



OSSERVATORIO
TMT·DATA PROTECTION

di Morri Rossetti

Monthly Roundup

Aprile 2022

MONTHLY ROUNDUP

Aprile 2022

I principali aggiornamenti in materia di TMT & Data Protection del mese di Aprile 2022

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

- **EDPB**

Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework [\[Link\]](#)

- **Garante Privacy**

- Riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani [\[Link\]](#)
 - Parere del Garante privacy sullo schema di decreto che disciplina i referendum online [\[Link\]](#)
-

PRINCIPALI AGGIORNAMENTI



Digital Services Act

The political agreement reached between the European Parliament and the Council of the European Union

On the 23 of April 2022, the European Parliament and the Council of the European Union has announced the political agreement reached on the Digital Services Act proposal.

On this regard, the President of the European Commission, Ursula von der Leyen, declared, among others, that the DSA "will upgrade the ground-rules for all online services in the EU. It will ensure that the online environment remains a safe space, safeguarding freedom of expression and opportunities for digital businesses. It gives practical effect to the principle that what is illegal offline, should be illegal online. The greater the size, the greater the responsibilities of online platforms".

The DSA and its provisions

The DSA is one of the two legislative initiatives proposed by the Commission on the 15 of December 2020, aimed at strengthening the rules provided for digital services – that include a large category of online services, such as websites, online platforms and internet infrastructure – and increasing the protection

of internet users. The DSA will apply to all online intermediaries providing services in the EU.

In January 2022, the European Parliament has approved an amended text of the DSA, which contains a new set of rules that would be applicable across the whole EU in order to create a safer digital space in which the fundamental rights of all users of digital services are protected and, specifically, set out a new standard for the accountability of online platforms regarding illegal and harmful content.

As mentioned by the President of the European Commission, the text of the DSA pays attention to the Big Tech, subjecting them to further specific obligations due to the particular risks which they could pose in the dissemination of illegal and harmful content online. Specifically, very large platforms shall, for example, take risk-based action in order to prevent the misuse of their systems and shall undergo independent audits of their risk management systems.

Beyond them, the DSA considers also others online intermediary services, such as but not limited to the very large online search engines with more than 10% of the 450 million consumers in the EU, internet access providers, online marketplaces and so on. Considering this, according to the DSA provisions, the obligations of online intermediary services depend on their role, size, and impact on the online ecosystem.

At this stage, as reported in the European Commission press release, the DSA contains, *inter alia*:

- measures to counter illegal goods, services or content online, such as:

- a mechanism for users to easily flag such content and for platforms to cooperate with so-called “trusted flaggers”;
- new obligations on traceability of business users in online market places, to help identify sellers of illegal goods or reasonable efforts by online market places to randomly check whether products or services have been identified as being illegal in any official database and, then, the obligation to remove the illegal product or service from its interface expeditiously and, where appropriate, inform the relevant authorities, such as the market surveillance authority or the custom authority of the decision taken;
- new measures to empower users and civil society such as:
- the possibility to easily and effectively challenge platforms' content moderation decisions and seek redress, either via an out-of-court dispute mechanism or judicial redress in accordance with the laws of the Member State concerned;
- provision of access to vetted researchers to the key data of the largest platforms and provision of access to NGOs as regards access to public data, to provide more insight into how online risks evolve;
- transparency measures for online platforms on a variety of issues, including on the algorithms used for recommending content or products to users;

- measures to assess and mitigate risks, such as:
- obligations for very large platforms and very large online search engines to take risk-based action to prevent the misuse of their systems such as the obligation to conduct, where appropriate, a risk assessment and to design risk mitigation measures with the involvement of representatives of the users, independent experts and civil society organizations, and undergo independent audits of their risk management systems;
- mechanisms to adapt swiftly and efficiently in reaction to crisis affecting public security or public health; very large online platforms should ensure public access to repositories of advertisements displayed on their online interfaces to facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality;
- new safeguards for the protection of minors such as the prohibition of using a minor's personal data for commercial purposes related to direct marketing, profiling and behaviorally targeted advertising, and limits or bans on the use of sensitive personal data (such as ethnicity, political views, sexual orientation) for targeted advertising.

