OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Gennaio 2024

MONTHLY ROUNDUP

Gennaio 2024

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

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Provvedimenti del Garante Privacy

- Giustizia: Garante Privacy, più tutele per gli atti videoregistrati [Link]
- Telemarketing: il Garante Privacy multa un call center per 60mila euro [Link]
- Salute, donazione del corpo alla scienza: ok del Garante [Link]

Provvedimenti EDPB

- L'EDPB individua aree di miglioramento per promuovere il ruolo e il riconoscimento dei DPO [Link]
- Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive [Link]

Provvedimenti AGCOM

- Linee-guida volte a garantire il rispetto delle disposizioni del testo unico da parte degli influencer e istituzione di un apposito tavolo tecnico [Link]

PRINCIPALI AGGIORNAMENTI

- I sistemi di IA generativa: le misure del legislatore cinese
- Artificial Intelligence Act: innovation, risks, and protection of fundamental rights
- Nuove tecniche di tracciamento: i chiarimenti dell'EDPB sull'ambito applicativo dell'art. 5(3) della Direttiva ePrivacy
- Influencer: finalmente approvate le Linee Guida dell'AGCOM

I sistemi di IA generativa: le misure del legislatore cinese

Il 15 agosto 2023, a seguito di un breve periodo di consultazione pubblica, sono entrate in vigore le c.d. "*Measures for the Management of Generative Artificial Intelligence Services*" (in cinese: 生成式人工智能服务管理暂行办法, le "Misure"), emanate dalla *Cyberspace Administration of China* ("**CAC**") (ovvero l'Autorità cinese competente in materia di supervisione e regolamentazione di Internet, protezione dei dati personali e antitrust), con l'obiettivo principale di dettare regole operative volte a disciplinare lo sviluppo e l'utilizzo sempre più rapido dei sistemi di intelligenza generale generativa[1].

Le Misure sono state predisposte tenendo in considerazione quanto previsto dai "3 pilastri" della disciplina cinese in materia di sicurezza e protezione dei dati: la *Cybersecurity Law, la Data Security Law e la Personal Information Protection Law*.

Il contenuto delle Misure

Le Misure si applicano agli sviluppatori e fornitori di sistemi di intelligenza artificiale generativa di testi, immagini, audio, video e altri contenuti destinati ai soggetti che vivono nella Repubblica Popolare Cinese (ad es. Ernie, il chatbot cinese di Baidu analogo a ChatGPT, che genera anche immagini – come Dall-E e Midjourney – e video).

Di contro, le società, nonché gli enti pubblici e gli istituti di ricerca che **sviluppano e utilizzano, ma che non forniscono a soggetti che vivono nella RPC**, servizi e tecnologie di intelligenza artificiale generativa, **non sono soggette alle Misure**.

La normativa prevede che i soggetti che rientrano nell'ambito di applicazione delle Misure devono:

- adottare misure adeguate volte a **prevenire la discriminazione** basata su etnia, convinzioni religiose, Stato, regione, genere, età, impiego di lavoro e stato di salute nel processo di elaborazione degli algoritmi, selezione dei dati di addestramento, generazione e ottimizzazione del modello e nella fornitura del servizio;
- **rispettare i diritti di proprietà intellettuale,** gli standard etici aziendali, mantenere i segreti aziendali e non utilizzare algoritmi, dati, piattaforme e altri strumenti per creare un monopolio e compiere atti di concorrenza sleale;
- rispettare i diritti e gli interessi degli individui, **evitando danneggiare la loro salute fisica e mentale**;
- **rispettare i diritti in materia di protezione dei dati personali**;
- in base al tipo di servizio, adottare misure efficaci per **migliorare la trasparenza** dei servizi di intelligenza artificiale generativa e **migliorare l'accuratezza e la affidabilità dei contenuti generati**;
- sottoscrivere con gli utenti[2] termini e condizioni di utilizzo di tali sistemi, precisando i diritti e gli obblighi di entrambe le parti;
- in un'ottica di tutela dei giovani, **impedire che i minori abusino di sistemi di intelligenza artificiale generativa** (sul tema della tutela dei

[1] Ovvero di tutti quei modelli o tecnologie analoghe in grado di produrre autonomamente contenuti, testi, video o immagini.
[2] Per utenti di sistemi di intelligenza artificiale generativa, ai sensi dell'art. 22 delle Misure, si intendono tutte le persone fisiche e giuridiche che utilizzano sistemi di intelligenza artificiale generativa per generare contenuti.

minori, il CAC ha pubblicato anche le linee guida volte a rafforzare la protezione dei minori online,ne abbiamo parlato qui "Utilizzo di Internet da parte dei minori: combattere la dipendenza attraverso le limitazioni imposte dalle Autorità");

- contrassegnare i contenuti creati dai sistemi di intelligenza artificiale generativa, conformemente a quanto previsto dalle "*Regulations on Administration of Deep Synthesis of Internet Information Services*";
- inserire meccanismi di **protezione delle informazioni** inserite dagli utenti;
- in un'ottica di minimizzazione dei dati, raccogliere soltanto i **dati personali necessari**;
- non conservare informazioni di input che possano identificare gli utenti.

