



DH
CENTRO
INTERDIPARTIMENTALE
DI RICERCA

MEDITERRANEAN OBSERVATORY
MODICT
DIGITAL CULTURE & TOURISM
Centro di ricerca del Dipartimento
di Storia, Società e Studi sull'Uomo

ANDIG
Associazione Nazionale Docenti
Informatica Giuridica
e Diritto dell'Informatica



L'IA AVRÀ UNA FONDAZIONE TUTTA SUA

A completamento all'AI Act, approvato il mese scorso, il Governo italiano si avventura nel territorio normativo del momento, con il suo **disegno di legge**, approvato in CdM, sull'intelligenza artificiale (AI).

Di settore in settore, gli **enti pubblici** sono chiamati a favorire "la creazione di un mercato dell'intelligenza artificiale innovativo, equo, aperto e concorrenziale e di ecosistemi innovativi", anche attraverso uno specifico mercato degli appalti pubblici (di cui si fa solo cenno), e "facilitano la disponibilità e l'accesso a dati di alta qualità per le imprese che sviluppano o utilizzano sistemi di intelligenza artificiale e per la comunità scientifica e dell'innovazione".

Tra gli elementi innovativi del ddl troviamo la proposta di istituire una **Fondazione dedicata all'AI**, volta a supportare la ricerca, lo sviluppo e l'adozione di tecnologie AI etiche e sostenibili. Questa fondazione, sotto la vigilanza di **Palazzo Chigi** e in collaborazione con i ministeri dell'Economia, delle Finanze e dell'**Università e della Ricerca**, avrà il compito di attrarre investimenti, finanziare progetti innovativi e facilitare il trasferimento tecnologico dall'ambito accademico al settore privato.

La Fondazione sarà, inoltre, punto di riferimento per la **formazione e l'aggiornamento professionale**, contribuendo a mitigare gli effetti dell'automazione sui posti di lavoro. Sul fronte del **copyright**, infine, il dipartimento di Palazzo Chigi propone di obbligare media, piattaforme social e di streaming a inserire un **bollino** per riconoscere i contenuti dell'AI. E in materia di finanziamenti?

ARGOMENTO E TEMI TRATTATI

da Luisa Di Giacomo nell'articolo "Intelligenza artificiale: approvato in CdM il disegno di legge italiano": <https://www.diritto.it/intelligenza-artificiale-bozza-disegno-legge-italia/>

RICERCA UNIVERSITARIA VIOLA LA PRIVACY DI MINORI

Il Garante per la Protezione dei Dati Personali ha sanzionato l'Università La Sapienza di Roma per violazioni della normativa privacy, nell'ambito di un **progetto di ricerca condotto in una scuola primaria** su una classe di terza elementare.

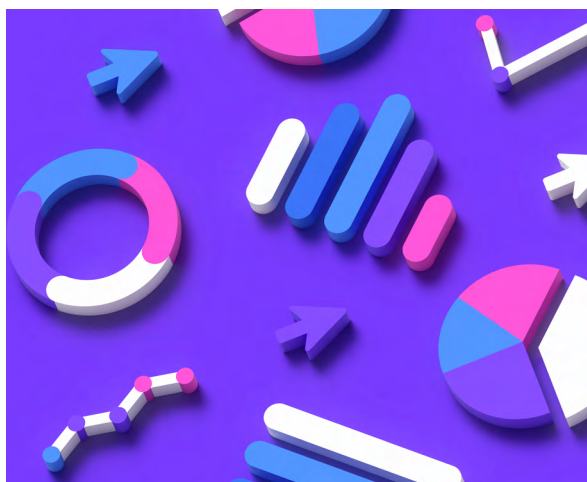
Nello specifico, per realizzare lo **studio sullo sviluppo delle competenze relazionali in età scolare**, erano stati somministrati a bambini di 7-8 anni questionari e colloqui che raccoglievano informazioni estremamente dettagliate e invasive sulla loro vita sessuale. Alcuni alunni ne erano rimasti turbati.

Numerose le criticità rilevate nel trattamento dei dati: l'Università non ha fornito un'adeguata informativa preventiva ai genitori, non ha acquisito un valido consenso per il trattamento di questi dati sensibilissimi relativi a minori, e non ha nemmeno designato formalmente la scuola come responsabile esterno del trattamento come previsto dal GDPR.

L'**informativa** fornita ai genitori è stata giudicata **carente sotto vari profili**, tra cui l'individuazione del titolare del trattamento, la tipologia di dati trattati, i tempi di conservazione e la chiara rappresentazione delle finalità, compromettendo l'autodeterminazione informativa.

Con il **provvedimento n. 136/2024**, l'Autorità ha quindi dichiarato illecita la condotta dell'Ateneo per violazione degli artt. 6, 9, 13 e 28 del Regolamento UE 2016/679, ammonendo La Sapienza in quanto titolare del trattamento.