Moreover, in order to ensure the supervision and enforcement of requirements under the DSA, the European Parliament and the Council

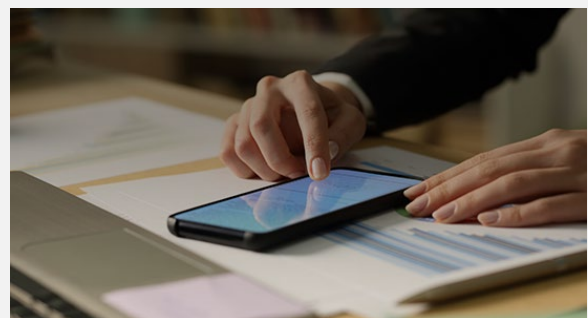
of the European Union have decided to confer on the EU Commission the exclusive power to supervise very large online platforms and very large online search engines for the obligations provided to them.

However, in order to maintain the country-of-origin principle, which will continue to apply to other actors and requirements covered by the DSA, the above mentioned two types of online intermediary services shall be supervised in cooperation with the Member States.

And now?

After the achievement of this political agreement, the text is now subject to formal approval by the European Parliament and the Council of the European Union. Once the DSA will be formally adopted by the EU co-legislators, the legislative text will be published in the Official Journal of the European Union and shall enter into force twenty days after its publication.

* * *



Contratti a distanza conclusi con mezzi elettronici: quando il point and click vincola il consumatore?

L'interpretazione della Corte di Giustizia europea

La Direttiva 2011/83/UE del Parlamento europeo e del Consiglio dell'Unione europea, adottata nell'ottobre del 2011, disciplina i diritti

dei consumatori nell'ambito dei contratti a distanza, stabilendo una serie di diritti contrattuali a favore degli stessi, nonché diversi obblighi informativi e relative sanzioni, in caso di mancata osservanza, in capo al professionista (la "**Direttiva**").

L'ambito di applicazione della Direttiva si estende a tutti i rapporti business to consumer ("B2C"), ove si è in presenza di un professionista, da un lato, e di un consumatore, dall'altro. Lo scopo della Direttiva è quello di semplificare, aggiornare e uniformare le regole applicabili alla tipologia dei contratti a distanza e di quelli negoziati fuori dai locali commerciali, ivi inclusi i contratti a distanza conclusi attraverso modalità telematiche.

La controversia

In data 7 aprile 2022, la Corte di Giustizia dell'Unione europea ("**CGUE**" o "**Corte**") si è pronunciata nella causa Fuhrmann-2-GmbH contro B. (C-249/21) (la "**Pronuncia**"), a seguito di una domanda di rinvio pregiudiziale, in merito all'interpretazione dell'art. 8, par. 2, secondo comma, della Direttiva, ove il Tribunale di Bottrop, Germania, chiedeva, in sostanza, se, nell'ambito di un processo di inoltro di un ordine relativo alla conclusione di un contratto a distanza con mezzi elettronici, la formulazione presente sul pulsante di inoltro "*conferma la prenotazione*" corrispondesse alla dicitura "*ordine con obbligo di pagare*" prevista dalla normativa in esame e se, ai fini di tale verifica, occorre basarsi soltanto sulla dicitura riportata sul pulsante o era possibile prendere in considerazione le altre circostanze che accompagnavano il processo di inoltro dell'ordine.

In particolare, la controversia vedeva coinvolte una società di diritto tedesco proprietaria di una struttura alberghiera (la "**Società**"), la quale si appoggiava, per la locazione delle camere dell'hotel, anche a una piattaforma di

prenotazione di alloggi online (i.e. Booking.com), e un consumatore tedesco il quale, interessato ad alcune camere del suddetto hotel, decideva di sfruttare la piattaforma di intermediazione e prenotava le stanze cliccando sul tasto "*prenoto*" e, successivamente, sul pulsante recante la dicitura "*completa la prenotazione*".

La questione giungeva al Tribunale tedesco a seguito del mancato saldo da parte del consumatore delle spese di cancellazione: il consumatore non si era presentato nelle date prenotate e la Società aveva addebitato allo stesso le suddette spese.

La Società aveva, infatti, deciso di procedere per il recupero giudiziale della somma dal momento che riteneva la dicitura "*conferma la prenotazione*", inserita dal gestore del sito Internet di intermediazione, sufficiente a far riconoscere espressamente al consumatore che l'ordine implicava l'obbligo di pagamento.