Le Misure stabiliscono altresì che i fornitori di sistemi di intelligenza artificiale generativa debbano svolgere attività di elaborazione dei dati di addestramento, quali il pre-addestramento e l'ottimizzazione dell'addestramento, osservando le seguenti prescrizioni:

- utilizzare dati e modelli di base derivanti da **fonti legittime**;
- non violare i diritti di proprietà intellettuale altrui;
- nel caso in cui vengano utilizzati dati personali degli interessati, **ottenere il loro preventivo consenso**;
- adottare misure tecniche adeguate volte a migliorare la qualità dei dati di addestramento e migliorare l'autenticità, l'accuratezza, l'oggettività e la diversità dei dati di addestramento; e
- **rispettare le ulteriori normative in vigore**, quali ad esempio la *Personal Information Protection Law*.

Inoltre, durante il *data labeling*[3], i fornitori di sistemi di intelligenza artificiale generativa devono formulare regole di etichettatura chiare, specifiche e operative che soddisfino i requisiti previsti dalle Misure, nonché svolgere una valutazione della qualità dell'etichettatura dei dati e condurre una verifica a campione dell'accuratezza dei contenuti etichettati.

Per quanto riguarda i dati personali, i fornitori di sistemi di intelligenza artificiale generativa, laddove questi sistemi trattino dati personali, sono considerati responsabili del trattamento.

In caso di richieste di cancellazione, modifica e copia dei dati personali da parte degli interessati, i fornitori dei sistemi di intelligenza artificiale generativa devono elaborare la richiesta in modo tempestivo, mettendo altresì a disposizione un meccanismo di reclamo e segnalazione.

Conclusioni

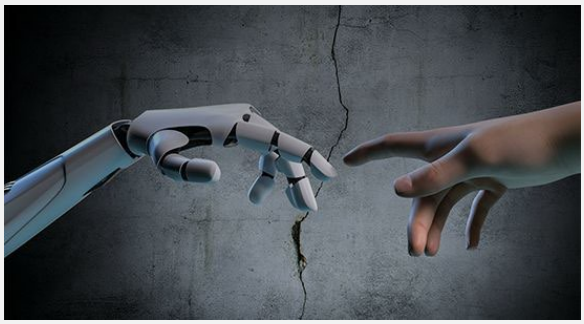
Le recenti iniziative cinesi non solo rappresentano un momento cruciale nel processo legislativo del paese, ma anticipano di fatto numerosi paesi concorrenti, facendo sì che la normativa cinese vada a costituire non solo un *benchmark* per un futuro quadro normativo più sistematico e approfondito, ma rappresenti anche un momento di cambiamento notevole nel contesto legislativo globale in materia di intelligenza artificiale.

[3] I dati sono disponibili in molte forme diverse come testo, immagini, audio e video. Per arricchire i dati in modo che la macchina possa riconoscerli tramite algoritmi di apprendimento automatico, i dati devono essere etichettati. L'etichettatura dei dati è, pertanto, il processo di identificazione dei dati grezzi in modo da attribuire un significato a diversi tipi di dati al fine di addestrare un modello di apprendimento automatico. Quando i dati vengono etichettati, vengono utilizzati per addestrare algoritmi avanzati per riconoscere i modelli in futuro. L'etichettatura è fondamentalmente contrassegnare i dati o aggiungere metadati per renderli più significativi e informativi in modo che le macchine possano capirli e imparare da essi. Ad esempio, un'etichetta può indicare che nell'immagine è raffigurata una persona o un animale, o un file audio è in quale lingua o per determinare il tipo di azione eseguita in un video.

Il legislatore cinese ha mostrato dunque chiaramente la sua determinazione a essere un leader nella regolamentazione di questa tecnologia, aprendo anche il campo a possibili impatti significativi sul futuro sviluppo economico e tecnologico mondiale.

Considerata, quindi, la velocità con cui la Cina si sta muovendo, ci si auspica che anche gli altri paesi (e in primis l'Unione europea) si dotino al più presto di adeguate regole che possano garantire dinamiche competitive nel mercato globale.

* * *



Artificial Intelligence Act: innovation, risks, and protection of fundamental rights

In April 2021, the European Commission (the "**Commission**") proposed the regulation laying down harmonised rules on artificial intelligence (the Artificial Intelligence Act, briefly the "**AI Act**"), the first european regulation on artificial intelligence ("**AI**"). In the following years, the Commission proposed other legal initiatives, connected to the AI systems, such as, in September 2022, the Proposal for a Directive on adapting non contractual civil liability rules to AI (the "**AI Liability Directive**") and a proposal for a Directive on liability for defective products, that shall revise the Directive 85/374/EEC in light of developments related to new technologies, including AI (the "**New Product Liability Directive**").

