FIVERS

Aggiornamento professionale nei settori Data protection, IP, IT e AI

n. 2 / 2024

DATA PROTECTION

13 Maggio 2024 – Suprema Corte di Cassazione: l'elaborazione e la selezione di materiale video per analizzare comportamenti costituisce un trattamento di dati biometrici ai sensi dell'articolo 9 del GDPR.

---

10 Maggio 2024 – Suprema Corte di Cassazione: la rimozione di un video da Internet comporta l'obbligo di attivarsi anche presso portali terzi.

---

8 Maggio 2024 - Lavoro: Garante Privacy, il dipendente ha il diritto di accedere ai propri dati personali a prescindere dal motivo della richiesta.

---

8 Maggio 2024 – Garante privacy spagnolo: pubblicate le Linee Guida sul trattamento dei dati personali mediante tracking dei sistemi Wi-Fi.

---

5 Maggio 2024 – Lo Stato della Città del Vaticano pubblica il Regolamento generale sulla protezione dei dati personali.

INTELLIGENZA ARTIFICIALE.

21 Maggio 2024 – Il Consiglio UE dà il via libera definitivo alle prime norme mondiali sull'IA.

---

17 Maggio 2024 - Il Consiglio d'Europa adotta il primo trattato internazionale al mondo sull'Intelligenza Artificiale.

---

17 Maggio 2024 - La Commissione obbliga Microsoft a fornire informazioni ai sensi del Digitale Services Act – DSA (Regolamento UE 2022/2065) sui rischi dell'IA generativa disponibile nel motore di ricerca Bing.

MERCATI DIGITALI.

21 Maggio 2024 – Consiglio di Stato e TAR: confermate le sanzioni Agcom a Google per aver diffuso pubblicità di giochi con vincite in denaro su Google Search e YouTube, contravvenendo al Decreto Dignità.

13 maggio 2024 – La Commissione UE designa Booking come gatekeeper ai sensi del Digital Markets Act - DMA (Regolamento UE 2022/1925) e avvia un'indagine di mercato su X.

---

12 maggio 2024 – La Commissione europea lancia gli strumenti di segnalazione per le violazioni del DSA e del DMA (*Whistleblower Tools*).

INFORMATION TECHNOLOGY

6 Maggio 2024 – Corte Suprema di Cassazione: la posta elettronica certificata (PEC) è idonea a dimostrare l'invio e la ricezione del messaggio, ma non a garantire il contenuto del documento ad essa allegato.

DATA PROTECTION

13 Maggio 2024 – Suprema Corte di Cassazione: l'elaborazione e la selezione di materiale video per analizzare comportamenti costituisce un trattamento di dati biometrici ai sensi dell'articolo 9 del GDPR.

La Corte di Cassazione, con ordinanza 13 maggio 2024, n. 12967, ha stabilito rilevanti principi su cosa debba intendersi per trattamento di dati biometrici ai sensi degli artt. 4, n. 14 e 9 del GDPR. Accogliendo il ricorso del Garante contro una sentenza del Tribunale che aveva annullato un suo provvedimento escludendo che vi fosse un trattamento dei dati biometrici nella mera registrazione video di studenti partecipanti ad esami universitari da remoto, con un software che analizzava i comportamenti, scattando foto e flaggando quelle che evidenziavano eventuali comportamenti anomali (es: tentativo di copia), foto poi raccolte in un video sottoposto alla valutazione del docente, ha stabilito che questo trattamento rappresenta un trattamento di dati biometrici poichè " *è palese che le riprese video e foto non hanno solo la funzione di documentare la prova di esame, ma si connotano per la contestuale elaborazione e selezione del materiale raccolto, che converge nella individuazione ed alla segnalazione di comportamenti anomali, attraverso la produzione del video finale*". Convince tuttavia poco l'interpretazione estensiva (tra l'altro di una norma imperativa di divieto come l'art. 9 del GDPR) che individua in questo trattamento di ripresa video tutte e quattro le fasi di un trattamento biometrico come indicato dal Provvedimento generale del Garante privacy sulla biometria del 2014 (1. rilevamento di caratteristiche biometriche; 2) acquisizione di un campione biometrico; 3) estrazione dal campione biometrico, mediante elaborazione matematica, di tratti caratteristici idonei a costituire il modello biometrico; 4) confronto o di match per l'identificazione univoca della persona fisica). Pare mancante soprattutto la fase 3. Tra l'altro "l'identificazione univoca" della persona dovrebbe essere il risultato, del tutto automatico, del trattamento biometrico, mentre nel caso del software analizzato dalla Cassazione, è poco condivisibile l'affermazione che l'Università ha a monte identificato i partecipanti all'esame e dunque il video dello studente sospetto (la cui identità il software non conosce) è ricondotto ex post dal docente alla persona in questione. Quindi titolari e responsabili del trattamento devono porre particolare attenzione a tali sistemi di riprese video assistiti da software di elaborazione immagini, poiché potrebbero ricadere negli stringenti divieti dell'art. 9 GDPR. Casi del genere saranno sempre più frequenti con l'AI Act, che contiene molti concetti relativi alla biometria (da quello di "categorizzazione biometrica" a quello di "sistema di riconoscimento delle emozioni" a quello di "identificazione biometrica", in tempo reale ed ex post). Ma i dubbi restano.