Nella Pronuncia, la Corte richiama la normativa in esame, sottolineando che, in un contratto a distanza concluso con mezzi elettronici, il professionista deve garantire che, al momento di inoltrare l'ordine, il consumatore riconosca espressamente l'obbligo di pagare derivante dall'inoltro e che, qualora l'inoltro dell'ordine venga azionato dall'attivazione di un pulsante o di una funzione analoga, tale pulsante o funzione devono riportare in modo facilmente leggibile le parole "*ordine con obbligo di pagare*" o una formulazione corrispondente inequivocabile indicante che il fatto di inoltrare l'ordine implichi l'obbligo, per il consumatore, di pagare il professionista.

Nel caso di specie, la CGUE ha, pertanto, censurato l'operato della Società, constatando che la sua condotta potrebbe essere in contrasto con la normativa che disciplina i diritti dei consumatori e specificando che

spetta al giudice del rinvio verificare se, nel procedimento principale, la formulazione utilizzata possa essere considerata corrispondente alla dicitura "*ordine con obbligo di pagare*" o a qualsiasi altra formulazione inequivocabilmente corrispondente.

Invero, come già riportato nell'interrogativo del giudice tedesco, il termine "*prenotazione*", contenuto nel pulsante che aziona l'ordine con obbligo di pagamento, non viene necessariamente associato, nel linguaggio corrente, all'obbligo di pagare un corrispettivo, ma viene spesso utilizzato anche come sinonimo di "*riservare o ordinare preventivamente a titolo gratuito*".

La Corte, inoltre, precisa anche che debba essere il pulsante o la funzione analoga a contenere la dicitura "*ordine con obbligo di pagare*" o a qualsiasi altra formulazione inequivocabilmente corrispondente, mentre non sono considerati equiparabili riferimenti all'obbligo di pagamento nel modulo dell'ordine o in altri punti della sito web stesso.

Infine, nella Pronuncia si legge, il rispetto di tale obbligo informativo non inficia la libertà di impresa dell'imprenditore, atteso che "*la redazione o la modificazione di una dicitura presente su un pulsante o su una funzione di inoltro elettronica di un ordine non implica alcun onere significativo tale da nuocere alla competitività o alla libertà di impresa dei professionisti interessati*".

La disciplina italiana

Seppur la domanda di pronuncia pregiudiziale sia stata presentata nell'ambito di una controversia tra una società di diritto tedesco e un consumatore tedesco, occorre tenere presente che il rinvio pregiudiziale alla CGUE, ex art. 267 del Trattato sul funzionamento dell'Unione europea, viene provocato da un'ordinanza del giudice nazionale, con la

quale lo stesso solleva una questione interpretativa su una norma europea e la sentenza della Corte - giuridicamente vincolante - è da ritenersi l'interpretazione ufficiale in merito alla questione e come tale produce effetto in tutti gli Stati membri - ivi compresa l'Italia - e le relative autorità di controllo.

Ma procediamo per gradi.

Sul piano nazionale, il contratto, indipendentemente dal mezzo tecnico utilizzato, si ritiene concluso quando il proponente viene a conoscenza dell'accettazione dell'altra parte, ex art. 1326 c.c.. La proposta e l'accettazione nell'ambito dei contratti digitali possono essere portati a conoscenza del destinatario e, quindi, il contratto può ritenersi perfezionato, tramite lo scambio di e-mail oppure tramite la pressione del c.d. tasto negoziale virtuale (*point and click*).

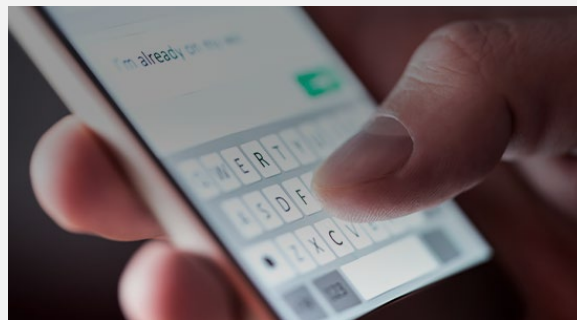
In particolare, l'art. 8, par. 2, secondo comma, della Direttiva è stato recepito in maniera letterale dall'art. 51, secondo comma, del D.lgs. n. 206/2005 (il "**Codice del Consumo**") il quale è dedicato ai requisiti formali per i contratti a distanza e, in generale, rientra fra le norme che disciplinano la tutela del consumatore in ambito digitale. L'articolo in esame specifica che, nell'ambito di un contratto a distanza concluso con mezzi elettronici che impone al consumatore l'obbligo di pagare, il professionista deve non solo comunicare in modo chiaro ed evidente alcune specifiche informazioni, ma anche garantire che il consumatore, al momento di inoltrare l'ordine, riconosca espressamente che tale inoltro implichi l'obbligo di pagare. Inoltre, specifica la norma, qualora il professionista non osservi tali obblighi, il consumatore non sarà vincolato dal contratto o dall'ordine.

