USR SICILIA
Ufficio Scolastico Regionale per la Sicilia

NEWSLETTER

AMMINISTRAZIONE DIGITALE E PRIVACY

A CURA DEL PROF. AVV. MARCO MANCARELLA

02
GIUGNO 2024

IN COLLABORAZIONE CON
UNIVERSITÀ DEL SALENTO
DiSUS DIPARTIMENTO DI Scienze Umane e Sociali
MEDITERRANEAN OBSERVATORY MODiCT DIGITAL CULTURE & TOURISM
Centro di ricerca del Dipartimento di Scienze Umane e Sociali

C.V. NEL TEST INVALSI, INDAGINE DEL GARANTE

Il Garante per la Protezione dei Dati Personali ha inviato una richiesta di informazioni all'Istituto Invalsi circa la possibile integrazione dei risultati dei test nazionali nel curriculum digitale degli studenti, allegato al diploma di scuola superiore. L'obiettivo dell'istruttoria è quello di **accertare il pieno rispetto dei principi di protezione dei dati personali dei minori** nell'ambito di questa possibile nuova modalità di utilizzo e diffusione dei risultati delle rilevazioni Invalsi.

Tra gli elementi su cui l'Invalsi dovrà fornire **riscontro entro 20 giorni** ci sono i presupposti normativi per l'inserimento dei risultati delle prove nel curriculum, le tipologie di test coinvolte, le finalità e la logica del trattamento.

Il Garante chiede, inoltre, di conoscere le misure adottate per **assicurare la qualità dei dati e l'intervento umano nel processo decisionale**, nell'eventualità che vengano effettuate attività automatizzate di profilazione e classificazione degli studenti sulla base delle prove.

PUBBLICATO SU: *https://www.federprivacy.org/informazione/garante-privacy/faro-del-garante-privacy-sui-test-invalsi-nel-curriculum-dello-studente*

EDPB, LA ROADMAP 2024-27

Nel corso della riunione plenaria dello **scorso 18 aprile**, l'European Data Protection Board (EDPB) ha definito la propria strategia per il quadriennio 2024-2027 – per rispondere alle esigenze attuali di **protezione dei dati personali** e al **contesto digitale** in rapido mutamento - articolandola in **4 punti fondamentali**: 1. Migliorare l'armonizzazione normativa e promuovere la compliance; 2. Rafforzare una cultura comune per l'applicazione delle norme e una cooperazione efficace; 3. Salvaguardare la tutela dei dati nel contesto dell'evoluzione digitale e interdisciplinare; 4. Contribuire al dialogo globale sulla protezione dati.

PUBBLICATO SU: *https://www.federprivacy.org/informazione/primo-piano/european-data-protection-board-la-nuova-strategia-per-il-periodo-2024-2027*

ANTI-BULLISMO A SCUOLA, LA NUOVA NORMATIVA

All'unanimità, la Camera ha approvato un **disegno di legge** che prevede una serie di misure concrete per prevenire e contrastare il fenomeno del bullismo e del cyberbullismo, con un focus specifico sull'ambito scolastico.

Tra le principali **novità** introdotte: Istituzione della "**Giornata del rispetto**" il 20 gennaio di ogni anno; Obbligo per ogni istituto scolastico di dotarsi di un **codice interno**, contenente regole e procedure per la prevenzione e il contrasto di bullismo e cyberbullismo; Potenziamento del servizio di **assistenza psicologica e legale** alle vittime di bullismo e cyberbullismo tramite il numero di pubblica utilità "**Emergenza infanzia 114**" e molto altro.

PUBBLICATO SU: *https://www.orizzontescuola.it/bullismo-e-cyberbullismo-ogni-scuola-dovra-adottare-codice-interno-e-tavolo-di-monitoraggio-nasce-la-giornata-del-rispetto-il-20-gennaio-via-libera-alla-proposta-di-legge/#:~:text=2024%20%2D%2018%3A32-,Bullismo%20e%20cyberbullismo%2C%20ogni%20scuola%20dovr%C3%A0%20adottare%20codice%20interno%20e,libera%20alla%20proposta%20di%20legge&text=La%20Camera%20dei%20Deputati%20ha,del%20bullismo%20e%20del%20cyberbullismo*

ARGOMENTO E TEMI TRATTATI
da Piermario Boccellato nell'articolo "Minori under 16 e social network, il Governo vara la stretta (anche per i baby influencer). I 6 articoli della bozza del ddl": *https://www.key4biz.it/minori-under-16-e-social-network-il-governo-vara-la-stretta-anche-per-i-baby-influencer-i-6-articoli-della-bozza-del-ddl/491226/*

MINORI E SOCIAL: IL DDL È STRINGENTE

Sono **6** gli **articoli** del disegno di legge, varato dal Governo, che ha come obiettivo quello di disciplinare "**la verifica dell'età dell'utente**" sui social.

