OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Dicembre 2023

MONTHLY ROUNDUP

Dicembre 2023

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

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Provvedimenti del Garante Privacy

- Mancato e non tempestivo riscontro a istanze dei dipendenti, il Garante multa Autostrade e Amazon trasporti [Link]
- Sanità: Il Garante Privacy sanziona società di formazione [Link]
- Condominio: no a sistemi di videosorveglianza senza delibera dell'assemblea [Link]
- Sanzione a un Comune per uso illecito delle registrazioni di un colloquio [Link]

Provvedimenti EU

- Commission opens formal proceedings against X under the Digital Services Act [Link]
- Commission welcomes political agreement on Artificial Intelligence Act [Link]
- Cookie Pledge A reflection on how to better empower consumers to make effective choices regarding tracking-based advertising models [Link]
- EDPB: Application of the GDPR successful, but sufficient resources are necessary to tackle the challenges of the future [Link]

PRINCIPALI AGGIORNAMENTI

- Cookie Pledge: how to empower consumers to make effective choices regarding tracking-based advertising models
- DSA: firmato l'accordo di collaborazione tra Agcom e Commissione europea
- *Hosting provider* attivo o passivo: quali sono gli elementi di individuazione?

Cookie Pledge: how to empower consumers to make effective choices regarding tracking-based advertising models

On December 19, 2023, the European Commission ("**EU Commission**") released draft pledging principles of cookies after having consulted the European Data Protection Board ("**EDPB**") which gave its opinion on their compliance with e-Privacy Directive and EU Regulation 2016/679 ("**GDPR**").

The cookie pledge initiative was developed by the EU Commission in response to concerns regarding the so-called "cookie fatigue" phenomenon and consists of a voluntary business pledge to simplify the management of cookies and personalised advertising choices by consumers.

The draft pledging principles would ensure that users receive concrete information on how their data is processed, as well as on the consequences of accepting different types of cookies. Users would therefore have greater control over the processing of their data.

Before explaining the principles, it is useful to clarify the context in which this initiative was developed.

Background

During the European Consumer Summit in March 2023, the Commissioner for Justice and Consumers unveiled the EU Commission's proactive initiative to collaborate with key players in addressing consumer concerns regarding cookies and targeted advertising. The initial roundtable discussions, held in April 2023, were limited to EU-level trade entities, consumer associations, and global businesses, as national trade associations or businesses couldn't participate at that stage.

Subsequent to the April roundtable, multiple working groups were established, and a dedicated digital "wiki" platform was set up for technical-level collaboration. Pledge participants were encouraged to contribute written insights, exchange perspectives, and engage in drafting the guiding "principles" through this wiki platform. The working groups reconvened in July, highlighting the necessity for further thorough discussion. As a result, technical meetings were convened in October to delve deeper into various topics, including consumer comprehension of diverse advertising models, their privacy preferences, and the viability of alternative advertising approaches.

Pledging principles in details

Specifically, the draft cookie pledging principles specify that:

- **Essential cookies**: given that such cookies do not require consent, the omission of their details within the consent request would streamline the information users need to read and understand. Furthermore, in accordance with Article 5(3) of the ePrivacy Directive, legitimate interest cannot serve as a legal basis for the processing of personal. Hence, it should be excluded from the cookie banner, it being understood that any subsequent data processing based on legitimate interest ought to be explained in supplementary layers.

- **Content financed at least partially by advertising**: when a business earns revenue through tracking-based advertising or by selling the rights to place trackers on consumers' devices, consumers should be informed about this business model concurrently with the request for cookie consent. Presenting complex cookie banners and subsequently issuing a "pay or leave" ultimatum after consumers decline consent might be seen as manipulative.

- **Clear presentation of the business model**: this will include clear explanations of the consequences of accepting or not-accepting trackers. Most cookies are used to implement a business model and therefore this concomitance should be easily described, understood and implemented in one joint panel regrouping the agreements under consumer law and consent under the e-Privacy/GDPR law. In this panel, the business model options (i.e. accepting advertising based on tracking, accepting other types of advertising or agreeing to pay a fee) will be presented together with the consequences in terms of the purpose of trackers, and this in plain and simple language.