Le possibili implicazioni della Pronuncia

L'interpretazione restrittiva della Corte in merito a quanto previsto dalla normativa potrebbe avere delle ripercussioni anche sui siti *e-commerce* nazionali. Invero, qualora tali piattaforme B2C, nella creazione dei pulsanti di accettazione online per l'inoltro di ordini e l'accettazione contrattuale, non riportino in modo facilmente leggibile le parole "ordine con obbligo di pagare" o una formulazione corrispondente inequivocabile indicante che l'inoltro dell'ordine implica l'obbligo di pagare il professionista, potrebbero vedersi, in sede giudiziale, non riconosciuto come vincolante il contratto stipulato a seguito del *point and click* e dunque, in caso di mancato pagamento da parte dei consumatori, essere impossibilitati ad impugnare il pagamento.

In conclusione, occorre ora chiedersi se la dicitura inserita sul pulsante – o la funzione analoga – ai fini dell'accettazione contrattuale possa essere associata al sorgere di un obbligo di pagare *"tanto nel linguaggio corrente quanto nella mente del consumatore medio, normalmente informato e ragionevolmente attento e avveduto"*. In caso negativo, si evidenzia, la dicitura non sarebbe inequivocabile e quindi non rispetterebbe il requisito di legge ripercuotendosi, potenzialmente, sull'esistenza del vincolo contrattuale tra il professionista e il consumatore.

* * *



Illegittimo l'invio di SMS commerciali in assenza di consenso dell'interessato. La Cassazione accoglie il ricorso del Garante Privacy

Lo scorso 28 marzo, la Corte Suprema di Cassazione ha depositato **l'ordinanza n. 9920, emessa il 16 febbraio 2022**, con la quale si è pronunciata in merito alle attività promozionali e pubblicitarie, mediante l'invio di sms, effettuate da una società (la "Società") al fine di acquisire il consenso al trattamento di dati personali per finalità di marketing da parte di destinatari che già in precedenza non lo avevano prestato o lo avevano deliberatamente ritirato.

Il caso

La vicenda ha avuto inizio con il **provvedimento n. 437, emesso dall'Autorità Garante per la protezione dei dati personali in data 27 ottobre 2016** a seguito di svariate segnalazioni provenienti da soggetti privati. In particolare, i reclamanti, clienti della Società, lamentavano la ricezione di sms indesiderati, aventi contenuto promozionale, inviati dalla Società stessa, senza che questi avessero prestato consenso esplicito a tale trattamento. A seguito delle segnalazioni ricevute, il Garante Privacy decideva di effettuare accertamenti in loco presso la Società e, nel corso delle verifiche, constatava che suddetto tipo di attività di marketing aveva interessato sia clienti di nuova acquisizione, sia clientela già presente nella *customer base* della Società.

La Società impugnava, quindi, il provvedimento del Garante Privacy davanti al Tribunale di Roma, il quale ne accoglieva le doglianze, ritenendo la fattispecie di invio di comunicazioni dirette ad acquisire il consenso **esclusa dalle attività pubblicitarie o promozionali** rientranti nell'art. 130, comma 1, del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018 ("**Codice Privacy**").

Di conseguenza, la sentenza del Tribunale di Roma veniva impugnata per Cassazione dal Garante Privacy, il quale, a sua volta, contestava che l'invio di sms a utenti o contraenti, i cui dati personali erano stati trattati in assenza di consenso ab origine, al fine di acquisirne il consenso per svolgere attività di marketing, integrasse certamente un'attività illegittima.

