FIVERS

Aggiornamento
Data protection, AI, IT e IP

n. 7 / 2024

DATA PROTECTION

25 luglio 2024 - Commissione UE: pubblicato il secondo rapporto sull'applicazione del GDPR.

---

25 Luglio 2024 – Corte di Giustizia UE: anche l'omessa informativa privacy è una violazione che abilita le associazioni rappresentative a ricorrere -anche senza mandato dell'interessato – ai sensi dell'articolo 80, comma 2, del GDPR.

---

22 Luglio 2024 – Modello "pay or consent": la Commissione UE coordina l'intervento delle autorità nazionali per la tutela dei consumatori nei confronti di Meta.

---

22 Luglio 2024 – Interactive Advertising Bureau (IAB) Europe: pubblicato un rapporto completo sugli aspetti critici della proposta di Regolamento procedurale del GDPR.

---

22 Luglio 2023 - Il Garante privacy avvia accertamenti sugli effetti del blocco informatico Crowdstrike.

---

18 Luglio 2024 – Consiglio d'Europa: pubblicata la versione in lingua araba del "Manuale sul diritto europeo in materia di protezione dei dati".

INTELLIGENZA ARTIFICIALE.

22 Luglio 2024 – La Commissione UE ha pubblicato la bozza del Patto per l'IA.

---

22 Luglio 2024 - Pubblicato il documento completo della Strategia Italiana per l'Intelligenza Artificiale 2024-2026.

---

22 Luglio 2024 – L'OCSE avvia la fase pilota per monitorare l'applicazione del Codice di condotta internazionale per le organizzazioni che sviluppano sistemi di intelligenza artificiale.

CYBERSECURITY

26 Luglio 2024 - L'Agenzia per la Cybersicurezza Nazionale pubblica la guida alla notifica al CSIRT Italia degli incidenti informatici.

---

22 Luglio 2024 – L'Agenzia per la Cybersicurezza Nazionale aggiorna le linee guida sulla crittografia.

INFORMATION TECHNOLOGY

26 Luglio 2024 – Ministero della Giustizia: attiva la piattaforma elettronica per la raccolta delle firme digitali valevoli per la sottoscrizione digitale dei referendum abrogativi o costituzionali e delle iniziative legislative di natura popolare.

---

26 Luglio 2024 - L'Organizzazione Mondiale per il Commercio – WTO adotta un Accordo sul Commercio Elettronico.

DATA PROTECTION

25 luglio 2024 - Commissione UE: pubblicato il secondo rapporto sull'applicazione del GDPR.

La Commissione europea ha sollevato rilevanti questioni e segnalato non poche criticità di applicazione del Regolamento generale sulla protezione dei dati (GDPR) e ha chiesto linee guida più chiare per rafforzare la protezione dei dati negli Stati membri nel secondo rapporto pubblicato.

Si tratta della seconda relazione della Commissione europea sull'applicazione del GDPR, in vigore dal 2018. Il rapporto periodico è richiesto ogni quattro anni, a partire dal 2020, e la Commissione UE pubblica revisioni del GDPR per identificare eventuali problemi applicativi, in vista di possibili modifiche del regolamento. Il primo rapporto sul GDPR è del 2020.

In particolare, la relazione ha evidenziato un aumento significativo dell'attività di applicazione delle norme da parte delle autorità di protezione dei dati negli ultimi anni, comprese le sanzioni pecuniarie per:

- la violazione della liceità e della sicurezza del trattamento;
- la violazione del trattamento di categorie particolari di dati personali; e
- il mancato rispetto dei diritti delle persone.

Per quanto riguarda le autorità di protezione dei dati, la relazione ha rilevato l'aumento delle risorse per le autorità di protezione dei dati in termini di bilancio e personale. Tuttavia, è stato notato che le autorità per la protezione dei dati hanno difficoltà a gestire un numero elevato di reclami dei consumatori e adottano interpretazioni divergenti del GDPR. Il rapporto ha inoltre evidenziato una applicazione frammentaria del GDPR in aree quali l'età minima per il consenso di un minore, l'introduzione di ulteriori condizioni per il trattamento di dati genetici, dati biometrici e dati sanitari e il trattamento di dati personali relativi a condanne penali e reati.