- **Alternative advertising options**: considering the small percentage of consumers willing to pay for various types of online content and the fact that consumers visit numerous websites daily, requesting payment doesn't seem to be a plausible substitute for tracking their online behavior for advertising, which legally necessitates obtaining consent.

- **Aggregate cookie consent**: consent to cookies for advertising purposes should not be necessary for every single tracker, and more information on the types of cookies used for advertising purposes should be given in a second layer, with the possibility to make a more fine-grained selection.

- **No separate consent for cookies** used to manage the advertising model selected by the consumer (e.g. cookies to measure performance of a specific ad or to perform contextual advertising) will be required as the consumers have already expressed their choice to one of the business models.

- **One-year cookie consent expiration**: the consumer should not be asked to accept cookies in one year period of time since the last request. The cookie to record the consumer's refusal is necessary to respect his/her choice. Recording such choice is indispensable for an efficient management of a website and for respecting consumers' choices.

- **App-based cookie preferences**: signals from applications providing consumers with the possibility to record their cookie preferences in advance with at least the same principles as described above will be accepted.

Next Steps

The EU Commission aims to finalize the draft cookie pledging principles in January 2024 and present a final version at the Consumer Summit in April 2024. Stakeholders will then be invited to discuss and adopt these principles on a voluntary basis.

In any case, as clarified by the EDPB, adherence to the cookie pledge principles by organisations

does not equal compliance with the GDPR or ePrivacy Directive and thus the data protection authorities remain competent to exercise their powers when necessary.

* * *

DSA: firmato l'accordo di collaborazione tra Agcom e Commissione europea

Il 30 ottobre 2023, l'Autorità per le garanzie nelle comunicazioni (l'"**Agcom**") ha annunciato di aver firmato un accordo di collaborazione con la Commissione europea per l'applicazione delle disposizioni del Regolamento n. 2022/2065/UE relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (il c.d. "*Digital Services Act*", in breve il "**DSA**").

L'accordo segue una raccomandazione della Commissione europea del 18 ottobre 2023, con la quale gli Stati membri dell'Unione europea erano stati invitati a definire meccanismi di preparazione, cooperazione e coordinamento per facilitare una transizione veloce verso il completamento del nuovo quadro istituzionale del DSA entro il 17 febbraio 2024. L'obiettivo della Commissione è quello di ottenere il supporto degli Stati membri per garantire che le grandi piattaforme online ("*Very Large Online Platforms*", in breve "**VLOPs**") e i grandi motori di ricerca ("*Very Large Online Search Engines*",in breve "**VLOSEs**") rispettino i nuovi obblighi introdotti dal DSA.

L'accordo rappresenta anche il primo passo per la creazione del nuovo sistema di vigilanza dei fornitori di servizi intermediari previsto dal DSA e definisce la cornice procedurale per lo scambio di informazioni, dati, metodologie, sistemi tecnici e strumenti tra l'Agcom e la Commissione europea. Questo scambio mira a identificare e valutare i rischi sistemici delle grandi piattaforme *online*, compresi quelli legati alla diffusione di contenuti illegali e disinformazione, nonché gli effetti negativi sui minori. Uno degli obiettivi del DSA, infatti, è creare un **ambiente digitale sicuro** e **proteggere i minori** dal rischio che questi possano entrare in contatto con contenuti pornografici disponibili *online*, nonché con altri contenuti illegali o vietati che vengono veicolati da piattaforme online o da altri fornitori di servizi intermediari.

Ai sensi del DSA, è previsto un sistema di vigilanza coordinato tra tutti gli Stati membri e a questi ultimi viene conferito il **potere esclusivo di vigilanza** per quanto riguarda i fornitori di servizi intermediari. L'art. 49 del DSA, infatti, richiede a tutti gli Stati membri dell'UE di designare una o più autorità competenti responsabili della supervisione dei fornitori di servizi intermediari e dell'applicazione della nuova regolamentazione digitale, anche a livello europeo, nonché di garantire il coordinamento a livello nazionale in relazione a tali questioni.