La decisione della Corte di Cassazione

La Corte di Cassazione ha ritenuto fondato il motivo del Garante Privacy e ha precisato, in linea con l'orientamento dell'Autorità, che l'art. 130 del Codice Privacy, che disciplina le comunicazioni indesiderate tramite l'uso di sistemi automatizzati senza l'intervento di un operatore, prevede che il consenso debba essere richiesto non soltanto per l'invio di materiale o per la vendita diretta, ma anche per il semplice invio di generiche comunicazioni commerciali.

Gli ermellini hanno, pertanto, precisato che, nel caso di specie, si fosse già in presenza di una comunicazione commerciale, dal momento che il consenso veniva richiesto per successive attività commerciali o promozionali ma il fine perseguito era il medesimo (in quanto la comunicazione si intende connessa e finalizzata all'invio di comunicazioni commerciali). La Corte si è poi soffermata sull'art. 130, comma 2, del Codice Privacy, chiarendo che la disposizione in esame si applica anche tramite l'invio, *inter alia*, di messaggi sms.

La Corte ha altresì ribadito che, già in passato, si era giunti alla medesima conclusione in relazione a comunicazioni telefoniche volte a ottenere il consenso a fini di marketing da parte di soggetti che lo avevano già precedentemente negato o non lo avevano legittimamente e manifestamente prestato. Anche in tale caso, si era ritenuto che tali comunicazioni rientrassero comunque nella definizione di comunicazione commerciale e integrassero, pertanto, un'attività illegittima (**Cass. Civ., sent. n. 11019/2021**).

In conclusione, con l'ordinanza in esame, la Corte di Cassazione ribadisce la ratio complessiva sottesa alla normativa in esame che induce a equiparare la mancanza di consenso degli utenti al dissenso. In ragione di ciò, la Corte arriva quindi a ritenere che, qualora il consenso non sia stato precedentemente prestato, lo stesso debba ritenersi come già negato al momento della stipulazione del contratto. Pertanto, qualsiasi successiva comunicazione commerciale volta ad acquisire il consenso al trattamento di dati personali per finalità di marketing dei medesimi utenti configura di per sé un trattamento illecito di dati in quanto non sorretta da apposita base giuridica (i.e. il consenso).

* * *

SEGUE →



Digital Markets Act

Accordo tra Parlamento e Consiglio dell'Unione europea sul testo

Lo scorso 24 marzo 2022, il Parlamento europeo e il Consiglio dell'Unione europea hanno raggiunto un accordo politico in merito al testo legislativo del Digital Markets Act ("**DMA**"), proposta di regolamento europeo presentata dalla Commissione europea nel dicembre 2020 e avente base giuridica l'art. 114 del Trattato sul funzionamento dell'UE, facendo così un ulteriore passo in avanti verso il perseguimento degli obiettivi della strategia digitale europea annunciata dalla Commissione stessa.

Obiettivi

La regolamentazione del mondo digitale avviata dall'Unione europea tramite l'introduzione di una serie di provvedimenti interconnessi, tra cui è possibile annoverare il DMA e il Digital Services Act ("**DSA**") è volta a:

- garantire che gli utenti digitali abbiano accesso a prodotti e contenuti sicuri, nonché a proteggere i diritti fondamentali degli stessi;
- assicurare il rispetto dei principi di libero mercato e della concorrenza nei settori digitali per stimolare l'innovazione e la crescita delle imprese all'interno del territorio europeo.

In particolare, il DSA mira a proteggere maggiormente gli utenti, tramite il

rafforzamento della disciplina prevista per i servizi digitali e, nello specifico, attraverso la limitazione della diffusione di contenuti illeciti e dannosi online e l'introduzione di ulteriori obblighi in capo agli operatori (in particolare intermediari e piattaforme), mentre il DMA ha l'obiettivo di uniformare le opportunità di crescita delle imprese europee, indipendentemente dalla loro dimensione, tramite la regolamentazione delle società che controllano i punti chiave dei canali di distribuzione del mercato digitale e che hanno, pertanto, assunto una rilevanza notevole nel mercato (c.d. "*Gatekeeper*").

Cosa prevede il DMA

Il Digital Markets Act definisce e disciplina il ruolo dei *Gatekeeper*, introducendo una serie di norme volte a garantire che i mercati nel settore digitale, ove si registra la presenza di tali figure, siano equi e contendibili in tutta l'Unione europea. In particolare, uno degli scopi di tale novità legislativa è quello di assicurare che nessuna piattaforma online di grandi dimensioni che venga ritenuta, quindi, in una posizione di *Gatekeeper* nei confronti di un gran numero di utenti, abusi di tale posizione a scapito dei piccoli operatori del settore digitale. La primaria finalità, dunque, del testo normativo in esame è vietare determinate pratiche commerciali sleali poste in essere dalle grandi società del settore digitale e creare condizioni di parità per le imprese europee di qualsivoglia dimensione.

