30-31

DICEMBRE 2023
GENNAIO 2024

NEWSADP

NEWSLETTER SU AMMINISTRAZIONE DIGITALE E PRIVACY
A CURA DEL PROF. AVV. MARCO MANCARELLA DI CONCERTO CON LA RITT

www.liquidlaw.it
@liquidlawsrl
liquidlaw

liquid LAW
spin-off
UniSalento 2018-22

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

CYBERSICUREZZA: SEGNALAZIONE ENTRO LE 24 ORE. MA, I FONDI?

Il governo italiano sta introducendo **misure stringenti** per **migliorare la cybersicurezza** nella **Pubblica Amministrazione**. Un nuovo disegno di legge, attualmente in fase di approvazione, richiede che entità come Comuni, Regioni, ASL e aziende di trasporto pubblico segnalino attacchi informatici all'Agenzia per la Cybersicurezza Nazionale **entro 24 ore**, **fornendo una notifica completa entro 72 ore** dalla stessa data. La **mancata segnalazione** comporta multe **da 25.000 a 125.000 euro**.

Inoltre, la legge propone una revisione dell'articolo 615-ter del codice penale, inasprendo le pene per i cybercriminali, con reclusione da due a dieci anni, e fino a dodici anni in caso di danni gravi. Tuttavia, offre agevolazioni a quegli hacker che collaborano con le autorità, consentendo una riduzione della pena da metà a due terzi per chi aiuta nella raccolta di prove o nel recupero dei proventi dei reati. Queste misure rappresentano un passo significativo verso il rafforzamento della sicurezza informatica nazionale.

Il DDL introduce una **figura chiave** nell'ambito delle **Pubbliche Amministrazioni: il referente per la cybersicurezza**. La valorizzazione l'intelligenza artificiale come risorsa chiave per il potenziamento della cybersicurezza nazionale, al contrario, è rimasta esclusa dall'approvazione nel Consiglio dei Ministri.

Però **mancano i fondi**. Pertanto, il Governo ha previsto che "le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente".

ARGOMENTO E TEMI TRATTATI
da Andrea Tironi nell'articolo "DDL Cybersicurezza: ambizioni alte, ma mancano i fondi": *https://www.agendadigitale.eu/sicurezza/ddl-cybersicurezza-ambizioni-alte-ma-mancano-i-fondi/*

PUBBLICATO SU: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020*

CHATGPT: OPENAI ACCUSATA DI VIOLARE LA NORMATIVA PRIVACY

Il Garante privacy italiano ha notificato a OpenAI un **atto di contestazione** per aver violato la normativa in materia di protezione dei dati personali.

A seguito del provvedimento di limitazione provvisoria del trattamento, adottato dal Garante nei confronti della Società lo scorso 30 marzo, e all'esito dell'**istruttoria svolta**, l'Autorità ha ritenuto che gli elementi acquisiti possano configurare uno o più illeciti rispetto a quanto stabilito dal Regolamento UE.

OpenAI, che gestisce la piattaforma di intelligenza artificiale ChatGPT, **avrà 30 giorni** per comunicare le proprie memorie difensive in merito alle presunte violazioni contestate.

GDPR: NO ALLA RESPONSABILITÀ OGGETTIVA DELL'ORGANIZZAZIONE

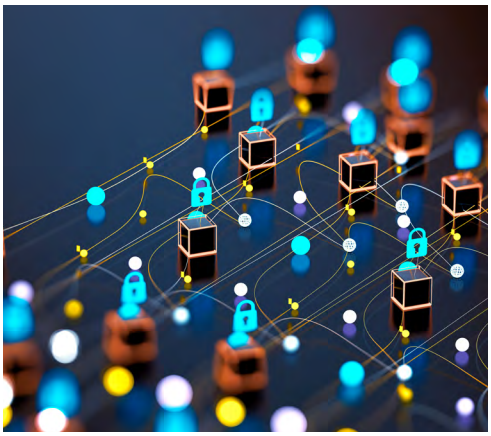
La **sentenza del 5 dicembre 2023 della Corte di giustizia dell'Unione Europea**, caso n. C-807/21, stabilisce che le organizzazioni (imprese, enti pubblici o privati) sono responsabili per le violazioni della privacy, indipendentemente dall'identificazione del singolo autore dell'infrazione (come un dipendente). Questo principio, che responsabilizza le organizzazioni come titolari o responsabili del trattamento dei dati, esclude la responsabilità oggettiva, ossia senza colpa. Pertanto, per applicare le sanzioni è necessario dimostrare che la violazione è stata commessa con dolo o colpa.