In considerazione di ciò, l'Agcom è stata designata, dall'art. 15 del d.l. n. 123 del 2023, quale coordinatore dei servizi digitali per l'Italia.

Il coordinatore dei servizi digitali, ai sensi dell'art. 49, comma 2, del DSA è responsabile di tutte le questioni relative alla vigilanza e all'applicazione del DSA nello Stato membro designante.

A partire dal 17 febbraio 2024, l'Agcom sarà pertanto parte del Comitato europeo per i servizi digitali, un gruppo consultivo indipendente composto da tutti i coordinatori di servizi digitali

finalizzato a garantire un'applicazione coerente del DSA.
Alla luce di tale accordo, l'Agcom ora definirà, attraverso proprie procedure, le modalità di esercizio delle sue nuove competenze, in qualità di coordinatore dei servizi digitali. I poteri di tale figura vengono definiti dall'art. 51 del DSA e sono:

- il potere di effettuare **ispezioni in loco** al fine di esaminare, sequestrare, prendere o ottenere copie di informazioni relative a una presunta violazione in qualsiasi forma, indipendentemente dal supporto di archiviazione;
- il potere di **chiedere spiegazioni** in merito a qualsiasi informazione relativa a una presunta violazione e di registrare le risposte con il consenso dell'interessato mediante qualsiasi mezzo tecnico;
- il potere di or**dinare la cessazione delle violazioni** e, ove opportuno, di imporre misure correttive proporzionate alle violazioni e necessarie per far cessare effettivamente le stesse o di chiedere a un'autorità giudiziaria dello Stato membro di farlo;
- il potere di **imporre sanzioni** pecuniarie o di chiedere a un'autorità giudiziaria dello Stato membro di farlo, in caso di inosservanza del DSA;
- il potere di **imporre penalità di mora** o di chiedere a un'autorità giudiziaria dello Stato membro di farlo, per garantire la cessazione di una violazione in ottemperanza a un ordine emesso dal coordinatore stesso o per il mancato rispetto di uno qualsiasi degli ordini di indagine.

L'Autorità garante della concorrenza e del mercato (l'"**AGCM**"), il Garante per la protezione dei dati personali (il "**Garante Privacy**") e ogni altra autorità nazionale competente, nell'ambito delle rispettive competenze, saranno tenute, ai sensi dell'art. 15 del d.l. n. 123 del 2023, a collaborare con l'Agcom per consentirle di svolgere la sua nuova funzione di coordinatore dei servizi digitali.

* * *

Hosting provider attivo o passivo: quali sono gli elementi di individuazione?

Il 5 dicembre 2023, il Consiglio di Stato (il "**CdS**") ha emesso un'importante sentenza (la n. 10510/2023) riguardante il ricorso presentato da Viagogo Ag ("**Viagogo**") a seguito della sanzione inflitta dall'Autorità per le garanzie nelle comunicazioni ("**Agcom**") con l'ordinanza ingiunzione n. 104/20/CONS.

Nel caso di specie, l'Agcom aveva multato Viagogo con una sanzione pari a **3.7 milioni** di euro per aver violato il divieto di *secondary ticketing* sulla propria piattaforma, in base all'art. 1, comma 545, della l. n. 232 del 2016. Il provvedimento di Agcom aveva altresì il pregio di fare chiarezza sul ruolo attivo svolto dalla società gestrice della piattaforma escludendo la possibilità della stessa di poter godere del regime di esenzione di responsabilità dell'*hosting provider* previsto dalla normativa applicabile.

Il CdS, pronunciatosi adesso, a seguito del ricorso promosso dalla società presso il Tar Lazio e dalla successiva pronuncia di rigetto con sentenza n. 3955/202, ha respinto le doglianze di Viagogo e confermato sostanzialmente sia la legittimità della sanzione inflitta da Agcom che l'impostazione sottesa al provvedimento

dell'Autorità, andando a costituire quindi un ulteriore importante precedente giurisprudenziale in tema di differenza tra hosting provider attivo e passivo.

Di seguito un'illustrazione dei principali aspetti della vicenda.