Regarding the AI Act, on December 6, 2022, the Council reached an agreement on the AI Act and, in mid-June 2023, it started interinstitutional talks with the European Parliament. **In Decembre 2023, the Council presidency and the European Parliament's negotiators reached a provisional agreement on the AI Act**. Subsequently and since the AI Act has raised multiple questions, on December 12, 2023, the Commission answered through a dedicated "Q&A" document (available **here**) and the report was then updated on December 14, 2023.

An overview of the AI Act, considering the Q&A's content

The AI Act aims to promote responsible and ethical use of AI while ensuring that health, safety, and fundamental rights of EU citizens are respected. It shall also protect democracy, rule of law and the environment. Furthermore, it aims to stimulate investment and innovation on AI in Europe. The Regulation will apply to both private and public actors inside and outside the EU as long as the AI system is placed on the Union market, or its use affects people located in the EU. The main idea is to regulate AI based on the latter's capacity to cause harm to society following a "risk-based" approach: **the higher the risk, the stricter the rules. As soon as the approval is reached, the AI Act will be the world's first comprehensive artificial intelligence law**.

Scope of application

The AI Act will apply to providers, deployers of high-risk AI system and importers of AI systems. Conversely, the Regulation shall not apply to providers of **free and open-source models** – which, nonetheless, should not be confused with GPAI providers with systemic risks. Furthermore, it will not apply to systems used exclusively for **military, defence, or national security**. Similarly, the AI Act will not apply to AI systems used for the sole purpose of **research and innovation**.

Different obligations for different risk levels

The new provisions shall establish obligations for providers and users depending on the level of risk from AI.

Specifically, a limited number of systems shall be banned because they may violate fundamental rights. By way of example and not exhaustively, these include AI system for social scoring for public and private purposes, and AI system that exploit the vulnerabilities of the individuals using subliminal techniques. These systems shall fall into the **category of unacceptable risk and shall be prohibited**.

Other **AI systems shall be considered high-risk**. A list of these systems is annexed to the AI Act, in Annex III, and this list can be updated by the Commission to align it with the evolution of AI use cases. The list shall contain systems that potentially can create an adverse impact on people's safety or their fundamental rights.

The following are examples of high-risk AI systems:

- education and vocational training, e.g. to evaluate learning outcomes, steer the learning process, and monitoring of cheating;
- employment, workers management and access to self-employment, e.g. to place targeted job advertisements, analyse and filter job applications, and evaluate candidates;
- access to essential private and public services and benefits (e.g. healthcare), creditworthiness evaluation of natural persons, and risk assessment and pricing in relation to life and health insurance;
- systems used in the fields of law enforcement, border control, administration of justice, and democratic processes;
- evaluation and classification of emergency calls;
- biometric identification, categorisation, and emotion recognition systems (outside the prohibited categories).

In the case of high-risk AI system, the provider – before placing the system on the EU market or otherwise putting into service – shall carry out a conformity assessment to demonstrate that its system complies with the mandatory requirements for trustworthy AI. The assessment shall be repeated if the system or its purpose are substantially modified.

Moreover, the provider of high-risk AI system shall also have to implement **quality and risk management systems** to ensure its compliance with the new requirements and minimise risks for users and affected persons, even after a product is placed on the market.

In the case of minimal risk AI system, which include the majority of AI systems currently in use or likely to be used in the EU (such as AI-enabled video games or spam filters), these systems can be used without additional legal obligations, beyond those mandated by the currently applicable legislation.

In addition, minimal-risk system providers may choose, on a voluntary basis, to implement the requirements for trustworthy AI and adhere to voluntary codes of conduct. The adherence to codes of conduct can be undertaken not only by providers of minimal-risk systems providers but, according to the Commission, also by all providers of non-high-risk applications. In this regard, providers can ensure that their AI system is trustworthy by adhering to codes of conduct adopted by other representative associations or even by developing their own voluntary codes of conduct.

Furthermore, for certain AI systems specific transparency requirements shall be imposed, for

example where there is a clear risk of manipulation (e.g. via use of chatbots). Users shall be aware that they are interacting with a machine.

Additionally, the AI Act considers systemic risks which could arise from general-purpose AI models (e.g. OpenAI's GPT-4, Google DeepMind's Gemini, Bard, etc.), including large generative AI models, because they are very capable or widely used (the "**GPAI**"). The GPAI are systems that can be used for a variety of tasks and are becoming the basis for many AI systems in the EU. For now, GPAI models that were trained using a total computing power of more than 10^25 FLOPs (*Floating Point Operations Per Second* – i.e. a measure of computer performance) are considered to carry systemic risks, given that models trained with larger compute tend to be more powerful.