La sentenza fa riferimento a un **caso in Germania** riguardante una holding immobiliare, sanzionata dal garante della privacy tedesco per trattamenti illegittimi dei dati. Il principio invocato dalla holding, tuttavia, è stato respinto dalla Corte, affermando che è **possibile sanzionare una persona giuridica anche in assenza di un colpevole individuato**.

PUBBLICATO SU previo login: *https://www.federprivacy.org/strumenti/accesso-ristretto/la-colpa-per-la-violazione-della-privacy-ricade-sull-organizzazione-anche-se-non-e-identificata-la-singola-persona-che-l-ha-causata*

La **Corte di Cassazione italiana** si è espressa in termini simili, sottolineando che la **responsabilità delle organizzazioni non è automatica, ma deriva dalla "colpa di organizzazione"**, ossia dalla mancata adozione delle misure necessarie a prevenire gli illeciti. Le organizzazioni, quindi, devono dotarsi di un sistema di controllo e di un apparato documentale dettagliato per dimostrare che eventuali illeciti commessi dai dipendenti siano stati agiti per fini personali e non nell'ambito delle scelte gestionali.

Inoltre, la sentenza chiarisce che in caso di estinzione del titolare del trattamento, come una società, la sanzione non può essere trasferita ai soci o al liquidatore, conformemente all'articolo 7 della legge 689/1981. Questo implica che la responsabilità per violazioni della privacy ricade sull'ente stesso e non può essere trasferita a seguito della sua estinzione.



ARGOMENTO E TEMI TRATTATI
da Patrizia Licata nell'articolo "Cybersecurity, accordo tra gli Stati Ue sulla "solidarietà informatica"i": *https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-accordo-tra-gli-stati-ue-sulla-solidarieta-informatica/*

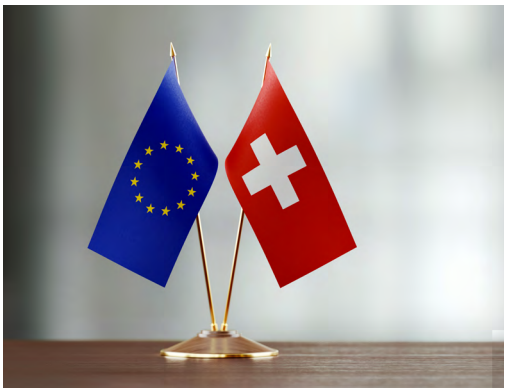
UE: ACCORDO SOLIDARIETÀ INFORMATICA

Un passo importante verso la cybersecurity quello fatto dall'Unione Europea con il "**Cyber Solidarity Act**". Questo regolamento, concordato dai rappresentanti degli Stati membri (Coreper), intende rendere l'Europa più resiliente e pronta a fronteggiare le minacce cibernetiche.

Il cuore di questo accordo è l'istituzione dello "**scudo informatico europeo**" (European cyber shield), una struttura paneuropea che include i centri operativi di sicurezza (Soc) di tutta l'UE. Inoltre, verrà creato un **meccanismo di emergenza cibernetica** e una **riserva di cybersecurity** dell'UE, con la partecipazione di fornitori privati affidabili, pronti a intervenire in caso di attacchi su vasta scala.

Il progetto prevede anche il rafforzamento del ruolo dell'Enisa (Agenzia dell'UE per la Sicurezza Informatica) nello studio e nella revisione degli attacchi cibernetici.

Queste misure mirano a rilevare rapidamente le minacce informatiche e a garantire una risposta efficace in caso di incidenti gravi.



UE VALIDA LA LEGGE SVIZZERA SULLA PRIVACY

Il **15 gennaio scorso**, la Commissione europea ha riconosciuto la nuova legge federale svizzera sulla protezione dei dati (nLPD) come equivalente al Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea (UE).

Il riconoscimento assicura che **i dati personali trasferiti dall'UE alla Svizzera** ricevano adeguate garanzie di protezione. Quindi, i dati personali possono essere trasferiti dall'UE alla Svizzera senza la necessità di ulteriori garanzie oltre a quelle fornite dalla nLPD. Tale decisione è significativa per la Svizzera, in quanto garantisce la continuazione del trasferimento agevole dei dati transfrontalieri, essenziale per la piazza economica e la competitività del paese.

