Studio Violi S.r.l.
Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015

2003-2023
oltre vent'anni di consulenza per le imprese

ISO 9001 BUREAU VERITAS Certification
IT309277

I Partners dello Studio

Giorgio Violi	tel: 3386132605	givioli@gmail.com
Alberto Sant'Unione	tel: 3409125853	santunionea@gmail.com

Qualità Sicurezza Privacy Ambiente Risk Management
Responsabilità Amministrativa 231 Etica Consulenza e Audit per la Direzione

Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015 per Progettazione ed erogazione di servizi di consulenza relativa ai Sistemi di Gestione Aziendale per la Qualità, la Sicurezza negli ambienti di lavoro, la Privacy, l'Ambiente, l'Etica, per i Modelli Organizzativi e Consulenza per la Direzione

2024 Luglio **Il nostro punto di vista su…** *Anno 17 – 1° sem*

Periodico di informazione per i CLIENTI dello STUDIO VIOLI

Indice delle NOTIZIE (N)

SENTENZE DI CASSAZIONE SUL LAVORO

- Sul sito http://www.dottrinalavoro.it/argomento/giurisprudenza-c/corte-di-cassazione-c sono presenti le ultime sentenze di Cassazione relative al lavoro

AFORISMA DEL MESE

"La soluzione dei problemi è un processo, non un evento"

Joseph Juran (Esperto di quality management)

Scadenziario di Luglio e agosto 2024 sul sito del Sole 24 Ore http://www.ilsole24ore.com/norme-e-tributi/scadenze.shtml

"Prevenzione e protezione dal sole durante il lavoro"

Notizie

- N1) Privacy: Garante Privacy, principali interventi del 2023. Tutti i numeri

Pubblicato il bilancio di tutti gli interventi del Garante Privacy nel 2023, con particolare attenzione per AI, sanità, giustizia digitale, data breach, videosorveglianza, riconoscimento facciale.

Il 2023 ha visto una serie di interventi centrati sulle grandi questioni legate alla tutela dei diritti fondamentali delle persone nel mondo digitale: **in particolare, le implicazioni etiche della tecnologia; l'Intelligenza Artificiale generativa; l'economia fondata sui dati; le grandi piattaforme e la tutela dei minori; i sistemi di age verification; i big data; le problematiche poste dagli algoritmi; la sicurezza dei sistemi e la protezione dello spazio cibernetico; la monetizzazione delle informazioni personali; i fenomeni del revenge porn e del cyberbullismo**.

Il 2023 è stato l'anno dell'AI

Il 2023 è stato l'anno della diffusione massiva dell'Intelligenza Artificiale con importanti interventi del Garante. Dopo un iniziale blocco di ChatGPT, per raccolta illecita di dati personali e assenza di sistemi per la verifica dell'età dei minori, la piattaforma è stata riaperta garantendo più trasparenza e più diritti agli utenti. Nel frattempo è stata costituita una task force ad hoc a livello europeo e sono in corso ulteriori verifiche dell'Autorità. Il Garante ha imposto lo stop anche alla chatbot Replika: troppi i rischi per i minori e le persone emotivamente fragili, ed ha avviato un'istruttoria su Sora il modello di intelligenza artificiale che crea brevi video da poche righe di testo.
Sotto la lente dell'Autorità anche Pornhub, chiesti chiarimenti su profilazione degli utenti e sistemi di tracciamento. Sempre in questo ambito, il provvedimento del Garante Privacy che detta le regole per difendere i dati personali dal webscraping.

Digitalizzazione

L'accelerazione del processo di digitalizzazione ha visto numerosi interventi dell'Autorità riguardanti in particolare la gestione centralizzata delle credenziali dell'identità digitale CIE (CIEId), il Single digital gateway (SDG) per lo scambio transfrontaliero di prove, la Piattaforma unica per le notifiche digitali di atti amministrativi. Proseguite anche le attività connesse ai trattamenti dell'Agenzia delle entrate che prevedono l'interscambio di informazioni fra amministrazioni per garantire l'esattezza e completezza della dichiarazione dei redditi precompilata, così come quelle legate all'operatività dell'Anagrafe nazionale dei residenti. Sempre per quanto riguarda la pubblica amministrazione, il Garante ha richiamato Ministeri, Enti locali e Regioni ad evitare diffusioni illecite di dati personali e a contemperare obblighi di pubblicità degli atti e dignità delle persone.

Digitalizzazione della giustizia

Un significativo contributo è stato fornito dal Garante per la piena realizzazione del processo di digitalizzazione della giustizia, rispetto sia al processo (ordinario) telematico, sia alla costituzione delle infrastrutture digitali per le intercettazioni.