The AI Act shall require to GPAI providers to ensure compliance with copyright law, assess and mitigate risks, report serious incidents, conduct state-of-the-art tests, and model evaluations, ensure cybersecurity, and provide information on the energy consumption of their models. As a central tool to detail out such rules and to demonstrate compliance with the relevant obligations from the AI Act, GPAI providers shall be engaged with the European AI Office ("**AI Office**") to draw up Codes of Conduct.

AI Act and fundamental rights

Moreover, since the application of the AI Act shall comply with fundamental rights legislation, deployers which are bodies governed by public law or private operators providing public services and operators providing high-risk systems shall conduct a fundamental rights impact assessment and shall notify the results to the national authority[4].

The assessment shall contain a description of some specific information (e.g. the deployer's processes in which the high-risk AI system will be used; the period of time and frequency in which the high-risk AI system is intended to be used; the categories of natural persons and groups likely to be affected by its use; the specific risks of harm likely to impact the affected categories of persons or group of persons; the implementation of human oversight measures; and the measures to be taken in case of the materialization of the risk).

If the provider already met this obligation through the data protection impact assessment according to Article 35 of the GDPR, the fundamental rights impact assessment shall be conducted in conjunction with that data protection impact assessment.

The Regulation also aim to ensure adherence to the principles of non-discrimination. The new mandatory requirements for all high-risk AI systems will serve this purpose. Indeed, those systems will have to be developed in such a way as to avoid discriminatory effects and unfair bias and support diversity, non-discrimination, and equity: they will need to be trained and tested with sufficiently representative datasets to minimise risk of unfair biases embedded in the model and ensure that these can be addressed through appropriate detection, correction and other mitigating measures.

The defence of fundamental right also regards environmental protection and sustainability. In fact, the Commission shall request the European organisations a standardisation deliverable on reporting and documentation processes to improve AI systems resource performance, such as reduction of energy and other resources consumption of the high-risk AI system during its lifecycle, and on energy efficient development of GPAI. In addition, providers of GPAI, which are

[4] All high-risk AI systems will be assessed before being put on the market and also throughout their lifecycle.

trained on large data amounts and therefore prone to high energy consumption, are required to disclose energy consumption. Moreover, such models need to assess energy efficiency.

Application of the AI Act

Following its adoption by the European Parliament and the Council, the AI Act shall enter into force on the 20th day following that of its publication in the official Journal, and it will be fully applicable 2 years after entry into force, with a graduated approach as follows:

- provisions regarding prohibited systems will become applicable 6 month after the effective date;
- obligations for General-purpose AI models ("GPAI") will become applicable 12 months after the effective date;
- obligations for high-risk systems defined in Annex II will become applicable 36 months after the effective date.

The application and the enforcement of the AI Act shall be carried out by the Member States, which hold a key role. For this purpose, each Member State shall designate one or more national competent authorities that will supervise the application and implementation of the AI Act, as well as carry out market surveillance activities. Moreover, in order to increase efficiency and to set an official point of contact with the public and other counterparts, each Member State shall designate one national supervisory authority, which will also represent the country in the European Artificial Intelligence Board – the authority which has extended tasks in advising and assisting the Commission and the Member States.

Moreover, whereas the AI Act shall introduce different level of risks and provides clear definitions, it also leaves the concrete technical solutions and operationalisation primarily to industry-driven standards: in this way the legal framework can be adapted to different use cases and new technologies.

Conclusions

Although the AI Act has not been approved yet, it could be better for business operators to already start to map out their AI compliance strategy as of now. Indeed, some of the obligations outlined above (i.e. provisions regarding prohibited systems and obligations for GPAI) are scheduled to be implemented earlier than the general deadline of 24 months following adoption. These strategies, shall imply, among other things, conducting preliminary assessments about the AI systems models that are intended to be developed, commercialized and/or adopted, the uses of such systems, as well as the associated risks.

Indeed, the business operators shall consider, among others, that every AI Act infringement will lead to the application of a financial penalty by the Member States, which shall be effective, proportionate, and dissuasive, and may be parameterized to the total worldwide annual turnover of the preceding financial year.

Specifically, penalties are expected to be equal:

- up to €35 million or 7% of the turnover, for infringements on prohibited practices or non-compliance related to requirements on data;
- up to €15 million or 3% of the turnover, for non-compliance with any of the other requirements or obligations of the AI Act, including infringements of the rules on GPAI;
- up to €7,5 million or 1,5% of the turnover, for the supply of incorrect, incomplete, or misleading information to notified bodies and national competent authorities in reply to a request.

For infringements committed by SMEs, it is provided a proportional penalty reduction.

Moreover, it shall be considered that, if an individual is affected by a rule violation, he/she can lodge a complaint with a national authority, which itself can launch market surveillance activities.