L'**articolo 3** stabilisce che "i contratti con i fornitori di servizi della società dell'informazione conclusi da minori di anni 16 sono nulli e non possono peraltro rappresentare idonea base giuridica per il trattamento dei dati personali". Spetterà, pertanto, ai fornitori dei servizi "l'onere di provare che i contratti siano stati firmata da ultra-sedicenni o da minori di anni 16 con l'assistenza di chi ne esercita la responsabilità genitoriale o ne è tutore".

L'**articolo 5** del ddl, invece, prevede una **regolamentazione più stringente** sul fenomeno dei **baby influencer**. In questo caso viene stabilito che "la diffusione, non occasionale, dell'immagine di un minore di sedici anni attraverso un servizio di piattaforma online" è soggetta "all'autorizzazione di chi ne esercita la responsabilità genitoriale o ne è tutore, nonché della direzione provinciale del lavoro", nel caso in cui la diffusione dell'immagine del minore produca o sia finalizzata a produrre "entrate dirette o indirette superiore ai 12mila euro all'anno".

PUBBLICATO SU: *https://www.rainews.it/articoli/2024/05/tik-tok-in-arrivo-le-etichette-per-smascherare-contenuti-fake--dbd38a1f-617c-4ada-8f88-0c602b12a0fa.html*

FAKE NEWS? LE ETICHETTE DI TIKTOK PER SMASCHERARLE

Se, da un lato, le organizzazioni stanno comprendendo, sempre più, l'importanza di adottare i Contenuti Generati dall'Intelligenza Artificiale (AIGC) in modo responsabile; dall'altro, come in tutte le cose, ci saranno sempre utenti che utilizzeranno questo strumento tecnologico per ingannare intenzionalmente gli altri.

È per questo motivo che **Tik Tok** ha pensato di inserire sulla propria piattaforma social le '***Content Credentials***', utili a "**marchiare**" i contenuti generati dall'IA tramite una '**etichetta**' in grado di lasciare una traccia – sotto forma di metadati – **anche nel caso in cui quel contenuto venga utilizzato su altri social**.

Sinora, Tik Tok era stato in grado di mettere solo un watermark sui video generati direttamente con l'AI mentre, per tutto il materiale generato su altre piattaforme, esisteva "solo" l'obbligo per gli utenti di segnalarlo manualmente.

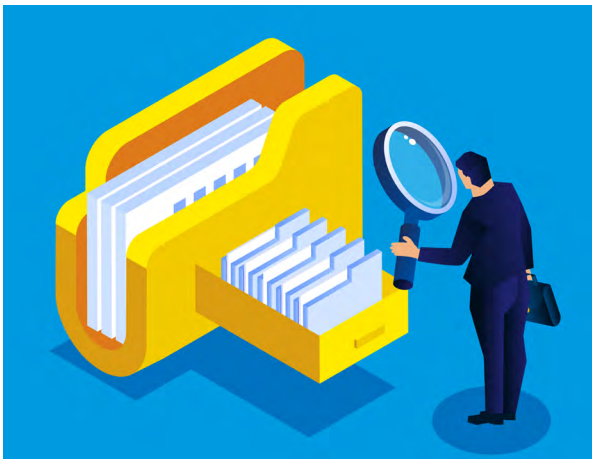
È DEFINITIVO, IL CONSIGLIO UE APPROVA L'AI ACT

Via libera definitivo all'AI Act, il primo quadro giuridico al mondo che disciplina lo sviluppo, l'immissione sul mercato e l'utilizzo dei sistemi di intelligenza artificiale (IA) nell'Ue.

Il regolamento, che gravita attorno a principi quali **diritti umani** e **trasparenza**, stabilisce una serie di **obblighi** per fornitori e sviluppatori di sistemi di IA, proporzionati al livello di rischio associato. Le nuove norme saranno applicabili **a partire da due anni dall'entrata in vigore**, con eccezione di alcune disposizioni.

Quali sono nel dettaglio i divieti che riguarderanno i contesti sia lavorativi che scolastici? Cosa dice l'AI Act circa l'IA generativa per regolamentare sistemi come ChatGPT?