Che cos'è il *secondary ticketing* e perché preoccupa tanto?

Il *secondary ticketing* (c.d. bagarinaggio) è una pratica scorretta consistente nella vendita di biglietti per eventi come concerti, partite sportive, spettacoli teatrali e altri eventi dal vivo effettuata su canali non autorizzati, da parte di soggetti diversi dai soggetti titolari di canali primari autorizzati, con finalità commerciali e a prezzi maggiorati rispetto al valore nominale.

Il fenomeno è talmente diffuso, specialmente nel mondo digitale, che il legislatore ha introdotto una modifica nell'art. 1, comma 545, della legge n. 232 del 2016, con la legge n. 145 del 2018, estendendo il divieto di vendita o di qualsiasi altra forma di collocamento di biglietti di eventi effettuata da soggetti diversi dai titolari anche ove la condotta avvenga attraverso reti di comunicazione elettronica.

Le sanzioni previste sono varie e includono la comminazione di sanzioni amministrative pecuniarie, nonché la rimozione dei contenuti e l'oscuramento dei siti internet attraverso i quali la violazione viene posta in essere.

Con il proliferare di tale tipo di pratica, già diversi siti web sono stati segnalati e – come nel caso di specie – sanzionati dall'Autorità. A titolo di esempio, basti ricordare lo scandalo scoppiato nel 2016 per i biglietti del concerto dei Coldplay rivenduti a prezzi eccessivamente maggiorati, a seguito di diverse denunce da parte delle associazioni di consumatori che avevano lamentato la vendita-lampo di migliaia di posti ricomparsi dopo qualche minuto su portali specializzati nella rivendita a costi decisamente più alti. Episodi simili sono stati riscontrati in concerti di artisti come Taylor Swift, Maneskin, Dua Lipa, ma anche tanti altri *festival*, concerti, eventi sportivi e per i biglietti d'ingresso in alcuni monumenti italiani come il Colosseo.

Il provvedimento dell'Agcom nei confronti di Viagogo

Viagogo è una società operante nel mercato secondario della vendita dei biglietti per eventi e la sua attività si sviluppa nell'intermediazione tra i soggetti in possesso di un biglietto che intendano rivenderlo (ad eccezione degli organizzatori o dei venditori primari di biglietti) e gli utenti che cercano un biglietto sul mercato secondario perché non più disponibile sul mercato primario.

In tale contesto, l'Agcom aveva condotto un'attività di controllo a seguito degli esposti pervenuti da diverse società attive nel settore dell'organizzazione di eventi musicali live, di società di vendita nel mercato primario di biglietti di eventi musicali e di associazioni di categoria. Queste segnalazioni denunciavano le condotte di Viagogo, effettuate tramite il suo sito web e alcuni canali social, consistenti nella rivendita secondaria di biglietti a specifici eventi musicali live, in violazione dell'art. 1, comma 545 della legge n. 232 del 2016 (c.d. legge di bilancio 2016).

In base a tale disposizione, il divieto di vendita o qualsiasi altro tipo di collocamento di biglietti da parte di soggetti diversi dai titolari autorizzati è finalizzato a contrastare l'elusione e l'evasione fiscale, tutelare il consumatore, il diritto d'autore e garantire l'ordine pubblico. Tale divieto si applica, salvo che l'attività non avvenga – da parte di persone fisiche – in modo occasionale e senza scopo commerciale, nonché ad un prezzo uguale o inferiore a quello nominale.

A seguito delle risultanze istruttorie, l'Agcom aveva sanzionato Viagogo per la vendita di biglietti relativi a 37 eventi e spettacoli senza essere titolare dei sistemi per la loro emissione, a un prezzo maggiorato rispetto al prezzo nominale. Oltre alla sanzione pecuniaria, l'Agcom aveva altresì diffidato Viagogo dal porre in essere ulteriori comportamenti in violazione della normativa.
Da parte sua, invece, Viagogo aveva dichiarato di agire come mero intermediario nella vendita di biglietti, sostenendo che la vendita sul mercato secondario da parte di soggetti non professionali fosse lecita e che l'illiceità fosse riconducibile esclusivamente alla vendita a prezzo più elevato rispetto a quello nominale del titolo: prezzo determinato liberamente dall'utente/venditore.