Tuttavia, sorge spontaneo chiedersi, quando una società è considerata *Gatekeeper*?

L'art. 3 del DMA (come da accordi, ad oggi, raggiunti) stabilisce una serie di criteri oggettivi e precisi per definire tali tipi di società di grandi dimensioni, prevedendo che un fornitore di servizi di piattaforma venga designato come *Gatekeeper* qualora:

- i. detenga una posizione economica forte, abbia un impatto significativo sul mercato interno e operi in più paesi dell'UE. Tale requisito si ritiene soddisfatto laddove l'impresa cui appartiene il fornitore di servizi di base abbia raggiunto un fatturato annuo nello Spazio economico europeo di almeno 7,5 miliardi di euro o qualora la capitalizzazione di mercato media o il valore equo di mercato equivalente dell'impresa cui appartiene sia pari ad almeno 75 miliardi di euro nell'ultimo esercizio finanziario, nonché nel caso in cui fornisca servizi di piattaforma di base (c.d. "*core platform services*", e.g. marketplace e app store, motori di ricerca, social network, servizi cloud, servizi pubblicitari, assistenti vocali e browser web) in almeno tre Stati membri;
- ii. occupi una forte "posizione di intermediazione", nel senso che gestisce un servizio di piattaforma di base che costituisce un punto di accesso (c.d. "*gateway*") importante affinché un gran numero di imprese raggiunga un'ampia base di utenti. Tale requisito si ritiene soddisfatto nel caso in cui il fornitore, nel mettere a disposizione un servizio di piattaforma di base, annoveri almeno 45 milioni di utenti finali attivi su base mensile, stabili o situati nell'Unione, e almeno 10 000 utenti commerciali attivi, durante l'ultimo esercizio finanziario, stabiliti nell'UE;
- iii. detenga (o stia per detenere) una posizione solida e duratura sul mercato. Tale requisito si ritiene soddisfatto nel caso in cui le soglie degli utenti finali e commerciali attivi, di cui alla precedente lett. ii), vengano raggiunte in ciascuno degli ultimi tre esercizi finanziari.

Qualora un fornitore di *core platform services* accerti la sussistenza dei suddetti requisiti e raggiunga, pertanto, le soglie previste dall'art. 3, comma 2, della normativa in esame, lo stesso ha l'obbligo di notificare tale informazione alla Commissione europea entro un arco temporale predeterminato (indicato dalla Commissione pari a 3 mesi e successivamente modificato a 2 dal nuovo accordo sul testo in esame) decorrente dal raggiungimento di tali soglie e fornire le informazioni pertinenti.

Inoltre, si tenga presente che le PMI sono esonerate, salvo casi eccezionali, dalla qualifica di *Gatekeeper* e che è stata prevista anche una categoria di "*gatekeeper emergenti*", la quale consentirà alla Commissione europea di imporre determinati obblighi alle imprese con una posizione concorrenziale assodata, ma ancora non consolidata.

In ogni caso, qualora un soggetto venga designato come *Gatekeeper*, questi, relativamente a ciascuno dei servizi offerti, avrà il dovere, *inter alia*, di:

- a. astenersi dal combinare e incrociare dati personali ricavati dai servizi di piattaforma di base con dati personali provenienti da qualsiasi altro servizio offerto dal *Gatekeeper* o con dati personali provenienti da terzi e dal far registrare gli utenti finali ad altri servizi del *Gatekeeper* al fine di combinare dati personali, a meno che sia stata presentata all'utente finale la scelta