Per quanto riguarda i diritti degli interessati, la relazione ha rilevato che il diritto di accesso è il diritto esercitato più frequentemente dagli interessati, anche se permangono difficoltà nell'interpretazione quando le richieste sono infondate o eccessive. E' poi incrementato l'esercizio del diritto alla portabilità dei dati, facilitato dall'obbligo, previsto dalla legge sui mercati digitali (DMA) per i "gatekeeper" di fornire un'effettiva portabilità dei dati degli utenti. Per quanto riguarda l'esercizio dei diritti degli interessati da parte dei minori, la relazione ha concluso che i minori non comprendono appieno i loro diritti.

Sono state altresì analizzate le sfide in materia di protezione dei dati affrontate dalle piccole e medie imprese (PMI) e in tale settore è stato evidenziato che parecchi problemi permangono per quanto riguarda il ruolo del responsabile della protezione dei dati (DPO), tra cui:

- nomina di DPO con la necessaria esperienza;
- mancanza di norme a livello dell'UE per l'istruzione e la formazione;
- mancata integrazione adeguata dei DPO;
- mancanza di risorse;
- altri compiti al di fuori della protezione dei dati; e
- insufficiente seniority.

La seconda relazione prende poi in considerazione il panorama del trasferimento dei dati, riconoscendo che le decisioni di adeguatezza della Commissione UE hanno facilitato i flussi internazionali dei dati. La relazione ha rilevato che le decisioni di adeguatezza adottate dalla Commissione sono sempre più rilevanti in quanto le giurisdizioni con uno status adeguato sono riconosciute anche da altre giurisdizioni come destinazioni sicure ai sensi delle proprie norme in materia di protezione dei dati. Sebbene la relazione riconosca che gli esportatori di dati hanno difficoltà a gestire le valutazioni d'impatto sui trasferimenti, le clausole contrattuali standard dell'UE e le norme vincolanti d'impresa sono ancora ampiamente utilizzate. L'adozione di clausole modello da parte di altre giurisdizioni ha infine aumentato la portata dei flussi transfrontalieri di dati.

Le raccomandazioni conclusive della seconda relazione per garantire una rafforzata protezione delle persone fisiche e assicurare la libera circolazione dei dati personali all'interno e all'esterno dell'UE, insistono, tra l'altro, sui seguenti aspetti:

- supporto proattivo da parte delle autorità di protezione dei dati;
- applicazione coerente del GDPR in tutta l'UE;
- cooperazione efficace tra le autorità di protezione dei dati;
- instaurare una cooperazione con le autorità di regolamentazione settoriali su questioni che hanno un impatto sulla protezione dei dati.

La relazione 2024 potrebbe portare finalmente a modifiche effettive del GDPR, ma non è chiaro quanto queste saranno sostanziali o se ci si limiterà a suggerire al Comitato europeo per la protezione dei dati personali l'adozione di nuove linee guida.

---

25 Luglio 2024 – Corte di Giustizia UE: anche l'omessa informativa privacy è una violazione che abilita le associazioni rappresentative a ricorrere -anche senza mandato dell'interessato – ai sensi dell'articolo 80, comma 2, del GDPR.

Il Bundesgerichtshof (Corte federale di giustizia, Germania) ha sollevato presso la CGUE una questione pregiudiziale relativa all'interpretazione dell'articolo 80, paragrafo 2, del GDPR. Conformemente a tale disposizione, gli Stati membri possono prevedere che un organismo, organizzazione o associazione, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, nello Stato membro in questione, un reclamo all'autorità di controllo, ai sensi dell'articolo 77 del GDPR, e di esercitare i diritti di cui agli articoli 78 e 79 dello stesso, qualora ritenga che i diritti di cui un interessato gode a norma di tale regolamento siano stati violati in "*seguito al trattamento di dati personali*".