---

10 Maggio 2024 – Suprema Corte di Cassazione: la rimozione di un video da Internet comporta l'obbligo di attivarsi anche presso portali terzi.

Con l'ordinanza n. 9068/2024 la Suprema Corte di Cassazione – occupandosi di un caso di responsabilità di una società di produzione televisiva per non aver limitato la diffusione di materiali video diffamatori – ha confermato la condanna al risarcimento del danno all'emittente televisiva ed ha ricordato – anche ai sensi dell'articolo 17 del Regolamento 679/2016 ("GDPR") e della Giurisprudenza della Corte di Giustizia UE nel caso *Google Spain* del 2013 che il titolare del trattamento dei dati personali ha l'obbligo non solo di cancellare i dati personali trattati illecitamente mediante i link che puntano ad un video, ma anche di attivarsi, attraverso ogni attività volta alla rimozione del servizio e delle notizie che lo riproducono dai motori di ricerca o dai portali di terzi (come YouTube) anche se non dipendenti direttamente da lui. La Corte ha anche precisato che il titolare deve dimostrare e dare prova di un suo approccio proattivo nella gestione delle questioni inerenti alla protezione dei dati personali, in particolare quando questi vengono diffusi in contesti critici per la possibilità offerte dal canale di diffusione e dalla tecnologia web di amplificare le conseguenze dannose della diffusione di notizie. Interessante anche la ricostruzione giurisprudenziale contenuta in questa ordinanza dei rapporti tra diritto di critica, diritto di cronaca, caratteristiche dell'attività giornalistica cosiddetta di inchiesta e profili di diffamazione.

---

8 Maggio 2024 - Lavoro: Garante Privacy, il dipendente ha il diritto di accedere ai propri dati personali a prescindere dal motivo della richiesta.

È quanto ha ribadito il Garante privacy accogliendo in un provvedimento decisorio il reclamo presentato da una donna che aveva chiesto, alla banca di cui era stata dipendente, di accedere al suo fascicolo personale per conoscere quali informazioni potevano aver dato origine ad una sanzione disciplinare nei suoi confronti.

La banca non aveva dato un adeguato riscontro alla richiesta e aveva fornito solo un elenco incompleto della documentazione raccolta, omettendo alcune informazioni in base alle quali era stata irrogata la sanzione disciplinare.

Solo a seguito dell'avvio dell'istruttoria da parte dell'Autorità, l'istituto di credito aveva consegnato all'ex dipendente l'ulteriore documentazione contenuta nel fascicolo.

Si trattava, in particolare, della corrispondenza intrattenuta dalla banca con una terza persona, che lamentava l'illecita comunicazione di informazioni riservate del marito correntista alla reclamante, che le aveva utilizzate nell'ambito di un procedimento giudiziario.

La banca, nelle note di riscontro all'Autorità, ha sostenuto di non aver fornito all'ex dipendente tale documentazione per tutelare il diritto di difesa e la riservatezza dei terzi coinvolti, nonché per l'assenza di interesse all'accesso da parte della reclamante.