- specifica, in modo chiaro e preciso, e che quest'ultimo abbia prestato il proprio consenso ai sensi del regolamento (UE) 2016/679;
- b. astenersi dall'applicare obblighi contrattuali che impediscano agli utenti commerciali di offrire gli stessi prodotti o servizi agli utenti finali attraverso servizi di intermediazione online di terzi o attraverso il proprio canale di vendita diretta online a prezzi o condizioni diversi da quelli offerti attraverso i servizi di intermediazione online del *Gatekeeper*;
 - c. permettere agli utenti commerciali di comunicare e promuovere offerte anche a condizioni d'acquisto diverse agli utenti finali acquisiti tramite il servizio di piattaforma di base o tramite altri canali, e di concludere contratti con questi utenti finali o ricevere pagamenti per i servizi forniti indipendentemente dal fatto che utilizzino a tal fine i servizi di piattaforma di base del *Gatekeeper*;
 - d. consentire agli utenti finali di accedere e utilizzare, attraverso i servizi di piattaforma di base del *Gatekeeper*, contenuti, abbonamenti, funzionalità o altri elementi utilizzando l'applicazione software di un utente commerciale, anche quando questi elementi sono stati acquisiti dagli utenti finali da parte dell'utente commerciale interessato senza utilizzare i servizi di piattaforma di base del *Gatekeeper*, a meno che il *Gatekeeper* possa dimostrare che tale accesso comprometta la protezione dei dati degli utenti finali o la sicurezza informatica;
 - e. astenersi dall'impedire o limitare, direttamente o indirettamente, agli utenti commerciali o agli utenti finali di sollevare questioni/problematiche presso qualsiasi autorità pubblica competente, compresi i tribunali nazionali, relative a qualsiasi pratica dei *Gatekeeper*;
 - f. astenersi dal richiedere agli utenti commerciali di utilizzare, offrire o interoperare con un servizio di identificazione o qualsiasi altro servizio accessorio del *Gatekeeper* nel contesto dei servizi offerti dagli utenti commerciali che utilizzano i servizi di piattaforma di base di tale *Gatekeeper*;
 - g. non richiedere agli utenti commerciali o agli utenti finali di abbonarsi o registrarsi a qualsiasi altro servizio di piattaforma di base come condizione per utilizzare, accedere, abbonarsi o registrarsi a uno qualsiasi dei loro servizi di piattaforma di base identificati ai sensi della normativa in esame;
 - h. fornire ad *advertiser* e *publisher* o a terzi autorizzati dagli *advertiser* e dai *publisher*, ai quali fornisce servizi di pubblicità digitale, un accesso gratuito, di alta qualità, efficace, continuo e in tempo reale a informazioni complete sulla visibilità e la disponibilità del portafoglio pubblicitario, tra cui le informazioni relative ai prezzi delle offerte e ai meccanismi di determinazione delle commissioni.

La normativa di riferimento pone altresì ulteriori obblighi in capo ai *Gatekeeper* nonché le misure volte a garantire l'osservanza di tali obblighi. Inoltre, è previsto che la

Commissione, nel rispetto delle disposizioni e dei limiti previsti dalla normativa, possa riconoscere e concedere eventuali sospensioni e/o esenzioni dall'osservanza di tali obblighi a favore di un *Gatekeeper* su richiesta motivata di quest'ultimo o di propria iniziativa.

Al fine di garantire il rispetto delle norme previste dal DMA, l'autorità europea preposta all'applicazione del DMA in esame sarà la Commissione europea, coadiuvata da un "comitato consultivo" e un "gruppo ad alto livello".

In caso di violazione delle norme stabilite dal DMA da parte del *Gatekeeper*, quest'ultimo potrà essere sanzionato con un'ammenda fino al 10% del suo fatturato totale a livello mondiale del precedente anno. In caso di ripetute violazioni, l'ammenda può arrivare

sino al 20% del suo fatturato totale a livello mondiale del precedente anno, mentre, qualora si configuri una sistematica violazione delle disposizioni contenute nel DMA, è previsto che vengano irrogate anche sanzioni di natura straordinaria nei confronti del *Gatekeeper*.

Stato dell'arte

A seguito dell'accordo raggiunto lo scorso 24 marzo, il provvedimento in esame dovrà ora essere approvato dal Consiglio dell'Unione europea e dal Parlamento europeo. Una volta approvato il testo legislativo, lo stesso entrerà in vigore il ventesimo giorno successivo alla pubblicazione in Gazzetta ufficiale dell'Unione europea e dovrà essere attuato entro sei mesi dalla sua entrata in vigore.

* * *

Per maggiori informazioni, potete contattare:

Carlo Impalà

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

LinkedIn

Morri Rossetti



Osservatorio TMT&DP





OSSERVATORIO
TMT·DATA PROTECTION

di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it