ARGOMENTO E TEMI TRATTATI
da Francesco Leone nell'articolo "Il consiglio UE approva in via definitiva l'AI ACT: i dettagli": *https://www.engage.it/tecnologia/il-consiglio-ue-approva-in-via-definitiva-lai-act-i-dettagli.aspx*



PUBBLICATO SU: *https://www.federprivacy.org/informazione/garante-privacy/il-dipendente-ha-diritto-di-accedere-al-proprio-fascicolo-per-conoscere-le-informazioni-da-cui-e-scaturita-una-sanzione-disciplinare-del-datore-d-i-lavoro*

DIPENDENTE SANZIONATO PUÒ ACCEDERE AI DATI

Il Garante per la Privacy ha ribadito il **diritto del lavoratore** di **accedere ai propri dati personali** detenuti dal datore di lavoro, **indipendentemente dal motivo della richiesta di accesso**.

La decisione fa seguito al reclamo di una ex dipendente di una banca, alla quale era stata negata la possibilità di visionare parte del proprio fascicolo contenente le informazioni che avevano portato a una sanzione disciplinare nei suoi confronti. Il Garante **ha sanzionato la banca**.

Per il Garante, infatti, il diritto di accesso ha lo scopo di permettere il controllo sui propri dati e la verifica della loro esattezza, senza che il titolare possa limitarlo in base alle motivazioni addotte dall'interessato. Un'interpretazione confermata anche dalle **linee guida** del **Comitato Europeo per la Protezione Dati**.

AI PER SICUREZZA LAVORATORI: COME GESTIRE LA COMPLIANCE PRIVACY

L'utilizzo di soluzioni di Intelligenza Artificiale (IA) per la sicurezza sul lavoro richiede una valutazione attenta degli aspetti legati alla protezione dei dati personali dei lavoratori, per evitare rischi di sanzioni e costi inutili. Pertanto, è necessario:

Comprendere se il prodotto comporta un trasferimento di dati personali dei lavoratori verso società terze. In tal caso, è necessario regolamentare questo flusso di dati tramite una **nomina a Responsabile del trattamento** ai sensi del GDPR, verificando le adeguate misure di sicurezza.

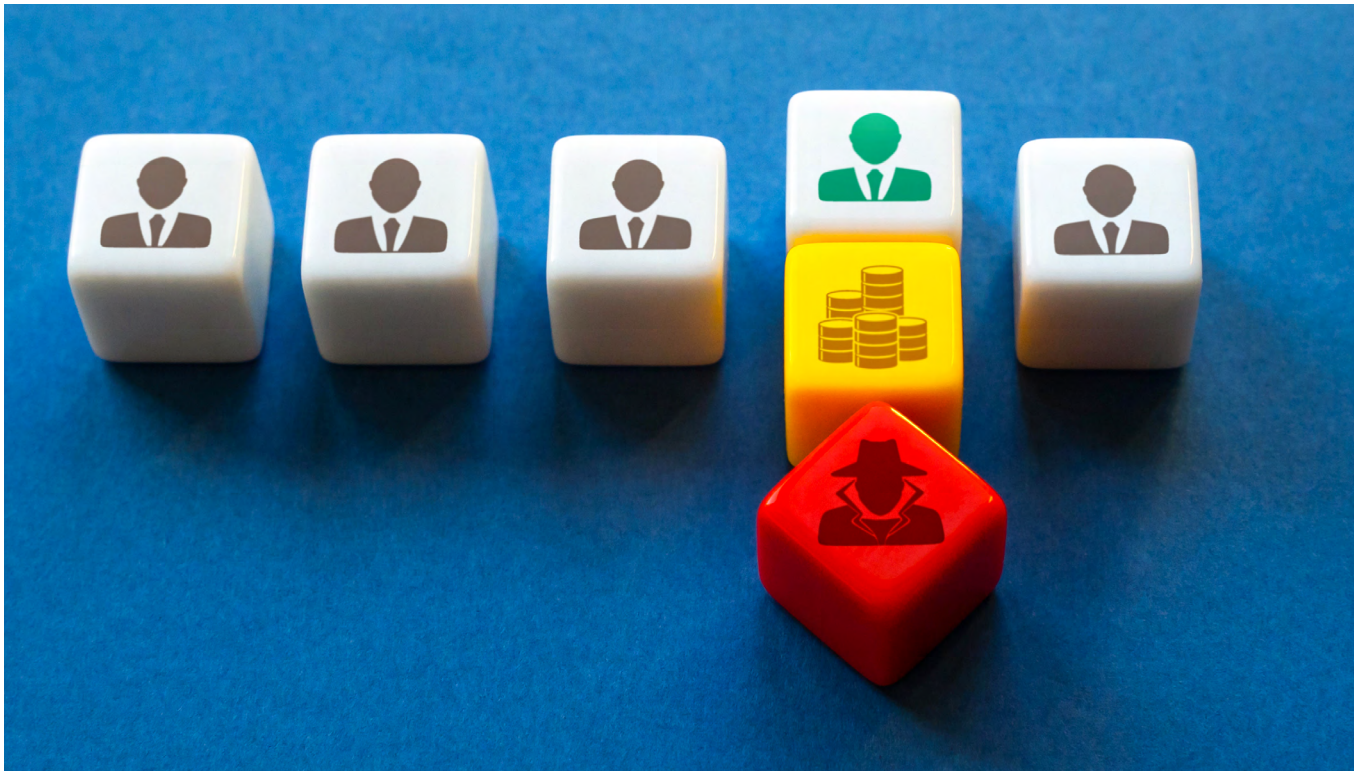
Valutare se l'implementazione dell'IA rispetti il **principio di minimizzazione dei dati**, trattandone solo quelli strettamente necessari per tutelare la sicurezza, senza eccedere.