* * *

Nuove tecniche di tracciamento: i chiarimenti dell'EDPB sull'ambito applicativo dell'art. 5(3) della Direttiva ePrivacy

Il 15 novembre 2023, *l'European Data Protection Board* ("**EDPB**") ha pubblicato le Linee Guida 2/2023 (le "**Linee Guida**") sull'ambito applicativo dell'art. 5(3) della Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (la "**Direttiva ePrivacy**" o la "**Direttiva**"). Le Linee Guida sono attualmente sottoposte a consultazione pubblica fino al 18 gennaio 2024 e, successivamente a tale data, ne verrà approvata e adottata la versione definitiva.

Introduzione

La Direttiva ePrivacy disciplina il trattamento dei dati personali e la tutela della vita privata nell'ambito di ogni forma di comunicazione digitale o elettronica. Nello specifico, l'art. 5 della Direttiva tutela la riservatezza delle comunicazioni, vietandone – senza l'esplicito consenso dell'utente – l'ascolto, la captazione, la memorizzazione e qualsiasi altra forma di intercettazione o di sorveglianza, salvo i casi espressamente previsti dalla legge riguardanti la sicurezza nazionale, la difesa e la sicurezza pubblica.

Ai sensi dell'art. 5(3) della Direttiva, il consenso è altresì richiesto laddove le reti di comunicazione elettronica vengano utilizzate per archiviare informazioni o avere accesso a informazioni archiviate nell'apparecchio. Questa disposizione si applica in particolare agli strumenti di tracciamento online, compresi i cookies [5] e le "tecnologie analoghe".[6]

Ma cosa si intende per "tecnologie analoghe" in un contesto tecnologico in continua evoluzione?

La risposta a questa domanda è fornita dalle Linee Guida che – in un contesto tecnologico in cui l'utilizzo dei cookie sta gradualmente perdendo rilevanza, lasciando spazio a strumenti di tracciamento all'avanguardia e tecnicamente più sofisticati – mirano a chiarire quali siano le nuove ed emergenti tecniche di tracciamento che rientrano nel campo di applicazione della Direttiva.

A testimoniare il progressivo "abbandono" dell'utilizzo dei cookie è proprio Google che, con il test "pilota" avviato su Chrome, conta - entro la fine del 2024 - di disabilitare gradualmente i

[5] I *cookies* sono stringhe di testo che i siti web visitati dall'utente ("prime parti") ovvero siti o web server diversi ("terze parti") posizionano ed archiviano all'interno di un dispositivo terminale dell'utente - *smartphone*, tablet, computer, ecc..

[6] Sul punto il *Working Party* ha affermato che il tracciamento, sia attraverso i cookies, sia attraverso simili tecnologie, rientra nell'ambito applicativo dell'art. 5(3) della Direttiva (WP 29, Opinione 4/2012 sull'esenzione dal consenso per i cookies e Opinione 9/2014 sull'applicazione della Direttiva 2002/58/CE).

cookies di navigazione di terza parte. Ciò significa che, in futuro, le attività degli utenti non saranno più tracciate direttamente dai siti e dagli inserzionisti, ma esclusivamente da Google, impedendo di fatto a terzi di conoscere il comportamento di navigazione dei singoli utenti. Tuttavia, questa nuova funzionalità di Google non elimina completamente il monitoraggio delle attività online.

Posto che tracciare le attività online implica e favorisce, per i *player* del mercato digitale, un maggiore controllo delle informazioni degli utenti, l'EDPB fornisce ai titolari del trattamento e alle parti interessate una maggiore certezza giuridica, chiarendo quali sono le emergenti tecniche di tracciamento e gli adempimenti necessari per il loro utilizzo nel rispetto della normativa applicabile in materia di protezione dei dati personali.

Contenuto delle Linee Guida

Per chiarire quali sono le nuove ed emergenti tecniche di tracciamento che rientrano nel campo di applicazione dell'art. 5(3) della Direttiva, le Linee Guida individuano quattro criteri, analizzando cinque nozioni chiave:

A. *"informazioni";*
B. *"apparecchiature terminali di un abbonato o di un utente";*
C. *"reti di comunicazione elettronica";*
D. *"accesso";* e *"memorizzazione/archiviazione"*.

L'EDPB fornisce altresì una serie di casi pratici, analizzando le tecniche di tracciamento più diffuse (a titolo esemplificativo e non esaustivo, i Pixel Tracking, gli URL, le API, l'IP, l'IoT, l'identificatore univoco) che rientrano nell'ambito di applicazione dell'art. 5(3) della Direttiva ePrivacy.

Pertanto, si è in presenza di operazioni tecniche quando:

A. le operazioni effettuate riguardano "informazioni"

L'EDPB sottolinea come la scelta del termine "informazioni", molto più ampia della nozione di "*dato personale*", sia perfettamente in linea con l'obiettivo dell'art. 5(3) della Direttiva ePrivacy.

Un qualsiasi evento inerente alla sfera privata, anche non coinvolgente dati personali, è esplicitamente coperto dalla formulazione dell'art. 5(3).