Il Garante ha osservato che, in via generale, il diritto di accesso ha lo scopo di consentire all'interessato di avere il controllo sui propri dati personali e di verificarne l'esattezza. Tale diritto, tuttavia, non può essere negato o limitato a secondo della finalità della richiesta. Infatti, in base alle disposizioni del Regolamento, non è chiesto agli interessati di indicare un motivo o una particolare esigenza per giustificare le proprie richieste di esercizio dei diritti, né il titolare del trattamento può verificare i motivi della richiesta. Tale interpretazione è stata chiarita anche dal Comitato europeo per la protezione dei dati (EDPB) mediante l'approvazione delle Linee guida sul diritto di accesso ed è frutto di un costante orientamento giurisprudenziale della Corte di Giustizia.

Nel sanzionare la banca per 20mila euro l'Autorità ha tenuto conto della natura, gravità e durata della violazione, ma anche dell'assenza di precedenti analoghi.

---

8 Maggio 2024 – Garante privacy spagnolo: pubblicate le Linee Guida sul trattamento dei dati personali mediante tracking dei sistemi Wi-Fi.

La localizzazione Wi-Fi è una tecnologia che consente di identificare e tracciare i dispositivi mobili attraverso i segnali Wi-Fi che emettono, per rilevare la presenza del dispositivo in un'area specifica e per identificare i modelli di movimento, motivo per cui viene utilizzata, ad esempio, nella stima della capacità, nell'analisi dei flussi di persone o nella misurazione dei tempi di permanenza.

Le applicazioni pratiche si trovano in centri commerciali, musei, luoghi di lavoro, aree pubbliche, trasporti pubblici o grandi eventi pubblici. Tuttavia, questa pratica pone seri rischi per la privacy, in quanto può consentire il tracciamento dei movimenti delle persone senza conoscenza da parte loro e senza un'adeguata base giuridica.

Molti di questi usi della localizzazione Wi-Fi comportano la raccolta e il trattamento di dati personali e sono soggetti al Regolamento 679/2016 ("GDPR"). IN quetsa prospettiva, l'AEPD – l'Autorità Garante spagnola per i dati personali – ha adottato le Le *linee guida sul trattamento dei dati personali nell'ambito del tracking via tecnologie wi-fi* che analizzano dal punto di vista tecnico e giuridico le implicazioni data protection dell'uso di questa tecnologia, identificando i principali rischi e offrendo una serie di raccomandazioni concrete per un utilizzo responsabile e compatibile con le norme sulla protezione dei dati.

---

5 Maggio 2024 – Lo Stato della Città del Vaticano pubblica il Regolamento generale sulla protezione dei dati personali.

Lo Stato della Città del Vaticano ha pubblicato un decreto che promulga il regolamento generale sulla protezione dei dati personali (il regolamento generale).

In particolare, la normativa generale si applica al trattamento dei dati personali effettuato dal Governatorato dello Stato della Città del Vaticano, limitatamente al territorio dello Stato della Città del Vaticano. I trattamenti effettuati per finalità esclusivamente personali, i dati personali resi manifestamente pubblici o i dati anonimizzati non sono soggetti alla normativa generale.

Il regolamento generale prevede, tra l'altro:

- definizioni chiave quali "dati personali", "trattamento" e "titolare del trattamento", nonché principi di liceità, correttezza, trasparenza, buona fede e proporzionalità;
- condizioni per il trattamento di categorie particolari di dati personali e condizioni per un consenso valido;
- responsabilità del titolare del trattamento, anche per quanto riguarda il registro delle attività di trattamento, l'incarico di un responsabile del trattamento e l'attuazione di misure di sicurezza adeguate;
- i diritti dell'interessato, quali il diritto all'informazione, all'accesso, alla rettifica, alla cancellazione, all'opposizione, alla portabilità dei dati e alla limitazione del trattamento, nonché la procedura per l'esercizio di tali diritti; e
- designazione di un responsabile della protezione dei dati (DPO), compreso il diritto di proporre reclamo al DPO e successiva valutazione da parte del Presidente del Governatorato dello Stato della Città del Vaticano.