La domanda di pronuncia pregiudiziale era stata presentata nell'ambito di una controversia in Germania tra Meta e l'Unione federale delle organizzazioni e associazioni di consumatori tedeschi in merito all'asserita violazione, da parte di Meta Platforms Ireland, della normativa tedesca in materia di protezione dei dati personali, che costituisce, allo stesso tempo, una pratica commerciale sleale, una violazione di una legge in materia di protezione dei consumatori e una violazione del divieto di utilizzazione di condizioni generali di contratto nulle.

Nell'ambito di tale ricorso, il giudice del rinvio ha espresso dubbi in merito alla ricevibilità dell'azione dell'Unione federale. Esso si chiedeva, in particolare, se la legittimazione ad agire dell'Unione federale potesse derivare dall'articolo 80, paragrafo 2, del RGPD anche in caso di semplice omissione da parte del titolare del trattamento di rendere l'informativa sul trattamento ai sensi degli articoli 12 e 13 del GDPR. È per tale ragione ha sottoposto alla Corte di Giustizia una questione pregiudiziale al fine di un'interpretazione di detta disposizione.

La CGUE ha concluso che l'articolo 80, comma 2 del HGDPR deve essere interpretato nel senso che la condizione secondo cui un ente legittimato, per poter proporre un'azione rappresentativa in forza di tale disposizione, deve far valere di ritenere che i diritti di un interessato previsti da tale regolamento siano stati violati «in seguito al trattamento», ai sensi di detta disposizione, è soddisfatta qualora tale ente faccia valere che la violazione dei diritti di tale persona interviene "in occasione di un trattamento" di dati personali e che essa deriva dall'inadempimento dell'obbligo incombente al titolare del trattamento ai sensi dell'articolo 12, paragrafo 1, prima frase, e dell'articolo 13, paragrafo 1, lettere c) ed e), di detto regolamento, di comunicare all'interessato da tale trattamento di dati, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, le informazioni relative alla finalità di tale trattamento di dati nonché ai destinatari di tali dati, al più tardi al momento della raccolta di questi ultimi.

---

22 Luglio 2024 – Modello "pay or consent": la Commissione UE coordina l'intervento delle autorità nazionali per la tutela dei consumatori nei confronti di Meta.

La rete di cooperazione per la tutela dei consumatori (CPC) ha inviato una lettera a Meta per esprimere preoccupazioni sulla possibilità che il modello "pay or consent" violi il diritto dell'UE sulla tutela dei

consumatori, in un'azione coordinata dalla Commissione UE e guidata dalla Direzione Generale francese per la Concorrenza, i consumatori e la lotta antifrode (DGCCRF). L'azione è stata avviata nel 2023, subito dopo che Meta aveva chiesto da un giorno all'altro ai consumatori di scegliere se abbonarsi e pagare per usare Facebook e Instagram oppure accettare che l'azienda usasse i loro dati personali per mostrare annunci personalizzati, traendone profitto ("pay or consent").

Le autorità per la tutela dei consumatori hanno esaminato diversi elementi che potevano costituire pratiche ingannevoli o aggressive, verificando in particolare se Meta avesse fornito fin da subito ai consumatori informazioni veritiere, chiare e sufficienti che consentissero di valutare in che modo la decisione di pagare o accettare il trattamento dei dati personali a fini commerciali avrebbe influito sui loro diritti di consumatori. Le autorità della rete CPC temono inoltre che molti consumatori possano essere stati esposti a pressioni indebite e si siano sentiti costretti a scegliere in fretta tra i due modelli, temendo di perdere immediatamente l'accesso ai loro account e alla loro rete di contatti.

L'azione coordinata della rete CPC nei confronti di Meta si aggiunge ad altre procedure europee e nazionali in corso relative allo stesso modello. Si concentra nello specifico sulla valutazione delle pratiche di **Meta** ai sensi del diritto UE in materia di tutela dei consumatori ed è distinta dalle indagini in corso volte a valutare se il modello "pay or consent" violi il regolamento sui mercati digitali, dalla richiesta formale di informazioni nell'ambito del regolamento sui servizi digitali e dalla valutazione della commissione irlandese per la protezione dei dati a norma del regolamento generale per la protezione dei dati (GDPR).