Fascicolo sanitario elettronico

Importanti in ambito sanitario, gli interventi sulla riforma del Fascicolo sanitario elettronico 2.0 (FSE) e la realizzazione del sistema nazionale di telemedicina, che sono parte delle azioni di attuazione della Missione 6 (salute) del PNRR. Significativa anche la pubblicazione di un decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di intelligenza artificiale e la recente segnalazione inviata al Governo sulle difformità riscontrate tra le varie Regioni nella realizzazione del FSE.

Riconoscimento facciale

Particolare attenzione è stata posta all'uso dei dati biometrici e al diffondersi di sistemi di riconoscimento facciale. In particolare, l'Autorità ha inviato un avvertimento a Worldcoin in relazione al progetto di scansione dell'iride in cambio di criptovalute, senza adeguate garanzie e la necessaria consapevolezza da parte degli utenti.

Age verification e revenge porn

Sul fronte della tutela on line dei minori nell'anno trascorso è proseguita l'azione di vigilanza sull'età di iscrizione ai social, anche attraverso sistemi di age verification. In questa direzione si muove il tavolo di lavoro istituito con un protocollo d'intesa tra Garante e Agcom.

Firmati anche nuovi protocolli tra Garante e Co. Re.Com di diverse Regioni per combattere revenge porn e cyberbullismo. Realizzati numerosi incontri con i giovani in diverse città italiane e premiate le scuole vincitrici del contest "Ambasciatori della Privacy".

In particolare, proprio il fenomeno del revenge porn risulta in preoccupante aumento: 299 le segnalazioni di persone che temono la diffusione di foto e video a contenuto sessualmente esplicito, raddoppiate rispetto allo scorso anno. Le segnalazioni ricevute sono state trattate tempestivamente e nella maggior parte dei casi l'esame si è concluso con un provvedimento diretto alle piattaforme coinvolte per ottenere il blocco preventivo della diffusione delle foto e dei video.

Garante Privacy e ACN, linee guida per la conservazione delle password

Sul fronte della cybersecurity, Garante Privacy e Agenzia per la Cybersicurezza Nazionale (ACN) hanno messo a punto le Linee guida per la conservazione delle password.

Data breach

Significativo a questo proposito il numero dei data breach notificati nel 2023 al Garante da parte di soggetti pubblici e privati: 2.037. Nel settore pubblico (37% dei casi), le violazioni hanno riguardato soprattutto Comuni, istituti scolastici e strutture sanitarie; nel settore privato (63% dei casi) sono stati coinvolte sia PMI e professionisti sia grandi società del settore delle telecomunicazioni, energetico, bancario, dei servizi e delle telecomunicazioni.

Nei casi più gravi sono stati adottati provvedimenti di tipo sanzionatorio.

Videosorveglianza

Numerosi, come in passato, i provvedimenti assunti nell'ambito del rapporto di lavoro, soprattutto con riguardo all'utilizzo della posta elettronica sul luogo di lavoro e all'impiego di sistemi di videosorveglianza. Da sottolineare

due documenti di indirizzo elaborati nel corso dell'anno: uno dedicato alla gestione della posta elettronica nel contesto lavorativo e al trattamento dei metadati, l'altro elaborato con ANAC e dedicato alla gestione delle procedure connesse al whistleblowing.
Sul fronte della tutela dei consumatori il Garante è intervenuto con decisione contro il telemarketing aggressivo con l'applicazione di pesanti sanzioni, la maggior parte delle quali riguardano l'utilizzo senza consenso dei dati degli abbonati. L'Autorità ha inoltre approvato il Codice di condotta per le attività di telemarketing e di teleselling.