Il Considerando 24 della Direttiva stessa afferma chiaramente che la finalità della Direttiva è la salvaguardia della sfera privata degli utenti e che i sistemi di tracciamento occulti e altri dispositivi che possono introdursi nel terminale dell'utente a sua insaputa per accedere e archiviare informazioni o seguire l'attività dell'utente possono costituire una grave intrusione della vita privata dell'utente.

Ne deriva, pertanto, che la definizione di "informazione" non è limitata alla sussistenza o meno di un collegamento con una persona fisica identificata o identificabile, bensì comprende sia dati personali che non personali, di una persona fisica o giuridica, a prescindere da come questi siano stati archiviati e da chi (i.e. da un'entità esterna, dall'utente, da un produttore o in un qualsiasi altro contesto).

B) Le operazioni effettuate riguardano una "*apparecchiatura terminale di un abbonato o di un utente*"

Posto che la Direttiva protegge la *privacy* degli utenti non solo in relazione alla riservatezza delle loro informazioni, ma anche salvaguardando l'integrità delle apparecchiature terminali degli utenti, l'EDPB ha chiarito che la nozione di "*apparecchiatura terminale di un abbonato o di un*

utente" si basa sulla definizione fornita dalla Direttiva 2008/63/CE relativa alla concorrenza sui mercati delle apparecchiature terminali di comunicazioni: si tratta quindi di "*apparecchiature allacciate direttamente o indirettamente all'interfaccia di una rete pubblica di telecomunicazioni per trasmettere, trattare o ricevere informazioni; [...]*".

Ciò posto, l'EDPB elenca nelle Linee Guida i casi in cui si può parlare di un'"*apparecchiatura terminale*" rilevante ai sensi dell'art. 5(3). In particolare:

- se un dispositivo funge unicamente da trasmettitore di comunicazioni – senza dunque apportare alcuna modifica alle informazioni – **non rientra tra le "*apparecchiature terminali*"** rilevanti per l'art. 5(3);
- la protezione dell'art. 5(3) è garantita direttamente all'"*apparecchiatura terminale*" associata all'utente o all'abbonato coinvolto nella comunicazione. Una medesima apparecchiatura può infatti essere condivisa da più utenti o abbonati nel contesto di comunicazioni multiple (si pensi, ad esempio, al caso di un'autovettura dotata di connessione) e una singola comunicazione può coinvolgere più apparecchiature. Ai fini dell'applicabilità della norma non rileva, pertanto, che la comunicazione sia stata avviata dall'utente né che l'utente sia a conoscenza di tale comunicazione.

C) Le operazioni svolte sono effettuate nell'ambito della fornitura di "*servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione*"

La nozione di "*rete di comunicazione elettronica*" non viene definita nella Direttiva ePrivacy. La sua definizione si può, tuttavia, rintracciare nella Direttiva 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, poi sostituita dalla Direttiva 2018/1972 la quale istituisce il Codice Europeo delle Comunicazioni Elettroniche. Tali direttive chiariscono che per *"rete di comunicazione elettronica"* **si intende qualsiasi sistema di rete che consente la trasmissione di segnali elettronici tra i suoi terminali, indipendentemente dal tipo di informazioni veicolato.**

Tale definizione risulta abbastanza ampia, in quanto (i) è neutrale rispetto alle tecnologie di trasmissione, (ii) copre ogni tipologia di apparecchiatura, indipendentemente dai protocolli utilizzati, (iii) non prevede alcun tipo di limitazione per quanto riguarda il numero di apparecchiature terminali connesse alla rete, (iv) non dipende dal modo in cui la rete è installata o gestita, né dalla natura pubblica o privata dell'infrastruttura.

In relazione a tale ultimo punto, è proprio la disponibilità pubblica del servizio di comunicazione sulla rete che fa sì che l'art. 5(3) possa trovare applicazione. Sul punto è importante precisare che il fatto che la rete viene messa a disposizione di un numero ristretto di utenti (ad esempio, gli abbonati) non rende il servizio privato.

D) Le operazioni effettuate costituiscono un "accesso" o una *memorizzazione/archiviazione*"

Posto che, ai sensi dell'art. 1 della Direttiva ePrivacy, la finalità è proteggere la riservatezza delle comunicazioni e l'integrità dei dispositivi, sia delle persone fisiche che delle persone giuridiche, la nozione di "*accesso*", secondo l'EDPB, dev'essere interpretata in modo da salvaguardare tali diritti dalla violazione da parte di terzi.

Pertanto, l'art. 5(3) della Direttiva troverà applicazione ogniqualvolta un **soggetto terzo desideri ottenere l'"accesso" alle informazioni archiviate in un'apparecchiatura e si adoperi attivamente per farlo.**

Nello specifico potranno verificarsi due diverse ipotesi, entrambe rientranti nell'art. 5(3):

- il soggetto terzo istruisce esplicitamente l'"*apparecchiatura terminale*" affinché questa gli invii – in un secondo momento – le informazioni richieste (ad es. *cookies, JavaScript*);
- il soggetto terzo che istruisce l'"*apparecchiatura terminale*" ad inviare i dati e il soggetto che riceve le informazioni sono due entità diverse.