È probabile che l'adozione di tali soluzioni richieda una **Valutazione d'Impatto sulla Protezione Dati**, considerando anche la potenziale attività di controllo a distanza sui lavoratori, da gestire secondo lo Statuto dei Lavoratori.

ARGOMENTO E TEMI TRATTATI
da Matteo Alessandro Pagani e Alessandro Burro nell'articolo "L'utilizzo dell'Intelligenza Artificiale nei prodotti per la sicurezza sul lavoro: gli aspetti privacy da valutare": *https://www.federprivacy.org/informazione/primo-piano/l-utilizzo-dell-intelligenza-artificiale-nei-prodotti-per-la-sicurezza-sul-lavoro-gli-aspetti-privacy-da-valutare*

Altre attività essenziali sono l'informativa ai dipendenti e la verifica del **rispetto del principio di privacy by design** nell'ideazione del prodotto/servizio IA.

Per non incorrere in violazioni e sanzioni, le organizzazioni sono invitate ad affidarsi a consulenti esperti sia in materia di **privacy** che di **diritto del lavoro**.



DATA BREACH: NON LIBERA DA RESPONSABILITÀ NEPPURE L'ASSENZA DI DANNI PER GLI INTERESSATI

Se le violazioni alla sicurezza dipendono da scelte del fornitore esterno, le sanzioni perviste dal GDPR vanno applicate a quest'ultimo.

Il principio ha trovato applicazione nell'**ingiunzione n. 198 dell'11/4/2024**, con la quale il Garante privacy italiano ha comminato una sanzione pecuniaria di 25 mila euro ad una azienda speciale fornitrice di servizi IT a una camera di commercio.

Nel caso specifico si è trattato di un **errore umano**, poiché il personale dell'azienda non ha cancellato un file con dati di oltre 22 mila utenti, di cui hacker si sono appropriati. Relativamente ai **ruoli privacy**, l'**azienda** aveva quello di **responsabile esterno del trattamento dei dati**, cioè di ente che tratta dati personali per conto del titolare del trattamento (in questo caso la camera di commercio).

L'ingiunzione del Garante è disponibile all'url: *www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10013321*

PUBBLICATO SU, PREVIO LOGIN: *https://www.federprivacy.org/strumenti/accesso-ristretto/se-le-violazioni-della-sicurezza-dipendono-da-scelte-del-fornitore-esterno-e-a-lui-che-vanno-applicate-le-sanzioni-previste-dal-gdpr*

ZOOM E SICUREZZA DEI MEETING: NUOVA CRITTOGRAFIA

Zoom ha deciso di adottare la **crittografia end-to-end post-quantum (E2EE)** per le riunioni all'interno della piattaforma Zoom Workplace, in risposta alla crescente sofisticazione delle minacce avversarie e al potenziale rischio futuro di compromissione dei dati criptati da parte del **quantum computing**, vale a dire quella tecnologia che sfrutta le leggi della meccanica quantistica per risolvere tutti quei problemi troppo complessi che i computer o i supercomputer classici non possono risolvere o non possono risolvere abbastanza rapidamente.

ARGOMENTO E TEMI TRATTATI
da Piermario Boccellato nell'articolo "Zoom introduce la crittografia end to end post-quantum per migliorare la sicurezza dei meeting": *https://www.key4biz.it/zoom-introduce-la-crittografia-end-to-end-post-quantum-per-migliorare-la-sicurezza-dei-meeting%ef%bf%bc/491387/*