Nel contesto dell'introduzione del nuovo modello commerciale di Meta, le autorità CPC hanno individuato diverse pratiche che destano preoccupazione e che potrebbero essere considerate sleali e contrarie alla direttiva sulle pratiche commerciali sleali e alla direttiva sulle clausole contrattuali abusive:

- uso fuorviante del termine "gratis", a fronte del fatto che gli utenti che non desiderano abbonarsi e pagare sono obbligati ad accettare che Meta possa guadagnare usando i loro dati personali per mostrare loro annunci personalizzati;
- utenti confusi perché costretti a navigare tra diverse schermate delle app o della versione web di Facebook e Instagram e a cliccare su link che portano a diverse parti delle condizioni di servizio o dell'informativa sulla privacy per scoprire in che modo Meta userà le loro preferenze, i loro dati personali e i dati da essi stessi generati per mostrare annunci personalizzati;
- uso di un linguaggio e di termini imprecisi, per esempio "le tue informazioni" per riferirsi ai "dati personali" dei consumatori, o tali da suggerire che i consumatori che decidono di pagare non vedranno nessun annuncio, anche se potrebbero ancora vederne quando interagiscono con contenuti condivisi tramite Facebook o Instagram da altri membri della piattaforma;
- pressione sui consumatori che hanno sempre usato Facebook e Instagram gratis prima dell'introduzione del nuovo modello commerciale e per i quali i due social network sono parte integrante della loro vita sociale e delle loro interazioni affinché compiano una scelta immediata, impedendo loro di accedere ai loro account prima di scegliere e senza quindi dare loro un preavviso, tempo sufficiente e una reale opportunità per valutare in che modo la scelta potrebbe influire sulla relazione contrattuale con Meta.

Meta ha tempo fino al 1º settembre 2024 per rispondere alla lettera della rete CPC e della Commissione UE e proporre soluzioni. Se Meta non interverrà per fugare le preoccupazioni espresse nella lettera, le autorità CPC possono decidere di adottare misure di esecuzione, anche di tipo sanzionatorio.

---

22 Luglio 2024 – Interactive Advertising Bureau (IAB) Europe: pubblicato un rapporto completo sugli aspetti critici della proposta di Regolamento procedurale del GDPR.

L'Interactive Advertising Bureau (IAB) Europe ha pubblicato un rapporto che solleva preoccupazioni significative in merito alle posizioni del Parlamento europeo e del Consiglio europeo sul regolamento procedurale del Regolamento generale sulla protezione dei dati (GDPR), tra cui:

- la necessità di meccanismi di risoluzione tempestiva e di ammissibilità dei reclami per accelerare la risoluzione dei reclami e ridurre i ritardi amministrativi, che attualmente stanno causando notevoli arretrati;

- l'importanza di mantenere il meccanismo dello sportello unico, che garantisce un'applicazione coerente del regolamento generale sulla protezione dei dati in tutte le diverse giurisdizioni;
- preoccupazioni per l'indebolimento delle tutele in materia di riservatezza delle informazioni commerciali, che potrebbe portare a fughe di notizie e compromettere l'indipendenza delle autorità di vigilanza; e
- la necessità di garantire un'applicazione uniforme del diritto di essere ascoltati in tutta Europa, consentendo alle parti indagate di esprimere efficacemente le loro opinioni durante i procedimenti amministrativi ed evitare l'incertezza giuridica.

---

22 Luglio 2023 - Il Garante privacy avvia accertamenti sugli effetti del blocco informatico Crowdstrike.

Il Garante per la protezione dei dati personali, sulla base delle notifiche di *data breach* ricevute, ha avviato accertamenti sulle conseguenze che il recente blackout dei sistemi informatici potrebbe aver prodotto sui dati personali degli utenti, in particolare nell'utilizzo dei servizi pubblici.

L'evento è derivato da un malfunzionamento del software di sicurezza *CrowdStrike* che nei giorni scorsi ha bloccato l'operatività di numerosi servizi online.

Il Garante si riserva ulteriori interventi qualora si ravvisassero specifiche violazioni che possano riguardare gli utenti italiani.