La nLPD è stata approvata nell'autunno del 2020 dopo tre anni di dibattiti e mira a essere compatibile con il diritto comunitario europeo.

Il **report della Commissione UE** sottolinea l'**alto livello di adeguatezza della legislazione svizzera in termini di protezione dei dati**, permettendo così alla Svizzera di mantenere standard elevati nella salvaguardia dei dati personali. Questo riconoscimento è fondamentale per facilitare le attività economiche e mantenere la competitività della Svizzera nel contesto europeo e globale.

PUBBLICATO SU: *https://www.federprivacy.org/informazione/mondo/l-ue-riconosce-come-adeguata-al-gdpr-la-legge-svizzera-sulla-protezione-dei-dati*

VALORIZZARE I RPD, NUOVE STRATEGIE DEL COMITATO EUROPEO

Il Comitato europeo per la protezione dei dati ha recentemente pubblicato una relazione che evidenzia le **aree di miglioramento** necessarie per **valorizzare il ruolo dei Responsabili della Protezione dei Dati** (RPD). Questo documento, frutto di un'azione coordinata a livello UE, mette in luce vari ostacoli affrontati dagli RPD e propone raccomandazioni per rafforzare la loro posizione.

La Relazione è stata compilata grazie a un'indagine UE, in cui sono state **coinvolte 25 autorità di protezione dei dati dello Spazio economico europe**o. Attraverso un'analisi di oltre 17.000 risposte raccolte da vari settori, il report offre una panoramica approfondita della situazione degli RPD, mettendo in luce le sfide che incontrano cinque anni dopo la piena applicazione del GDPR.

Gli **ostacoli principali identificati** includono la mancanza di nomina di un RPD, risorse e competenze insufficienti, e la mancanza di indipendenza e coinvolgimento nei processi decisionali. Inoltre, è stato osservato che, in molti casi, i RPD non riportano direttamente ai vertici gerarchici, ma sono subordinati ad altre funzioni aziendali.

Questa relazione sottolinea l'**importanza cruciale dei RPD** nel garantire il rispetto delle normative sulla protezione dei dati e nella tutela dei diritti dei cittadini, evidenziando che il loro ruolo va ben oltre un semplice adempimento burocratico e costituisce una risorsa fondamentale per le organizzazioni.

PUBBLICATO SU: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9975545*

PUBBLICATO SU: *https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2024/01/15/appalti-innovativi-firmato-laccordo-collaborazione-listituto-poligrafico-dello*

ACCORDO AGID-IPZS PER APPALTI TECNOLOGICI INNOVATIVI

Il 15 gennaio 2024, l'Agenzia per l'Italia Digitale (AgID) e l'Istituto Poligrafico Zecca dello Stato (IPZS) hanno firmato un accordo esecutivo per dare il via a un progetto di collaborazione.

Questo accordo prevede la realizzazione di un appalto innovativo finalizzato allo **sviluppo di soluzioni tecnologiche avanzate per documenti e contrassegni**. L'obiettivo principale è quello di ideare e sviluppare soluzioni innovative basate su elementi di sicurezza fisici, autenticati tramite applicazioni di validazione come mobile e web app. Queste soluzioni hanno lo scopo di **contrastare le tecniche di falsificazione e contraffazione in continua evoluzione**.

GUIDA OPERATIVA PER DATI AD ALTO VALORE

Il 22 dicembre 2023, l'Agenzia per l'Italia Digitale ha pubblicato una Guida operativa dedicata alle serie di dati di elevato valore, destinata alle Pubbliche Amministrazioni (PA).

A partire dal **9 giugno 2024**, infatti, **i dati di elevato valore dovranno essere disponibili gratuitamente come open data**, accessibili tramite API e download in blocco.

I "dati di elevato valore" sono definiti dalla **Direttiva Open Data (UE) 2019/1024** come dati che, se riutilizzati, possono apportare benefici significativi alla società, all'ambiente e all'economia. La Direttiva classifica questi dati in sei categorie: Dati **geospaziali**, Dati **ambientali**, Dati **meteorologici**, Dati **statistici**, Dati **aziendali** e Dati sulla **mobilità**.