Il regolamento generale è entrato immediatamente in vigore al momento della pubblicazione e per un periodo sperimentale di tre anni.

INTELLIGENZA ARTIFICIALE.

21 Maggio 2024 – Il Consiglio UE dà il via libera definitivo alle prime norme mondiali sull'IA.

Il Consiglio ha definitivamente approvato il 21 Maggio 2024 l'AI Act, la prima legge organica volta ad armonizzare le norme sull'intelligenza artificiale. La legislazione faro segue un approccio "basato sul rischio", il che significa che maggiore è il rischio di causare danni alla società, più severe sono le norme. È il primo del suo genere al mondo e può stabilire uno standard globale per la regolamentazione dell'IA. La nuova legge mira a promuovere lo sviluppo e l'adozione di sistemi di IA sicuri e affidabili in tutto il mercato unico dell'UE da parte di attori pubblici e privati. Allo stesso tempo, mira a garantire il rispetto dei diritti fondamentali dei cittadini dell'UE e a stimolare gli investimenti e l'innovazione nell'intelligenza artificiale in Europa. La legge sull'IA si applica solo ai settori all'interno del diritto dell'UE e prevede esenzioni, ad esempio per i sistemi utilizzati esclusivamente per scopi militari e di difesa, nonché per scopi di ricerca.

17 Maggio 2024 - Il Consiglio d'Europa adotta il primo trattato internazionale al mondo sull'intelligenza artificiale.

Il Consiglio d'Europa ha adottato il primo trattato internazionale giuridicamente vincolante volto a garantire il rispetto dei diritti umani, dello Stato di diritto e delle norme giuridiche in materia di democrazia nell'uso dei sistemi di intelligenza artificiale (IA). Il trattato, aperto anche ai paesi extraeuropei, stabilisce un quadro giuridico che copre l'intero ciclo di vita dei sistemi di IA e affronta i rischi che questi possono comportare, promuovendo nel contempo l'innovazione responsabile. La convenzione adotta un approccio basato sul

rischio in ogni fase (progettazione, sviluppo, uso dei sistemi di IA) e richiede un'attenta considerazione di tutte le potenziali conseguenze negative dell'utilizzo dei sistemi di IA.

La Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto è stata adottata a Strasburgo durante la riunione ministeriale annuale del Comitato dei Ministri del Consiglio d'Europa, che riunisce i ministri degli Affari esteri dei 46 Stati membri del Consiglio d'Europa. E' accompagnata da una Relazione esplicativa.

La convenzione è il risultato di due anni di lavoro da parte di un organismo intergovernativo, il Comitato sull'Intelligenza Artificiale (CAI), che ha riunito per redigere il trattato i 46 Stati membri del Consiglio d'Europa, l'Unione europea e 11 Stati non membri (Argentina, Australia, Canada, Costa Rica, Santa Sede, Israele, Giappone, Messico, Perù, Stati Uniti d'America, e Uruguay), nonché rappresentanti del settore privato, della società civile e del mondo accademico, che hanno partecipato in qualità di osservatori.

Il trattato riguarda l'uso dei sistemi di IA nel settore pubblico, comprese le società che agiscono per conto di enti pubblici, e nel settore privato. La convenzione offre alle parti due modi per conformarsi ai suoi principi e obblighi in materia di regolamentazione: le parti possono scegliere di essere direttamente obbligate dalle pertinenti disposizioni della convenzione o, in alternativa, adottare altre misure per conformarsi alle disposizioni del trattato nel pieno rispetto dei loro obblighi internazionali in materia di diritti umani, democrazia e stato di diritto. Questo approccio è necessario a causa delle differenze tra i sistemi giuridici in tutto il mondo.

La convenzione stabilisce requisiti di trasparenza e sorveglianza adattati a contesti e rischi specifici, compresa l'identificazione dei contenuti generati dai sistemi di IA. Le parti dovranno adottare misure per individuare, valutare, prevenire e mitigare i possibili rischi e valutare la necessità di una moratoria, di un divieto o di altre misure appropriate riguardanti gli usi dei sistemi di IA qualora i loro rischi possano essere incompatibili con le norme in materia di diritti umani.

