MONITORAGGIO NORMATIVO PRIVACY

ULTIME NOTIZIE DAL MONDO PRIVACY

Gentilissimi,
vogliamo condividere con voi le ultime notizie e i provvedimenti più significativi che riguardano il mondo Privacy. In un'epoca in cui la protezione dei dati personali è di cruciale importanza, è fondamentale rimanere costantemente aggiornati sulle ultime tendenze per affrontare con successo le sfide legate alla protezione dei dati e al loro uso responsabile.
Di seguito un estratto delle notizie.

Buona lettura!

I dipendenti in smartworking possono essere geolocalizzati?

"In data 13 marzo 2025 **il Garante per la Protezione dei Dati Personali ha sanzionato** l'Azienda regionale per lo sviluppo e per i servizi in agricoltura **(ARSAC) con una sanzione di 50.000** euro per il trattamento illecito dei dati relativi alla geolocalizzazione del personale in modalità agile, effettuato attraverso l'applicativo Time Relax.
Il Garante, nel corso dell'istruttoria, ha rilevato che **ARSAC**, tramite l'applicativo Time Relax, **chiedeva la posizione geografica dei dipendenti che lavoravano in modalità agile**, al fine di verificare se la loro posizione corrispondeva a quella prevista nell'accordo individuale. Nonostante ARSAC avesse ratificato l'impiego dell'applicativo di geolocalizzazione a mezzo di accordo sindacale, **tale monitoraggio non è consentito dalla normativa** per violazione **dell'art. 4 dello Statuto dei lavoratori**, che ammette solo controlli incidentali e preterintenzionali.
Secondo il Garante, **il trattamento è avvenuto in violazione dei principi di cui agli articoli 5, 13, 25 e 35 del GDPR**. Peraltro, ARSAC aveva individuato come base giuridica del trattamento l'atto amministrativo generale (ossia una deliberazione con in allegato il regolamento sul "Lavoro Agile", che prevedeva la geolocalizzazione), tuttavia il Garante ha evidenziato che tale base giuridica non è idonea, in quanto **gli atti amministrativi generali non possono derogare a norme sovraordinate,** quale è appunto lo Statuto dei Lavoratori (L. 300/1970).
Inoltre, il Garante ha sottolineato che il consenso richiesto ai dipendenti, per accedere alla loro posizione, non è una valida base giuridica, atteso che i dipendenti sono considerati soggetti vulnerabili, in considerazione dell'asimmetria contrattuale che viene in essere.
Infine, è stato considerato illecito l'utilizzo dei dati di localizzazione per fini disciplinari, perché **sono stati raccolti illegittimamente.**
Da tale provvedimento emerge, quindi, che il datore di lavoro non può geolocalizzare i dipendenti in smart working."

Per ulteriori approfondimenti, si rimanda al relativo link.

News Italia:

ACN: sicurezza per le infrastrutture critiche

"L'Agenzia per la Cybersicurezza Nazionale, con la determinazione 164179, ha delineato delle **specifiche tecniche** che dovranno essere implementate dalle organizzazioni per **conformarsi al decreto NIS 2**. In particolare, con tale determinazione, l'ACN definisce le **misure concrete** che i soggetti dovranno adottare per garantire la sicurezza dei propri sistemi informativi e stabilisce le tempistiche per l'adeguamento. **Il documento si basa sul "Framework Nazionale per la Cybersecurity e la Data Protection" (edizione 2025) e si compone di quattro allegati tecnici**:

- Allegato 1: Misure di sicurezza di base per i soggetti importanti;
- Allegato 2: Misure di sicurezza di base per i soggetti essenziali;
- Allegato 3: Specifiche per gli incidenti significativi di base per i soggetti importanti;
- Allegato 4: Specifiche per gli incidenti significativi di base per i soggetti essenziali.

La pubblicazione della determinazione segna un passo importante, **l'inizio di un percorso di adeguamento**."

Per ulteriori approfondimenti, si rimanda al relativo link.

Garante e Arma dei Carabinieri

"Il Garante per la Protezione dei Dati Personali e l'Arma dei Carabinieri hanno sottoscritto un protocollo d'intesa. Tale protocollo mira a rafforzare la collaborazione tra le due Istituzioni, attraverso **iniziative formative e operative**. In particolare, gli ambiti di collaborazione concernono due aspetti: **l'organizzazione di incontri rivolti ai giovani**, al fine di indirizzarli ad **uso consapevole e corretto del web e la realizzazione di progetti formativi**. L'Arma dei Carabinieri, al fine di favorire l'organizzazione degli incontri per i giovani, mette a disposizione i propri rappresentanti che illustrano gli **strumenti di tutela e di contrasto ai fenomeni di "Cyberbullismo" e di "Revenge Porn",** e divulga materiale informativo per promuovere la consapevolezza sui diritti delle vittime dei suddetti reati.
La sottoscrizione del protocollo assicura un'efficace prevenzione dei rischi correlati alle nuove tecnologie."

Per ulteriori approfondimenti, si rimanda al relativo link.