La decisione ribadisce come **anche per fini di ricerca scientifica vadano rispettate tutte le garanzie previste in materia di privacy**, con particolare attenzione ai trattamenti di **dati sensibilissimi** relativi a minori d'età, che richiedono adeguate misure di sicurezza e il pieno consenso informato da parte degli esercenti la responsabilità genitoriale.



ARGOMENTO E TEMI TRATTATI

da Laura Biarella nell'articolo "In una scuola primaria test su informazioni relative alla vita sessuale degli alunni: genitori denunciano, interviene il Garante. Ecco cosa ha detto": <https://www.orizzontescuola.it/in-una-scuola-primaria-test-su-informazioni-relative-alla-vita-sessuale-degli-alunni-genitori-denunciano-interviene-il-garante-ecco-cosa-ha-detto/>



ARGOMENTO E TEMI TRATTATI

da Carla Ponti nell'articolo "No al risarcimento danni automatico per violazione del GDPR, ora lo dice anche la CGUE": <https://www.cybersecurity360.it/news/no-al-risarcimento-dei-danni-automatico-per-violazione-del-gdpr-ora-lo-dice-anche-la-cgue/>

NON BASTA LA VIOLAZIONE DEI DATI PER IL RISARCIMENTO

Con una importante sentenza dell'11 aprile 2024, la Corte di Giustizia dell'Unione Europea ha stabilito che una **violazione del GDPR non è sufficiente** di per sé a giustificare automaticamente una richiesta di risarcimento dei danni immateriali o morali.

La Corte ha ribadito che per poter avanzare una richiesta di questo tipo **occorre dimostrare la sussistenza di tre elementi**: 1. una violazione della normativa privacy; 2. l'esistenza di un danno effettivo (materiale o immateriale); 3. un nesso causale tra violazione e danno subito.

La sentenza rappresenta quindi un monito contro l'assimilazione troppo sbrigativa tra violazione della disciplina privacy e automatico risarcimento del danno, stabilendo che per quest'ultimo devono sempre ricorrere i medesimi presupposti richiesti in generale dall'istituto della responsabilità civile.

COMUNI, VIDEOSORVEGLIANZA, AI E PRIVACY: UN QUADRO SCONFORTANTE

Sono trascorsi quasi sei anni dell'entrata in operatività del **GDPR** e quattro dall'emanazione delle **Linee Guida n.3/2019**, del Comitato Europeo per la Protezione dei Dati, sul trattamento dei dati personali attraverso dispositivi video, ma l'**elevato numero di provvedimenti sanzionatori** effettuati dal Garante Privacy sul territorio italiano, lascia intravedere una sensibilità ancora carente, da parte dei **titolari del trattamento**, in tema di videosorveglianza, anche alla luce dell'interazione con l'intelligenza artificiale e con le problematiche connesse alla riservatezza.

ARGOMENTO E TEMI TRATTATI

da Emanuele Cofanelli nell'articolo "Videosorveglianza e privacy nei Comuni: attenzione alle sanzioni e all'Intelligenza Artificiale": <https://www.lentepubblica.it/pa-digitale/videosorveglianza-privacy-sanzioni-intelligenza-artificiale/>



ARRIVA L'IDENTITÀ DIGITALE EUROPEA: COSA CAMBIA PER LO SPID?

Il Parlamento europeo ha approvato il **nuovo regolamento eIDAS 2.0** sull'identità digitale. Entro il 2026 ogni Stato membro dovrà mettere a disposizione dei cittadini un **portafoglio digitale europeo** in grado di collegare l'identità digitale nazionale ad altri attributi come patente, qualifiche, conto bancario.

L'Italia procede su questa strada con l'**It Wallet**, il cui via libera è arrivato a fine febbraio. Dall'estate carta d'identità, tessera sanitaria, patente e altri documenti diventeranno digitali e accessibili tramite l'app IO, in una prima fase sperimentale.

Il nuovo regolamento europeo lascia aperti interrogativi sul **futuro di SPID**, visto che il governo sembra rivolto a diffondere maggiormente la CIE, che faciliterà il passaggio al portafoglio digitale europeo.

ARGOMENTO E TEMI TRATTATI

da Claudia Bertozzi nell'articolo "IT Wallet: che cos'è e come funzionerà il nuovo portafoglio di identità digitale": <https://www.forumipa.it/pa-digitale/it-wallet-che-cose-e-come-funzionera-il-nuovo-portafoglio-di-identita-digitale/>

IA NELLA PA, ABBIAMO IL "PIANO" PERFETTO?

Uno degli obiettivi principali del **Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026** è l'aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale utili a modernizzare e migliorare l'efficienza dei servizi pubblici incentrati sull'utente, seppur garantendo principi fondamentali come trasparenza, equità, non discriminazione, privacy e sicurezza nell'implementazione di soluzioni di IA da parte della Pubblica Amministrazione.

Tuttavia, serve anche un piano per far ripartire una industria nazionale dell'ICT e dell'IA stessa.

Servono un cambio di paradigma nella Pubblica Amministrazione e investimenti mirati, senza i quali le soluzioni di IA rischiano di essere meno efficaci per le specificità linguistiche e culturali italiane.