Dovranno inoltre garantire la responsabilità per gli impatti negativi e che i sistemi di IA rispettino l'uguaglianza, compresa la parità di genere, il divieto di discriminazione e i diritti alla privacy. Inoltre, le parti del trattato dovranno garantire la disponibilità di mezzi di ricorso per le vittime di violazioni dei diritti umani connesse all'uso di sistemi di IA e di garanzie procedurali, compresa la notifica a tutte le persone che interagiscono con i sistemi di IA che stanno interagendo con tali sistemi.

Per quanto riguarda i rischi per la democrazia, il trattato impone alle parti di adottare misure volte a garantire che i sistemi di IA non siano utilizzati per compromettere le istituzioni e i processi democratici, compresi il principio della separazione dei poteri, il rispetto dell'indipendenza della magistratura e l'accesso alla giustizia.

Le parti della convenzione non saranno tenute ad applicare le disposizioni del trattato alle attività relative alla protezione degli interessi di sicurezza nazionale, ma saranno obbligate a garantire che tali attività rispettino il diritto internazionale e le istituzioni e i processi democratici. La convenzione non si applicherà alle questioni di difesa nazionale né alle attività di ricerca e sviluppo, tranne nei casi in cui la sperimentazione dei sistemi di IA possa avere il potenziale di interferire con i diritti umani, la democrazia o lo Stato di diritto.

Al fine di garantirne l'effettiva attuazione, la convenzione istituisce un meccanismo di follow-up sotto forma di una conferenza delle parti. Infine, la convenzione richiede che ciascuna parte istituisca un meccanismo di supervisione indipendente per supervisionare il rispetto della convenzione, sensibilizza, stimola un dibattito pubblico informato e svolge consultazioni multilaterali su come dovrebbe essere utilizzata la tecnologia di IA. La convenzione quadro sarà aperta alla firma a Vilnius (Lituania) il 5 settembre in occasione di una conferenza dei ministri della giustizia.

17 Maggio 2024 - La Commissione obbliga Microsoft a fornire informazioni ai sensi del Digitale Services Act – DSA (Regolamento UE 2022/2065) sui rischi dell'IA generativa disponibile nel motore di ricerca Bing.

La Commissione intensifica le sue azioni esecutive nei confronti di Microsoft: dopo non aver ricevuto risposta alla sua richiesta di informazioni del 14 marzo in merito ai rischi specifici derivanti dalle funzionalità di IA generativa di Bing, in particolare "*Copilot in Bing*" e "*Image Creator by Designer",* la società ha ora tempo fino al 27 maggio per fornire le informazioni richieste alla Commissione.

Con tale richiesta di informazioni - giuridicamente vincolante - la Commissione chiede a Bing di fornire documenti e dati interni che non sono stati divulgati nella precedente risposta. La richiesta di informazioni si basa sul sospetto che Bing possa aver violato il DSA per rischi legati all'IA generativa, come le cosiddette "allucinazioni", la diffusione virale di deepfake, nonché la manipolazione automatizzata di servizi che possono fuorviare gli elettori. Ai sensi del DSA, i servizi designati, incluso Bing, devono effettuare un'adeguata valutazione del rischio e adottare le rispettive misure di mitigazione del rischio (articoli 34 e 35 del DSA). L'IA generativa è uno dei rischi individuati dalla Commissione nei suoi orientamenti sull'integrità dei processi elettorali, in particolare per le prossime elezioni del Parlamento europeo di giugno.

Nel caso in cui Bing non risponda entro il termine, la Commissione può imporre ammende fino all'1% del reddito annuo totale o del fatturato mondiale del fornitore e sanzioni periodiche fino al 5% del reddito medio giornaliero del fornitore o del fatturato annuo mondiale. La Commissione può inoltre infliggere ammende fino all'1% del reddito annuo totale o del fatturato mondiale del fornitore per informazioni inesatte, incomplete o fuorvianti in risposta a una richiesta di informazioni.