---

18 Luglio 2024 – Consiglio d'Europa: pubblicata la versione in lingua araba del "Manuale sul diritto europeo in materia di protezione dei dati".

Nell'ambito di una cooperazione tra l'Agenzia dell'Unione europea per i diritti fondamentali (FRA) e il Consiglio d'Europa, il "Manuale sul diritto europeo in materia di protezione dei dati" è stato tradotto in arabo.

Questo manuale è stato sviluppato congiuntamente ed è pubblicato dal Consiglio d'Europa, dalla Corte europea dei diritti dell'uomo (CEDU) e dalla FRA.

La traduzione del manuale in arabo mira a promuovere un quadro giuridico comune in tutto il Mediterraneo e a consentire alle parti interessate, in particolare ai professionisti del diritto nei paesi del Mediterraneo meridionale, di approfondire la loro comprensione dei diritti umani in relazione alla privacy e alla protezione dei dati personali.

La traduzione faciliterà l'introduzione di riforme e l'adozione di leggi sulla protezione dei dati personali nei paesi della regione.

L'iniziativa è sostenuta dal programma congiunto tra il Consiglio d'Europa e l'Unione europea, "Proteggere i diritti umani, lo stato di diritto e la democrazia attraverso norme condivise nel Mediterraneo meridionale" (Programma Sud V), cofinanziato da entrambe le organizzazioni e attuato dal Consiglio d'Europa.

INTELLIGENZA ARTIFICIALE.

22 Luglio 2024 – La Commissione UE ha pubblicato la bozza del Patto per l'IA.

La Commissione europea ha pubblicato la bozza del Patto per l'IA ai sensi del AI Act europeo appena pubblicato in Gazzetta. Il progetto di patto per l'IA è un impegno volontario che anticipa i requisiti previsti dal Regolamento 2024/1689 sull'IA e li attua prima delle scadenze normative. Ad oggi hanno aderito oltre 550 organizzazioni.

Il progetto di AI *Pact* è incentrato sui due pilastri seguenti:

pilastro I - come porta d'accesso per coinvolgere la rete del patto per l'IA, incoraggiando lo scambio delle migliori pratiche e fornendo informazioni pratiche sull'attuazione della legge dell'UE sull'IA attraverso (1) l'organizzazione dei laboratori di ricerca e (2) la creazione e la gestione di uno spazio online dedicato allo scambio di buone pratiche;

pilastro II: incoraggiare i fornitori e gli operatori di sistemi di IA a prepararsi tempestivamente e ad adottare misure per conformarsi ai requisiti e agli obblighi stabiliti dalla normativa dell'UE sull'IA attraverso (1) la creazione di modelli e schemi di monitoraggio; (2) l'impegno ad adottare azioni concrete in merito ai requisiti della normativa dell'UE sull'IA; e (3) la rendicontazione periodica degli impegni, pubblicati dall'Ufficio per l'IA della Commissione UE.

Le organizzazioni possono contribuire alla bozza del Patto per l'IA qui.

---

22 Luglio 2024 – Pubblicato il documento completo della Strategia Italiana per l'Intelligenza Artificiale 2024-2026.

A pochi giorni dalla pubblicazione del Regolamento UE sull'IA n. 2024/1689 sulla Gazzetta Ufficiale dell'Unione Europea e dall'inizio delle audizioni in commissione, presso il Senato della Repubblica, del disegno di legge del Governo italiano sull'intelligenza artificiale, è disponibile online il documento integrale della *Strategia Italiana per l'Intelligenza Artificiale 2024-2026*.

Il testo è stato redatto dal Comitato di esperti di supporto al Governo nella definizione di una normativa nazionale e delle strategie relative a questa tecnologia. Il documento riflette l'impegno del Governo nel creare un ambiente in cui l'IA possa svilupparsi in modo sicuro, etico e inclusivo, massimizzando i benefici e minimizzando i potenziali effetti avversi.

Dopo un'analisi del contesto globale e del posizionamento italiano, il documento definisce le azioni strategiche, raggruppate in quattro macroaree: Ricerca, Pubblica Amministrazione, Imprese e Formazione. La strategia propone, inoltre, un sistema di monitoraggio della relativa attuazione e un'analisi del contesto regolativo che traccia la cornice entro cui dovrà essere dispiegata.

