diritto di reclamo eventualmente stabiliti dai Prestatori devono essere **proporzionati** per non pregiudicarne l'efficacia e devono essere espressamente previsti nelle condizioni generali di fornitura del servizio o in altre parti, purché ne sia garantita la **visibilità** e la **comprensibilità**;
- il meccanismo e, in ogni caso, le informazioni relative all'esercizio del diritto di reclamo devono essere rese disponibili in **lingua italiana**;
- il Prestatore deve predisporre un meccanismo in modo che la relativa procedura possa essere gestita dall'utente mediante il suo ***account*** o tramite indirizzo ***e-mail*** associato all'*account*.

La procedura di reclamo

La procedura di reclamo prevede che l'utente mediante istanza – redatta dallo stesso o da un rappresentante munito di procura speciale – fornisca le proprie generalità e i propri recapiti. L'utente può inoltre allegare idonea documentazione ed esporre i motivi per cui ritiene legittimo il caricamento dei contenuti oggetto di contestazione, e quindi infondata la disabilitazione all'accesso o la rimozione agli stessi.

Il Prestatore alla trattazione dell'istanza di reclamo ricevuta dall'utente:

- non riabilita i contenuti che devono, invece, rimanere disabilitati;
- se ritiene che il reclamo non sia irricevibile, informa tempestivamente il soggetto legittimato, inoltrando altresì l'istanza ricevuta. Il soggetto legittimato può confermare i motivi della sua richiesta di disabilitazione o rimozione, giustificando la natura lesiva, entro 7 giorni dalla ricezione della comunicazione da parte del Prestatore o può non riscontrare lo stesso. In quest'ultimo caso, il Prestatore decide senza il coinvolgimento del soggetto legittimato sulla possibilità o meno di riabilitare i contenuti. Nel caso in cui, invece, il soggetto legittimato riscontri il Prestatore, quest'ultimo deve assumere una decisione mediante una verifica da parte di un soggetto umano in relazione al contenuto oggetto del reclamo.

In caso di complessità, il Prestatore può chiedere ulteriori informazioni e il termine è prorogato di altri 7 giorni.

La decisione del Prestatore

Il Prestatore, per garantire l'efficacia del meccanismo, deve comunicare la decisione all'utente **immediatamente** o, in ogni caso, **entro 24 ore** dall'adozione della stessa e la comunicazione deve avere un contenuto minimo (ad es. l'oggetto della decisione, le ragioni per cui ha agito specificando le motivazioni addotte dai titolari dei diritti o da altri soggetti legittimati, la loro identità e – previa autorizzazione – i loro contatti, nonché i termini e le modalità per effettuare il reclamo).

Il Prestatore deve decidere entro un termine proporzionato al fine di garantire l'efficacia del meccanismo di reclamo e, in ogni caso, **non oltre 20 giorni** dal ricevimento dell'istanza da parte dell'utente. Il termine è diverso per i nuovi Prestatori, i quali possono decidere **entro 30 giorni** dal ricevimento dell'istanza.

Inoltre, la decisione deve contenere un avviso per l'utente che espliciti il suo diritto di impugnare la decisione sul reclamo davanti all'AgCOM, il quale deciderà sulla fondatezza della decisione presa dal Prestatore.

Nel caso in cui il reclamo venga accolto, il Prestatore ha l'obbligo di riabilitare **tempestivamente** i contenuti disabilitati.

A chi si applica

L'art. 102-sexies stabilisce che per Prestatore si intendono i prestatori di servizi della società dell'informazione che:

- hanno come scopo principale, o tra i principali scopi, di memorizzare e dare accesso al pubblico a grandi quantità di opere o di altri materiali protetti dal diritto d'autore;
- condividono opere o altri materiali protetti caricati dagli utenti; e
- organizzano e promuovono le opere o gli altri materiali protetti per trarne profitto, direttamente o indirettamente.

Non rientrano invece in tale categoria, i prestatori che, a titolo esemplificativo e non esaustivo, danno accesso alle enciclopedie online senza scopo di lucro (ad es. Wikipedia), a repertori didattici o scientifici senza scopo di lucro, nonché le piattaforme di sviluppo e di condivisione di *software open source* (ad es. Linux), i fornitori di servizi di comunicazione elettronica, i prestatori di mercati online.

Cosa devono fare i Prestatori

Oltre ad adeguare e/o implementare, ove necessario, i meccanismi di reclamo conformemente alle Linee Guida, l'AgCOM prevede altresì che i Prestatori, entro 180 giorni dall'entrata in vigore delle Linee Guida, debbano inviare all'Autorità stessa una comunicazione contenete i meccanismi di reclamo adottati.

I Prestatori, inoltre, a metà e alla fine di ogni anno, devono inviare all'AgCOM un *report* che indichi il numero di contenuti disabilitati o rimossi e il numero di reclami presentati.

Ad ogni modo, si rammenta che questo non è il primo provvedimento che l'AgCOM ha adottato a seguito del recepimento della Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio dell'UE da parte del legislatore italiano.

Infatti, già lo scorso 19 gennaio, l'Autorità aveva approvato, con un solo voto contrario, il regolamento in materia di determinazione dell'equo compenso per l'utilizzo online delle pubblicazioni di carattere giornalistico, in attuazione dell'art. 43-bis della LdA, di cui alla delibera n. 3/23/CONS (ne abbiamo parlato nel nostro Osservatorio qui).

* * *

Per maggiori informazioni, potete contattare:

Carlo Impalà
Partner e Responsabile Dip. TMT e Data Protection
(Carlo.Impala@MorriRossetti.it)

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it