L'**obiettivo del documento** è quello di fornire **indicazioni dettagliate alle Amministrazioni per una migliore implementazione del Regolamento e supportarle nell'apertura di questi dati specifici**. Il documento offre un'analisi dello stato attuale nella pubblicazione e riutilizzo dei dati, proponendo miglioramenti tecnici e giuridici per ottimizzare il processo e aumentare la disponibilità di questi dati preziosi.

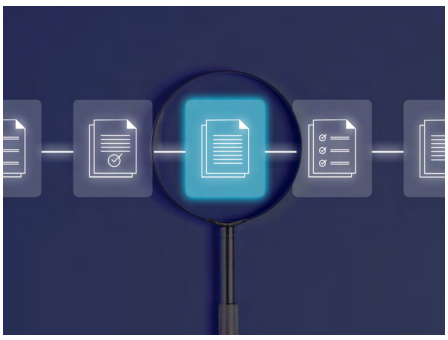
La guida si inserisce nell'**aggiornamento 2022-2024 del Piano Triennale per l'Informatica nella Pubblica Amministrazione** e contribuisce agli sforzi europei per armonizzare l'identificazione e la gestione dei dati di elevato valore, in linea con le iniziative a livello europeo, come evidenziato dallo studio "***Report on Data Homogenisation for High-value Datasets***" disponibile sul portale europeo dei dati.

PUBBLICATO SU: *https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/12/22/open-data-online-guida-operativa-sui-dati-elevato-valore*

FVOE 2.0: INNOVAZIONE NELLE GARE PUBBLICHE

Il Fascicolo Virtuale dell'Operatore Economico (FVOE) versione 2.0, ora pienamente operativo sul sito dell'ANAC, è uno strumento essenziale per la partecipazione alle procedure di gara pubblica **a partire dal 1° gennaio 2024**. Numerose le innovazioni.

Il FVOE 2.0 permette agli **Operatori Economici** di creare un *repository* personale con i documenti necessari per l'affidamento di contratti pubblici. Allo stesso tempo, le **Stazioni Appaltanti** possono acquisire la documentazione necessaria per verificare i requisiti degli operatori. Questo aggiornamento rappresenta un passo significativo verso la **digitalizzazione e l'efficienza nelle procedure di gara pubblica**, garantendo **maggiore trasparenza e facilità di accesso** alle informazioni rilevanti.



PUBBLICATO SU: *https://www.orizzontescuola.it/fascicolo-virtuale-delloperatore-economico-su-anac-pienamente-operativa-la-versione-2-0-le-novita/*

VIDEOSORVEGLIANZA, SANZIONATO IL COMUNE DI TRENTO

Marvel e Protector, i nomi dei progetti di ricerca scientifici al centro della sanzione pari a 50.000 euro, che il Garante privacy italiano ha comminato al Comune di Trento, chiamato altresì a cancellare i dati trattati in violazione di legge.

Dei due progetti, nati con l'obiettivo lo sviluppo di soluzioni tecnologiche volte a migliorare la sicurezza in ambito urbano, secondo il paradigma delle "città intelligenti" (smart cities), il **primo** prevedeva l'**acquisizione di filmati dalle telecamere di videosorveglianza** - già installate nel territorio comunale per finalità di sicurezza urbana, nonché dell'**audio** ottenuto da microfoni appositamente collocati sulla pubblica via. A detta del Comune, i dati - che sarebbero stati immediatamente anonimizzati dopo la raccolta - venivano analizzati per rilevare in maniera automatizzata, mediante tecniche di Intelligenza Artificiale, eventi di rischio per la pubblica sicurezza.

Il **secondo progetto**, invece, prevedeva oltre all'acquisizione dei filmati di videosorveglianza (senza segnale audio), la raccolta e l'analisi di messaggi e commenti d'odio pubblicati sui social, rilevando eventuali emozioni negative ed elaborando informazioni d'interesse per le Forze dell'ordine, allo scopo di identificare rischi e minacce per la sicurezza dei luoghi di culto.

Dopo un'**approfondita istruttoria**, tuttavia, il Garante ha rilevato **molteplici violazioni della normativa privacy**.

PUBBLICATO SU: *https://dirittodellinformazione.it/videosorveglianza-no-allintelligenza-artificiale-che-viola-la-privacy/*