---

22 Luglio 2024 – L'OCSE avvia la fase pilota per monitorare l'applicazione del Codice di condotta internazionale per le organizzazioni che sviluppano sistemi di intelligenza artificiale.

L'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) ha annunciato una fase pilota per monitorare l'applicazione del Codice di condotta internazionale del processo di Hiroshima per le organizzazioni che sviluppano sistemi di intelligenza artificiale (*G7 Hiroshima AI Process*). Il *G7 Hiroshima AI Process* è un quadro politico completo sull'intelligenza artificiale (IA) composto da:

- Rapporto dell'OCSE verso un'intesa comune del G7 sull'IA generativa;
- Principi guida internazionali;
- Codice di condotta internazionale; e
- cooperazione basata su progetti in materia di IA.

La fase pilota è aperta alla partecipazione fino al 6 settembre 2024 ed è aperta al contributo delle organizzazioni che sviluppano sistemi di intelligenza artificiale avanzati.

Il Codice di Condotta prevede 11 Principi, tra cui:

- l'adozione di misure adeguate per individuare, valutare e mitigare i rischi durante l'intero ciclo di vita dell'IA;
- monitoraggio dei modelli di uso improprio, dopo l'introduzione, compresa l'immissione sul mercato;
- comunicare pubblicamente le capacità, i limiti e i domini di uso appropriato e inappropriato dei sistemi avanzati di IA, al fine di sostenere la trasparenza;

- lavorare per la condivisione delle informazioni e la segnalazione degli incidenti tra le organizzazioni che sviluppano sistemi avanzati di intelligenza artificiale;
- lo sviluppo, l'attuazione e la divulgazione delle politiche di governance e di gestione del rischio dell'IA;
- investire e attuare solidi controlli di sicurezza, comprese misure fisiche;
- lo sviluppo e l'implementazione di meccanismi affidabili di autenticazione e provenienza dei contenuti, ove tecnicamente fattibile;
- dare priorità alla ricerca per mitigare i rischi per la società, la sicurezza e la protezione;
- dare priorità allo sviluppo di sistemi avanzati di IA per affrontare le sfide globali, tra cui il clima, la salute e l'istruzione;
- promuovere lo sviluppo e l'adozione di norme tecniche internazionali; e
- l'attuazione di adeguate misure di inserimento dei dati, la protezione dei dati personali e la proprietà intellettuale.

CYBERSECURITY

26 Luglio 2024 - L'Agenzia per la Cybersicurezza Nazionale pubblica la guida alla notifica al CSIRT Italia degli incidenti informatici.

L'ACN ha pubblicato la Guida alla notifica degli incidenti al CSIRT Italia. La corretta adozione della procedura di notifica degli incidenti cibernetici costituisce infatti un elemento cruciale per garantire sicurezza e resilienza delle reti, dei sistemi informativi e dei servizi informatici.

La prontezza e la precisione delle informazioni fornite durante il processo di notifica rivestono un ruolo fondamentale per consentire al CSIRT Italia di acquisire una conoscenza completa ed esaustiva dell'incidente occorso ai fini dell'attività di allertamento e per fornire ai soggetti impattati il supporto necessario nell'ottica del ripristino dei servizi stessi.

La Guida rappresenta un compendio – una sorta di "testo unico" - delle istruzioni per i diversi soggetti, pubblici e privati, tenuti per legge alla notifica degli incidenti, soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), quelli operanti in ambito NIS e Telco, cui si aggiungono quelle puntualmente rivolte alle entità oggi considerate dalla Legge 2 luglio 2024 n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

Il flusso informativo verso il CSIRT Italia si snoda nelle seguenti quattro fasi:

1. Una fase preparatoria, con l'obiettivo di raccogliere le prime informazioni idonee a garantire una sufficiente conoscenza dell'evento;