A seguito della sua designazione come motore di ricerca online di grandi dimensioni, Bing è tenuto a rispettare integralmente le disposizioni introdotte dal DSA. In questo caso particolare, la Commissione ritiene che le sospette violazioni della legge sui servizi digitali possano presentare rischi legati ai processi elettorali. Ai sensi dell'articolo 67, paragrafo 3, del DSA, dunque, la Commissione ha il potere di chiedere ulteriori informazioni relative a presunte infrazioni.

La richiesta di informazioni è un atto investigativo che non pregiudica eventuali ulteriori misure che la Commissione può decidere o meno di adottare. Sulla base della valutazione delle risposte, la Commissione valuterà le prossime tappe. Ciò potrebbe comportare l'avvio di un procedimento formale, ai sensi dell'articolo 66 della legge sui servizi digitali.

MERCATI DIGITALI.

21 Maggio 2024 – Consiglio di Stato e TAR: confermate le sanzioni Agcom a Google per aver diffuso pubblicità di giochi con vincite in denaro su Google Search e YouTube, contravvenendo al Decreto Dignità.

Il Consiglio di Stato (con la sentenza n. 4277 del 13 maggio 2024 relativamente al servizio di motore di ricerca “Google Search”) e il TAR Lazio (con l’ordinanza n. 1940 del 16 maggio 2024, relativamente al servizio di condivisione di video “YouTube”) hanno confermato le sanzioni che AGCOM aveva comminato per violazione del divieto di pubblicità di giochi con vincite in denaro introdotto dall’articolo 9 del Decreto Legge n. 87 del 12 luglio 2018, convertito con modifiche con la Legge n. 96 del 9 agosto 2018 (“*Decreto Dignità*”). Si tratta di una fondamentale Giurisprudenza (in linea anche con la sentenza della Suprema Corte di Cassazione n. 7708 del 19 marzo 2019 in tema di responsabilità dei provider) che per la prima volta ha riconosciuto la responsabilità di Google/YouTube per violazione – mediante fornitura del proprio servizio *Google Ads* – del Decreto Dignità. Google è stato dunque considerato dai giudici amministrativi un *hosting provider attivo* (perché – spiega il Consiglio di Stato – Google compie un controllo sui contenuti del servizio *Google Ads*, in modo da ottimizzare i propri interessi economici) e, dunque, direttamente responsabile per i contenuti promossi mediante tale servizio pubblicitario. Il “ribaltamento”

giurisprudenziale è assolutamente rilevante perché in un certo senso contrasta con la precedente pronuncia della Corte di Giustizia della UE (del 23 marzo 2010 sul caso C-236/08) in cui Google era stato ritenuto soggetto avente funzione "*meramente tecnica, automatica e passiva*" del servizio Google Ads e dunque irresponsabile nella sua qualificazione di *hosting provider passivo*. Per la prima volta – poi - una sentenza stabilisce che chi ospita una pubblicità su internet non è esonerato dalla responsabilità di vigilare sul contenuto. Il principio supportato dalla sentenza del Consiglio di Stato apre la strada alla responsabilità delle piattaforme per qualsiasi pubblicità illegale, anche di contenuti che violano il diritto d'autore, evidenziando effetti che in teoria si annunciano come dirompenti. Il Consiglio di Stato ha stabilito che il momento in cui la piattaforma viene, necessariamente, a conoscenza della natura del contenuto (in alcuni casi "*esplicitamente illecita*") coincide con il momento in cui l'ha accettato per pubblicarlo (e non con quello – successivo – di notifica da parte di partner commerciali e/o di utenti). E ciò appare in linea anche con la tempistica rapida della rimozione di contenuti illegali ora prevista dalla nuova normativa introdotta dal Digital Services Act (Regolamento UE 2022/2065).

---

13 maggio 2024 – La Commissione UE designa Booking come gatekeeper ai sensi del Digital Markets Act - DMA (Regolamento UE 2022/1925) e avvia un'indagine di mercato su X.