Obblighi per le PA nei contratti ICT

"Il 30 aprile 2025 è stato pubblicato sulla Gazzetta Ufficiale il DPCM n. 102 del 5 maggio 2025, con il quale entra in vigore una nuova **disciplina vincolante per le Pubbliche Amministrazioni** e i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica. In particolare, i**l decreto disciplina i contratti per la fornitura di beni e servizi ICT destinati a contesti critici e stabilisce gli elementi essenziali di cybersicurezza** che devono essere integrati nei capitolati e nelle specifiche di gara, al fine di uniformare i requisiti minimi in fase contrattuale e garantire la protezione delle infrastrutture strategiche nazionali da rischi informatici.
Da un punto di vista tecnico i prodotti ICT devono garantire i seguenti requisiti:

- **integrità, riservatezza e disponibilità delle informazioni;**
- **protezione da accessi non autorizzati;**
- **resilienza agli attacchi esterni** (inclusi attacchi DDoS), nonché funzionalità di aggiornamento automatico e di tracciabilità delle operazioni.

Particolare attenzione è dedicata al **requisito di "*secure by default*",** che impone la configurazione sicura per impostazione predefinita. Per la gestione delle vulnerabilità il decreto prevede l'obbligo per i fornitori di predisporre una distinta base del software (Software Bill of Materials – SBOM), **nonché obblighi in tema di correzione tempestiva in caso di problemi di sicurezza, comunicazione trasparente delle vulnerabilità, e valutazione del rischio lungo tutta la catena di fornitura."**

Per ulteriori approfondimenti, si rimanda al relativo link.

News Europa:

Spagna: sanzione di 500 mila euro per mancata gestione dei sub responsabili

"Una società che gestisce servizi sanitari, e tratta dati sanitari per conto della pubblica amministrazione, è stata sanzionata **dall'Agenzia spagnola per la protezione dei dati per un ammontare pari a 500 mila euro**. La sanzione è stata irrogata per una **mancata gestione dei sub responsabili, in violazione dell'articolo 28 del GDPR**. Invero, la società aveva sottoscritto tre contratti con fornitori di soluzioni IT per la realizzazione di un software di gestione dei pazienti e per l'informatizzazione del laboratorio di analisi. Del ricorso a tali sub responsabili, la società, non ha informato il titolare del trattamento. **La mancata comunicazione rappresenta una violazione procedurale**, e pone l'accento sull'importanza di una corretta governance e compliance organizzativa. L'articolo 28 del GDPR, infatti, impone che **ogni responsabile del trattamento informi preventivamente il titolare dell'intenzione di ricorrere ad un altro sub responsabile** in quanto, in assenza di tale comunicazione, il titolare non può verificare la conformità dei contratti stipulati con terze parti. Nel caso di specie la violazione risulta essere aggravata dalla natura dei dati trattati, ossia dati sanitari per i quali il GDPR prevede un livello di protezione maggiore."

Per ulteriori approfondimenti, si rimanda al relativo link.

Intelligenza artificiale: piano d'azione per il continente dell'IA

"Il piano d'azione dell'IA, della Commissione Europea, mira a **promuovere l'intelligenza artificiale in Europa e a sfruttarne il potenziale** in diverse aree, come l'assistenza sanitaria, la ricerca e tanti altri ambiti.
Il piano d'azione si pone l'obiettivo di:

- aumentare **l'accesso ad un gran numero di dati**;
- **creare 13 fabbriche di IA in tutta Europa,** per promuovere lo sviluppo di modelli e applicazioni di IA all'avanguardia;
- **istituire 5 *gigafactory* di IA**, ossia impianti che operano su larga scala e che sono in grado di addestrare modelli di IA complessi;
- **promuovere l'intelligenza artificiale nei settori strategici**;
- **rafforzare le competenze in materia IA**."

Per ulteriori approfondimenti, si rimanda al relativo link.

Polonia: videosorveglianza e misure di sicurezza

"L'Autorità Garante Polacca ha imposto, ad un Centro medico, **una sanzione di 262 500 euro**, per violazione delle disposizioni dettate **in materia di videosorveglianza e misure di sicurezza**.
In particolare, il Centro medico con sede a Cracovia, a luglio del 2023, nel reparto di neonatologia, ha registrato delle immagini che mostravano i neonati e le loro madri mentre svolgevano attività intime.
A seguito di un **furto o smarrimento** delle schede di memoria dei dispositivi di registrazione video nelle due sale del reparto di neonatologia, **il Centro medico ha notificato all'Autorità la violazione.**
I pazienti e i dipendenti non erano a conoscenza di tale videosorveglianza, e inoltre, nel corso delle indagini, è emerso che non erano state adottate adeguate misure di sicurezza. Infatti, le schede di memoria che contenevano le registrazioni non erano state criptate, e l'analisi dei rischi fornita dal Centro non identificava le misure di sicurezza che avrebbero potuto evitare l'incidente."

Per ulteriori approfondimenti, si rimanda al relativo link.