2. ad essa fa seguito la fase di segnalazione dell'incidente, che avviene attraverso la compila-zione di un modulo disponibile sul sito internet del CSIRT Italia: https://www.csirt.gov.it/segnalazione. Tale comunicazione occorre che venga effettuata al Csirt con una tempistica definita nelle linee guida, e diversamente declinata in funzione dell'appartenenza del soggetto ai diversi presidi normativi. In ogni caso, la segnalazione è strettamente correlata al principio di immediatezza della conoscenza dell'incidente, inteso nella sua magnitudo e nel suo carattere di impatto sistemico eventuale;

3. una terza fase attiene alla vera e propria gestione della notifica, cioè le operazioni di *incident handling,* da parte del personale del CSIRT Italia, per dare supporto alla vittima con efficaci azioni di contenimento e di ripristino dei servizi;

4. il processo si conclude, infine, con la fase di chiusura dell'incidente.

Le linee guida si rivolgono anche ai soggetti, pubblici e privati che, pur non essendo obbligati alla notifica intendono tuttavia segnalare volontariamente l'incidente allo CSIRT, in questo modo contribuendo a una migliore condivisione della conoscenza del livello e dell'intensità della minaccia, per rafforzare la resilienza dell'ecosistema digitale italiano.

22 Luglio 2024 – L'Agenzia per la Cybersicurezza Nazionale aggiorna le linee guida sulla crittografia.

La crittografia permette di proteggere le comunicazioni nel mondo digitale in maniera sicura ed efficiente. Dopo le linee guida sulla conservazione delle password, le funzioni di *hash* e i codici di autenticazione messaggi, l'Agenzia per la cybersicurezza nazionale, ACN, pubblica altri approfondimenti sulla crittografia dedicati alla confidenzialità dei dati e alle tecniche di preparazione alla minaccia quantistica**.**

Dal documento introduttivo alle indicazioni sui cifrari a blocchi, ovvero uno degli strumenti più importanti per garantire la confidenzialità dei dati, i nuovi documenti aiutano ad orientarsi tra le specifiche degli algoritmi crittografici e a comprendere meglio il funzionamento dei cifrati e l'interazione con i messaggi da inviare.

È disponibile, inoltre, il primo dei documenti informativi che ACN mette a disposizione per approfondire i temi crittografici. A differenza delle "Linee Guida Funzioni crittografiche", questi documenti hanno lo scopo di informare e sensibilizzare su argomenti centrali per la crittografia moderna, fornendo un'ampia panoramica e includendo le informazioni più rilevanti per le strutture e gli enti del nostro Paese. Il primo della serie è dedicato alla "Crittografia post-quantum e quantistica" per la preparazione alla minaccia quantistica e contiene una panoramica sullo scenario attuale, utile a considerare le principali alternative post-quantum o quantistiche e gli sviluppi a livello internazionale.

Tra le linee guida già pubblicate a dicembre 2023 ci sono indicazioni per la conservazione delle password, realizzate insieme al Garante per la protezione dei dati personali e che riguardano il modo in cui il fornitore del servizio a cui si accede deve proteggere la password per accedervi; indicazioni sulle funzioni di hash crittografiche, strumenti fondamentali per la cybersicurezza poiché, grazie alle loro proprietà, rendono possibile assicurare l'integrità dei dati, cioè consentono di verificare l'alterazione di un dato o un messaggio; e i codici di autenticazione del messaggio o MAC, che permettono di garantire l'integrità di un messaggio e di verificare l'identità del mittente.

Linee guida Funzioni crittografiche

Le linee guida e i documenti informativi fanno parte di una serie di pubblicazioni tecniche che servono a proteggere il cyberspace in cui tutti ci muoviamo. Queste linee guida, tutte insieme, forniscono delle indicazioni precise per l'impiego degli algoritmi crittografici lungo l'intero ciclo di vita dei sistemi e servizi ICT, in conformità con i principi di sicurezza e tutela della privacy**.** In ogni documento, l'ultimo capitolo contiene le conclusioni tratte in seguito alla dissertazione svolta e la lista degli algoritmi e dei parametri raccomandati da ACN.
Sull'esempio di altre realtà internazionali, la Divisione Scrutinio tecnologico e crittografia, all'interno del Servizio di Certificazione e Vigilanza dell'Agenzia, ha deciso di avviare la pubblicazione della serie "Linee Guida Funzioni Crittografiche", che rappresentano le principali funzioni (primitive) crittografiche sia da un punto di vista teorico, che pratico.