La Commissione europea ha designato Booking come *gatekeeper* ai sensi del DMA per il suo servizio Booking.com di intermediazione online e ha deciso di non designare X Ads e TikTok Ads. Parallelamente, la Commissione ha avviato un'indagine di mercato per valutare ulteriormente il reclamo presentato da X in relazione al servizio di social network online X. Queste decisioni fanno seguito a un processo di riesame condotto dalla Commissione UE dopo aver ricevuto le notifiche delle tre società in merito al loro potenziale status di *gatekeeper* il 1º marzo 2024.
Sulla base dell'autovalutazione di Booking presentata il 1˚ marzo 2024 in merito al raggiungimento delle soglie pertinenti, la Commissione europea ha stabilito che questo servizio di piattaforma di base costituisce un importante punto di accesso tra le imprese e i consumatori.
Parallelamente, la Commissione ha avviato un'indagine di mercato per valutare ulteriormente la confutazione presentata il 1° marzo 2024 in relazione al servizio di social network online X. Tale confutazione sostiene che, nonostante il raggiungimento delle soglie, X il servizio non possa qualificarsi come un importante punto di accesso tra le imprese e i consumatori. L'inchiesta dovrebbe concludersi entro cinque mesi.

---

12 maggio 2024 – La Commissione europea lancia gli strumenti di segnalazione per le violazioni del DSA e del DMA (*Whistleblower Tools*).

La Commissione europea ha lanciato due strumenti di segnalazione per il Digital Services Act (DSA) e il Digital Markets Act (DMA). Gli strumenti consentiranno alle persone di fornire, senza timore di rappresaglie, informazioni che consentano di identificare e scoprire le pratiche dannose delle piattaforme online di grandi dimensioni (VLOP) o dei motori di ricerca di grandi dimensioni (VLOSE) designati ai sensi della legge sui servizi digitali (DSA) o di eventuali violazioni degli obblighi dei *gatekeeper* ai sensi della legge sui mercati digitali (DMA).

Gli informatori possono fornire informazioni pertinenti in forma anonima o meno, in una qualsiasi delle lingue ufficiali dell'UE e in qualsiasi formato pertinente (ad esempio, segnalazioni, promemoria, scambi di e-mail, metriche di dati, ricerche interne, decisioni o qualsiasi circostanza pertinente). Gli strumenti di segnalazione offrono un modo sicuro per segnalare tali informazioni. Tutti i dati sono crittografati, garantendo una solida protezione e il rispetto dei quadri legali standard. Gli strumenti sono stati certificati da un ente terzo indipendente, garantendo la completa privacy dell'informatore in tutte le sue comunicazioni con la Commissione.

Le persone che si imbattono in pratiche dannose da parte di VLOP o VLOSE possono, ai sensi della legge sui servizi digitali, presentare reclami al proprio coordinatore nazionale dei servizi digitali. Qualsiasi caso di inosservanza della legge sui mercati digitali da parte dei *gatekeepers* può essere segnalato all'apposito punto di contatto della Commissione o alle autorità nazionali garanti della concorrenza del rispettivo Stato membro in cui ha sede il denunciante.

INFORMATION TECHNOLOGY

6 Maggio 2024 – Corte Suprema di Cassazione: la posta elettronica certificata (PEC) è idonea a dimostrare l'invio e la ricezione del messaggio, ma non a garantire il contenuto del documento ad essa allegato.

La posta elettronica certificata (PEC) certifica la provenienza della stessa, e la data dell'invio, ma da questa non si può durre che anche il documento allegato sia riferibile al suo autore e che abbia effettivamente quel contenuto. Dunque, la posta elettronica certificata (PEC) è in grado di attestare in maniera certa l'avvenuta trasmissione e ricezione del messaggio, le modalità di spedizione (data, ora e formato) ed anche il suo contenuto, ma limitatamente alla PEC stessa, non al file allegato ad essa.
Se alla PEC è stato allegato un file con un determinato nome, estensione, formato e dimensioni, la ricevuta lo attesterà, ma non farà prova del contenuto di quel file, occorrendo, a tal fine, che sul file allegato sia apposta la firma digitale, che certificherà la provenienza del documento e la sua integrità.

La produzione della posta elettronica certificata in formato elettronico non è quindi idonea a fornire la prova del contenuto del documento allegato (e della data certa). Altresì, la certezza della data della PEC non si estende alla scrittura privata dalla prima richiamata.