ARGOMENTO E TEMI TRATTATI

da Paolino Madotto nell'articolo "IA nella PA, cosa c'è e cosa manca nel Piano triennale 2024-2026": <https://www.agendadigitale.eu/cittadinanza-digitale/ia-nella-pa-strategie-e-obiettivi-del-piano-triennale-2024-2026-cosa-ce-cosa-manca/>



IA E PA, COSA NE PENSANO I DIPENDENTI PUBBLICI?

Sono **4 i pilastri** sui quali si fonda la **strategia 2024-2027** definita dall'European Data Protection Board (EDPB) durante l'ultima plenaria dello scorso 18 aprile: 1. Migliorare l'armonizzazione e promuovere la compliance; 2. Rafforzare una cultura comune per l'applicazione delle norme e una cooperazione efficace; 3. Salvaguardare la protezione dei dati nel panorama dell'evoluzione digitale ed interdisciplinare; 4. Contribuire al dialogo globale sulla protezione dei dati.

Secondo l'EDPB, questa nuova strategia è necessaria per rispondere alle esigenze odierne di protezione dei dati e al panorama digitale in continua evoluzione.

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

PNRR E DIGITALIZZAZIONE PA: SOGGETTI ATTUATORI, LE NOVITÀ

Gli aggiornamenti che riguardano i soggetti attuatori sono ora accessibili online e riguardano vari avvisi pubblici nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR), tra cui l'abilitazione al cloud per le Pa locali, l'esperienza del cittadino nei servizi pubblici, l'adozione dell'identità digitale e la digitalizzazione degli avvisi pubblici. Alcuni punti critici richiedono particolare attenzione.

PUBBLICATO SU: <https://www.lentepubblica.it/pa-digitale/pnrr-digitalizzazione-pa-linee-guida-soggetti-attuatori/>



DPO: SANZIONI IN CASO DI MANCATA COMUNICAZIONE DATI DI CONTATTO

Nelle Linee-guida sui Responsabili della Protezione dei Dati (RPD), si specifica che “L’articolo 37, settimo paragrafo, del Regolamento 2016/679 impone al Titolare o al Responsabile del trattamento di pubblicare i dati di recapito del RPD, e di trasmetterli alla pertinente Autorità di controllo. Queste disposizioni mirano a garantire che tanto gli interessati, quanto il Garante, possano contattare il RPD in modo facile e diretto senza doversi rivolgere a un’altra struttura operante presso il Titolare/Responsabile”.

Il 2024 è iniziato con **4 provvedimenti sanzionatori** (provvedimenti nn. 9979112, 9979128, 9979152, 9979171) adottati dal Garante Privacy nei confronti di altrettanti Enti Locali, a conclusione della prima fase di un’indagine avviata per verificare il rispetto dell’obbligo di comunicazione all’Autorità stessa dei dati di contatto del Responsabile per la Protezione dei Dati (RPD/DPO).

In tutti i provvedimenti sanzionatori l’Autorità ha ricordato che, **se il Titolare del trattamento dei dati personali è un soggetto pubblico, è obbligato a designare un RPD** e a comunicare i relativi dati attraverso l’apposita procedura messa a disposizione sul suo sito web.

FAQ relative alla procedura telematica per la comunicazione dei dati del RPD: <https://www.garanteprivacy.it/regolamentoue/rpd/faq-relative-alla-procedura-telematica-per-la-comunicazione-dei-dati>

PUBBLICATO SU:

<https://www.key4biz.it/mancata-comunicazione-dei-dati-di-contatto-del-rpd-le-sanzioni-del-garante-privacy/487499/>

VIOLA LA PRIVACY MANTENERE ATTIVA L’EMAIL DI UN EX DIPENDENTE

Il Garante per la protezione dei dati personali italiano, nel Provvedimento del 7 marzo 2024 [10009004], Registro dei provvedimenti n. 140 del 7 marzo 2024, ha comminato una sanzione amministrativa al Titolare del trattamento di un’azienda piacentina.

Quest’ultimo, infatti, aveva mantenuto attivi, “per diversi mesi oltre la cessazione dei rapporti lavorativi, con contestuale accesso ai messaggi ivi pervenuti”, gli account di posta elettronica aziendale di due ex dipendenti.

L’operazione illecita di trattamento, tra l’altro, ha portato alla condanna a ventimila euro di sanzione, con la facoltà di definire la controversia mediante il pagamento, entro i termini, di un importo pari alla metà della stessa.

ARGOMENTO E TEMI TRATTATI

da Domenico Battaglia nell’articolo “Mantenere attiva l’email aziendale dopo la cessazione del rapporto di lavoro per ‘garantire la continuità operativa’ viola la privacy dell’ex dipendente”: <https://www.federprivacy.org/informazione/primo-piano/mantenere-attivo-l-account-dell-email-aziendale-dopo-la-cessazione-del-rapporto-di-lavoro-per-garantire-la-continuita-operativa-viola-la-privacy-dell-ex-dipendente>