La realizzazione di questi documenti rientra proprio tra le funzioni attribuite all'Agenzia per la Cybersicurezza Nazionale per la prima volta sancita dalla legislazione italiana (dal DL 82/2021), per cui l'ACN è promotrice dell'utilizzo della crittografia come strumento di cybersicurezza, in attuazione della misura #22 della Strategia Nazionale di Cybersicurezza.

INFORMATION TECHNOLOGY

26 Luglio 2024 – Ministero della Giustizia: attiva la piattaforma elettronica per la raccolta delle firme digitali valevoli per la sottoscrizione digitale dei referendum abrogativi o costituzionali e delle iniziative legislative di natura popolare.

È stato pubblicato in Gazzetta Ufficiale n. 173/2024 il D.P.C.M. 18 luglio 2024 recante «Attestazione dell'operatività della Piattaforma per la raccolta delle firme espresse nell'ambito del referendum, di cui all'articolo 1, commi 341 e seguenti, della legge 30 dicembre 2020, n. 178» che prevede l'attivazione della nuova piattaforma digitale dedicata alla raccolta delle firme per i referendum.

La piattaforma è concepita per agevolare la sottoscrizione digitale dei referendum abrogativi o costituzionali e delle iniziative legislative di natura popolare. La sua attivazione è prevista dal DPCM 18 luglio 2024, pubblicato in Gazzetta Ufficiale n. 173/2024.

Il sistema ha ottenuto il parere del Garante Privacy ed è utilizzabile dai promotori di proposte referendarie e dagli uffici della Corte di Cassazione e delle Camere per gestire tutte le fasi del processo di raccolta delle firme dei sostenitori in formato digitale. Il sistema effettua poi la verifica della presenza e validità delle firme, mediante interoperabilità con il sistema dell'Anagrafe Nazionale della Popolazione Residente (ANPR), presso le anagrafi dei comuni ove sono residenti i cittadini firmatari delle proposte.

---

26 Luglio 2024 - L'Organizzazione Mondiale per il Commercio – WTO adotta un Accordo sul Commercio Elettronico.

L'Organizzazione mondiale del commercio (WTO) ha annunciato l'adozione dell'Accordo sul commercio elettronico che si applicherà alle misure adottate o mantenute in vigore da una Parte che incidono sugli scambi per via elettronica. Tuttavia, l'Accordo non si applica:

- agli appalti pubblici;
- a servizi forniti nell'esercizio di pubblici poteri; o
- ad eccezione degli articoli 8, 9 e 12 dell'accordo, alle informazioni detenute o trattate da o per conto di una Parte o alle misure relative a tali informazioni, comprese le misure relative alla loro raccolta.

L'Accordo contiene disposizioni volte a rafforzare la fiducia nel commercio elettronico, tra cui impegni per consolidare la protezione dei dati personali, contrastare le comunicazioni elettroniche non richieste e rafforzare la cybersecurity.

L'Accordo impegna la Parte aderente ad adottare o mantenere in vigore misure idonee a:

- imporre ai fornitori di messaggi elettronici commerciali di agevolare la capacità dei destinatari di impedire la ricezione continua di tali messaggi;
- richiedere il consenso, come specificato nelle leggi o regolamenti applicabili alla Parte in sede locale, dei destinatari per la ricezione di messaggi elettronici commerciali; o
- prevedere la riduzione al minimo dei messaggi elettronici commerciali non richiesti.

L'Accordo richiede inoltre a ciascuna Parte di adottare o mantenere un quadro giuridico che preveda la protezione dei dati personali degli utenti dell'e-commerce e stabilisce che ciascuna Parte deve pubblicare informazioni sulla protezione dei dati personali garantita agli utenti del commercio elettronico, comprese le indicazioni su come una persona fisica può perseguire i rimedi e su come le imprese possono conformarsi ai requisiti legali.