La società affermava di agire come *hosting provider* passivo, offrendo una "bacheca virtuale" dove gli inserzionisti potevano pubblicare annunci senza che Viagogo avesse effettiva conoscenza o controllo sul loro contenuto, in quanto la piattaforma trattava i dati inseriti dagli inserzionisti attraverso modalità meramente **tecniche, automatiche e passive**.

L'Agcom, al contrario, aveva rilevato che Viagogo svolgeva un ruolo attivo e finalizzato alla vendita. La società, infatti, non si limitava a connettere i venditori con i potenziali acquirenti, ma interveniva attivamente ed estensivamente in tutte le fasi della transazione commerciale, contribuendo alla definizione di parametri giuridici ed economici (ivi compreso il prezzo). A titolo di esempio, la consapevolezza della società risultava provata dal fatto che questa contribuiva alla formazione del prezzo finale della transazione attraverso la funzionalità di "*prezzo consigliato*", nonché attraverso la visualizzazione di un messaggio che recitava "*per vendere più rapidamente i biglietti ti consigliamo di venderli ad un prezzo pari a […] per biglietto*".

In ragione di ciò, l'Agcom aveva affermato che Viagogo non poteva godere dell'esenzione di responsabilità dell'*hosting provider* di cui agli artt. 16 e 17 del D.lgs n. 70/2003, nonché ex artt. 14 e 15 della Direttiva 2000/31/CE (c.d. Direttiva *e-Commerce*; oggi artt. 6 e 8 del Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE, c.d. *Digital Services Act*, in breve "**DSA**"), poiché "*era a conoscenza dei singoli dati caricati dagli utenti ed era consapevole del loro trattamento*".

Alla luce di quanto sopra, pertanto, il tema centrale che rileva è quando un soggetto può essere considerato hosting provider attivo.

Su tali argomentazioni si è espresso di recente anche il CdS, nella sentenza in esame. La pronuncia del CdS potrà avere un effetto rilevante per Viagogo, in quanto, a meno che questa non faccia ricorso in Cassazione e le doglianze vengano accolte, la società dovrà pagare la sanzione inflitta dall'Autorità. Ma la pronuncia con molta probabilità impatterà a cascata sulle altre sanzioni comminate dall'Agcom per contrastare il fenomeno del bagarinaggio digitale (oltre alla multa comminata dall'Agcom nel 2020, nei confronti della stessa Viagogo, con l'ordinanza ingiunzione n. 104/20/CONS, diverse sono infatti le altre violazioni delle norme in materia di *secondary ticketing* per le quali l'Autorità ha già comminato ingenti sanzioni. Si pensi, ad esempio, ai seguenti provvedimenti:

- n. 212/21/CONS, per un importo pari a 750 mila euro (ridotta a causa della pandemia che ha cancellato molti concerti);
- n. 224/22/CONS, per una sanzione pari a 23,580 milioni di euro;
- n. 75/23/CONS, per un importo pari a 12,24 milioni di euro.

Sulla differenza tra hosting provider attivo e passive

L'hosting provider permette ai propri utenti di accedere alla rete internet e ai servizi connessi all'utilizzo di essa e la sua disciplinaè contenuta nel D.lgs. n. 70/2003 che ha dato attuazione alla Direttiva *e-Commerce*, nonché nel DSA.

Secondo l'art. 16 del D.lgs. n. 70/2003, *l'hosting provider* non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che il prestatore (i) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e che (ii) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

In relazione a tale figura, la giurisprudenza europea ha distinto due figure di *hosting provider*:

- ***hosting provider* passivo**, che svolge un'attività di prestazione di servizi di ordine meramente tecnico e automatico, non potendo conoscere né controllare le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi;

- ***hosting provider* attivo**, quando l'attività prestata non è una mera fornitura del servizio di memorizzazione in modo tecnico e automatico, ma ha ad oggetto anche i contenuti della prestazione resa.