Di contro, la "*memorizzazione*" di cui all'art. 5(3) della Direttiva ePrivacy fa riferimento al salvataggio di informazioni su un supporto fisico di archiviazione elettronica che fa parte dell'"*apparecchiatura terminale dell'utente o dell'abbonato*". In altri termini, il software dell'"*apparecchiatura terminale*" viene istruito a generare informazioni specifiche. Ciò avviene mediante l'utilizzo di protocolli consolidati, come la memorizzazione dei *cookies* del browser e di software personalizzati, indipendentemente da chi ha creato o installato i protocolli o il software sull'"*apparecchiatura terminale*".

La Direttiva, tuttavia, non pone alcun limite né per il periodo di tempo in cui le informazioni devono essere conservate sul supporto di archiviazione per essere considerate "*memorizzate*", né per la quantità di informazioni da memorizzare.

Allo stesso modo, la nozione di "*archiviazione*" non dipende dal tipo di supporto su cui le informazioni sono memorizzate (ad es. *hard disk drives - HDD, solid state drives - SDD, flash drives* e *random-access memory* - RAM, nastro magnetico o *central processing unit* - CPU), pertanto, finché il tipo di supporto costituisce un equivalente funzionale di un supporto di memorizzazione, tale supporto verrà considerato parte dell'apparecchiatura terminale.

Esempi di sistemi di tracciamento

Le Linee Guida dell'EDPB forniscono altresì ad un **elenco non esaustivo di tecniche di tracciamento** di dati ampiamente utilizzate nella prassi, in particolare:

- i **Pixel Tracking**, vale a dire collegamenti ipertestuali ad una risorsa, solitamente un'immagine, incorporati in un contenuto, come un sito web o un'e-mail, il cui unico scopo è quello di stabilire una connessione tra il *client* e l'*host* del Pixel al fine di trasmettere svariate informazioni e, dunque, di tracciare il comportamento degli utenti;
- gli **URL** (*Uniform Resource Locator*), che funzionano nelle stesse modalità dei Pixel Tracking, ma il loro relativo codice identificativo viene aggiunto all'indirizzo del sito web, il quale li utilizza per identificare l'origine del traffico in entrata;
- **l'elaborazione locale** su cui si basano alcune tecnologie che vengono istruite da un software installato sull'"*apparecchiatura terminale*" dell'utente, in cui le informazioni prodotte da tale elaborazione sono poi rese disponibili a soggetti selezionati tramite un'**API** (*Application Programming Interface*) lato client. Se in qualsiasi momento, ad esempio nel software lato client, le informazioni elaborate rese disponibili vengono rinviate in rete, ad esempio ad un server, tale operazione rientra perfettamente nella nozione di "*accesso*" a informazioni già archiviate. Infatti, la circostanza che tali informazioni vengano prodotte localmente non

preclude l'applicazione dell'art. 5(3) della Direttiva.

- il **tracciamento basato solo sull'IP**. Alcuni *provider* hanno sviluppato soluzioni pubblicitarie basate sulla raccolta di un unico componente, ossia l'indirizzo IP, al fine di tracciare la navigazione dell'utente. In questo caso, l'art. 5(3) potrebbe trovare applicazione anche se l'istruzione di rendere accessibile l'IP sia stata impartita da un soggetto diverso rispetto a quello che la riceve. Tuttavia, l'"*accesso*" agli indirizzi IP porterebbe all'applicazione dell'art. 5(3) solo nel caso in cui tali informazioni provengano dall'"*apparecchiatura terminale di un abbonato o di un utente*". In altri termini, a meno che l'ente non sia in grado di garantire che l'indirizzo IP non provenga dall'"*apparecchiatura terminale di un utente o di un abbonato*", dovrà adottare tutte le misure prevista della norma;
- la **segnalazione intermittente e mediata dell'*Internet of Things* (IoT),** in quanto i dispositivi IoT producono informazioni in modo continuo nel tempo che possono essere o meno pre-elaborate localmente. Alcuni di questi dispositivi hanno una connessione diretta a una rete di comunicazione pubblica (ad es. attraverso l'uso del Wi-Fi o di una scheda SIM cellulare) e vengono istruiti dal produttore a trasmettere sempre in streaming le informazioni raccolte, pur memorizzandole prima a livello locale; altri invece non dispongono di una connessione diretta ad una rete di comunicazione pubblica e vengono istruiti a trasmettere le informazioni ad un altro dispositivo ripetitore (uno smartphone, un hub dedicato, ecc.) attraverso una connessione c.d. point-to-point (ad esempio, tramite *Bluetooth*). Nel caso in cui il dispositivo IoT abbia una connessione diretta, questo è considerato un'"*apparecchiatura terminale*" e attraverso la trasmissione da parte del dispositivo IoT dei dati archiviati digitalmente al server remoto, si verifica un "*accesso*". In caso di **connessione point-to-point** la trasmissione dei dati potrebbe non rientrare nell'ambito di applicazione dell'art. 5(3) proprio perché tale trasmissione non avviene su una rete di comunicazione pubblica. Tuttavia, le informazioni ricevute dal dispositivo ripetitore possono essere considerate come "*memorizzate*" da un'"*apparecchiatura terminale*" e, dunque, l'art. 5(3) potrebbe trovare applicazione non appena il dispositivo ripetitore riceve l'istruzione di inviare tali informazioni ad un server remoto;
- **l'identificatore univoco** (o c.d. "persistente"), vale a dire uno strumento, comunemente utilizzato dalle aziende pubblicitarie, ricavato da dati personali "*permanenti*" (nome e cognome, e-mail, numero di telefono, ecc.), che vengono sottoposti ad un processo di *hashing* sul dispositivo dell'utente, raccolti e condivisi tra diversi soggetti per identificare in modo univoco una persona su diversi insiemi di dati (ad es. i dati di utilizzo raccolti attraverso l'uso di un sito web o di un'applicazione). In questo caso l'art. 5(3) risulta essere applicabile in quanto l'entità che effettua la raccolta di dati sta istruendo il browser ad inviare tali informazioni e si verifica dunque un "*accesso*".

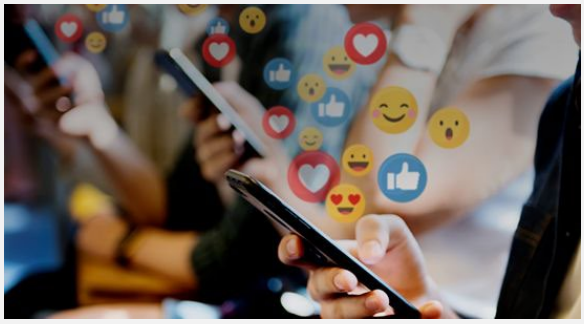
Conclusioni

Attualmente in fase di consultazione pubblica fino al 18 gennaio 2024, le Linee Guida in esame diventeranno un elemento essenziale per definire le attività qualificabili come tracciamento delle attività degli utenti online. Dopo oltre due anni

dall'ultima bozza pubblicata del Regolamento sulla ePrivacy, i progetti per una più ampia riforma della Direttiva ePrivacy sembrano essere ancora in una fase di stallo.

* * *

Influencer: finalmente approvate le Linee Guida dell'AGCOM



Il 10 gennaio 2024, **l'AGCOM** ha finalmente approvato le **Linee guida volte a garantire il rispetto da parte degli influencer** delle disposizioni del decreto legislativo 208/2021 (noto come "*Testo Unico dei servizi di media audiovisivi*" o "**TUSMA**").

Le Linee Guida rappresentano quindi una risposta importante alla crescente rilevanza e diffusione dell'attività degli *influencer*, definiti come **coloro che creano, producono e diffondono contenuti audiovisivi al pubblico**, **assumendo responsabilità editoriale, attraverso piattaforme di condivisione video e *social media***, e costituiscono un passo iniziale significativo da parte delle autorità competenti all'esigenza di regolamentazione dovuta al proliferare di tali figure sul mercato.

L'approvazione delle Linee guida in questione segue la consultazione pubblica avviata dall'Autorità stessa con la Delibera n. 178/23/CONS, terminata lo scorso 21 settembre 2023.

Lo scopo principale dell'Autorità è quello di fornire orientamenti che chiariscano il più possibile l'ambito di applicazione delle **regole del TUSMA agli *influencer*** e i casi in cui la loro attività sia assimilabile alla fornitura di servizi di media audiovisivi, con ciò che ne consegue in termini di obblighi e responsabilità legali.

Le Linee Guida si concentrano, in particolare, sugli *influencer* operanti nel mercato italiano che raggiungono almeno un milione di *follower* e che hanno un valore di *engagement* rate medio pari o superiore al 2% su una piattaforma o social media, e includono misure specifiche per:

- le **comunicazioni commerciali** (ad es. in presenza di contenuti pubblicitari, gli influencer devono chiaramente indicare la natura pubblicitaria del contenuto);
- **la tutela dei diritti fondamentali della persona, dei minori e dei valori dello sport**;
- **meccanismi di richiamo e la rimozione o l'adeguamento dei contenuti**.

In attesa della pubblicazione del testo definitivo delle Linee Guida approvate dall'AGCOM, per maggiori approfondimenti sul tema si rinvia all'articolo Influencer Marketing: nuove regole dell'AGCOM, disponibile sul nostro Osservatorio.

* * *

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