La Corte di Giustizia ha enucleato alcuni "*indici di interferenza*", ovvero elementi idonei a individuare la figura dell'*hosting provider* attivo comprendente attività quali di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti pubblicati dagli utenti, operante mediante una gestione imprenditoriale del servizio, nonché l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione.

Gli indici elaborati sono meramente esemplificativi e non devono essere tutti compresenti: in pratica, il ruolo attivo sussiste in caso di qualsiasi condotta che abbia in sostanza l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati.

Anche la giurisprudenza nazionale ha accolto la nozione di *hosting provider* attivo elaborata dalla Corte europea, affermando che in tutti i casi in cui non sussista un'attività di ordine meramente tecnico, automatico e passivo, le limitazioni di responsabilità non sono applicabili.

Infatti, sebbene l'hosting provider non abbia, ai sensi dell'art. 17 del D.lgs. n. 70/2003 (nonché ai sensi dell'art. 15 della Direttiva *e-Commerce*, oggi art. 8 del DSA), un obbligo generale di sorveglianza, per poter invocare l'esenzione generale di responsabilità, la piattaforma non deve essere in alcun caso a conoscenza dell'illiceità del contenuto trasportato.

Peraltro, considerando l'avanzamento tecnologico, l'Agcom, nell'ordinanza ingiunzione n. 318/23/CONS emessa nei confronti di Twitch, aveva rilevato quanto affermato dalla Cassazione nella sentenza n. 39763 del 2021: "*l'evoluzione tecnologica e la capacità di elaborare in modo automatizzato quelle informazioni e quei dati, che prima erano solo "ospitati", temporaneamente o definitivamente sui server, comporta che oggi essi siano "elaborati" per trarre ulteriori profitti e, quindi, risulta oggi non più predicabile alcuna presunzione di "ignoranza" sui contenuti ospitati per conto terzi*".

Tuttavia, occorre valutare in concreto l'attività svolta dall'hosting provider.Infatti, in un'altra

circostanza, il Tar Lazio aveva assolto Google dalla sanzione inflitta dall'Agcom con la delibera n. 541/20/CONS per aver consentito, in qualità di *hosting provider*, la promozione di siti web di gioco d'azzardo che offrono vincite in denaro attraverso video caricati sulla piattaforma YouTube, in violazione del divieto di pubblicità del gioco d'azzardo sancito dall'art. 9 del Decreto Dignità (Tar Lazio n. 11036 del 2021). Nel caso di specie, il Collegio aveva ritenuto che il servizio fornito con "Google ADS" e, quindi, la mera valorizzazione di indici quali la strumentalità alla diffusione del messaggio e la elaborazione di quest'ultimo dal sistema utilizzato dal servizio di posizionamento, non era di per sé sufficiente a fondare la responsabilità del gestore della piattaforma per la violazione del Decreto Dignità. Infatti, seppur Google non fosse del tutto estranea rispetto ai contenuti di cui consentiva la diffusione, non vi era, nella sostanza, un ruolo attivo del gestore.

Conclusioni

Alla luce di quanto sopra è opportuno verificare caso per casola partecipazione (eventuale) della piattaforma rispetto ai contenuti da essa veicolati, tenendo in considerazione non solo gli indici di interferenza individuati dalla giurisprudenza europea e nazionale, ma anche valutando se le condotte poste in essere abbiano in sostanza l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati.

Ad ogni modo, occorre considerare che la crescita esponenziale del ricorso a servizi della società dell'informazione (compreso il servizio di *hosting provider*), principalmente per finalità legittime e socialmente utili di qualsiasi tipo, ha anche accresciuto il ruolo nell'intermediazione e nella diffusione di informazioni e attività illegali o comunque dannose.

Conseguentemente, un comportamento responsabile e diligente da parte dei prestatori di servizi intermediari risulta essenziale per un ambiente *online* sicuro, prevedibile e affidabile e per consentire agli utenti di esercitare i loro diritti fondamentali quali la libertà di espressione e di informazione, la libertà di impresa, il diritto alla non discriminazione e il conseguimento di un livello elevato di protezione dei consumatori.

* * *

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