LE CIFRE

Nel 2023 sono stati adottati 634 provvedimenti collegiali.
I provvedimenti correttivi e sanzionatori sono stati 394. Le sanzioni riscosse sono state di circa 8 milioni. 2037 i data breach notificati all'Autorità. Le ispezioni effettuate nel 2023 sono state 144 in linea rispetto a quelle dell'anno precedente. Gli accertamenti svolti, anche con il contributo del Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza, hanno riguardato diversi settori, sia nell'ambito pubblico che privato: in particolare, SPID, ricerca scientifica, tecnologie di riconoscimento facciale, data breach, telemarketing, siti web ed uso dei cookie.
Effettuate le verifiche periodiche al VIS (Visa Information System), il sistema sui visti d'ingresso nello spazio Schengen.
L'Autorità ha fornito riscontro a 19.281 reclami e segnalazioni riguardanti, tra l'altro il marketing e le reti telematiche; i dati on line delle pubbliche amministrazioni; la sanità; la giustizia, il cyberbullismo e il revenge porn, la sicurezza informatica; il settore bancario e finanziario; il lavoro.
I pareri resi dal Collegio su atti normativi e amministrativi sono stati 59 ed hanno riguardato la digitalizzazione della P.a.; la sanità; il fisco; la giustizia; l'istruzione; funzioni di interesse pubblico. 6 sono stati i pareri su norme di rango primario: in particolare, riguardo accertamento fiscale, digitalizzazione della Pa, giustizia, open data.
Le comunicazioni di notizie di reato all'autorità giudiziaria sono state 7 e hanno riguardato violazioni in materia di controllo a distanza dei lavoratori, falsità nelle dichiarazioni e notificazioni al Garante, accesso abusivo a un sistema informatico.
Per quanto riguarda l'attività di relazione con il pubblico si è dato riscontro a oltre 19.200 quesiti, che hanno riguardato, in maniera preponderante, gli adempimenti connessi all'applicazione del Regolamento Ue e all'attività dei Responsabili del trattamento, seguiti dalle questioni legate al telemarketing indesiderato; al rapporto di lavoro pubblico e privato; alla videosorveglianza; alle problematiche poste dal web; alla salute e alla ricerca; all'intelligenza artificiale.
Oltre 4 milioni e 200 mila gli accessi al sito web dell'Autorità. Per quanto riguarda l'attività di informazione e comunicazione istituzionale, nel 2023 l'Autorità ha diffuso 62 comunicati stampa, 17 Newsletter, realizzato 4 campagne informative, e prodotto 45 video informativi su temi di maggiore interesse per il pubblico, di cui 9 diffusi sui canali Rai Radio e Tv, sul web e sui social media.

- N2) Privacy: Trattamento dei metadati, o log di posta elettronica, nell'ambito lavorativo: le indicazioni operative

Il Garante per la protezione dei dati personali, con provvedimento del 6 giugno 2024, ha emesso il documento di indirizzo aggiornato e definitivo sul trattamento dei log di posta elettronica nel contesto lavorativo,

con l'obiettivo di rendere una ricostruzione sistematica delle disposizioni applicabili in tale specifico ambito, che presenta punti di intersezione tra i diritti costituzionali inviolabili (art. 2 Cost.), di libertà e segretezza (15 Cost.), la disciplina di protezione dei dati e le norme che stabiliscono le condizioni per l'impiego degli strumenti tecnologici nei luoghi di lavoro (Legge n. 300/70).

E' stato chiarito che i metadati, cui si fa riferimento, corrispondono ai dati esteriori delle comunicazioni, nonché ai file allegati, cioè a quelle informazioni registrate automaticamente nei log generati dai sistemi server di gestione e smistamento della posta elettronica e possono comprendere: gli indirizzi e-mail del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati ed anche l'oggetto del messaggio spedito o ricevuto.

Nel suddetto documento di indirizzo sono evidenziati gli adempimenti cui sono tenuti i datori di lavoro (titolari del trattamento), per la corretta gestione del trattamento in questione.

Pertanto, si tenterà di focalizzare e sintetizzare i vari adempimenti, col fine di rendere concretamente applicabile il provvedimento mediante indicazioni operative.

1) L'analisi preliminare

I datori di lavoro, o più in generale i titolari del trattamento dei metadati della posta elettronica in ambito lavorativo, dovranno preliminarmente analizzare il trattamento posto in essere dei log di posta elettronica nel contesto lavorativo, individuando:

- **le categorie di dati personali**, o informazioni riguardanti gli interessati identificati o identificabili, che vengono trattate (ad esempio: indirizzi e-mail del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati ed anche l'oggetto del messaggio spedito o ricevuto).
- **Le finalità del trattamento** (ad esempio: sicurezza informatica; tutela del patrimonio informatico aziendale; rilevamento e mitigazione di eventuali incidenti di sicurezza; assolvimento degli obblighi inerenti alla prestazione lavorativa; acquisizione di informazioni riferite alla sfera personale o alle opinioni degli interessati; monitoraggio sistematico degli interessati, inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati").
- **La base giuridica del trattamento** (ad esempio: legittimo interesse, obbligo legale, esecuzione di un contratto).
- **Le categorie di destinatari**, ovvero i soggetti che ricevono la comunicazione dei metadati della posta elettronica (ad esempio: i fornitori dei servizi di posta elettronica).
- **Eventuali trasferimenti dei metadati ad un paese terzo o extra UE** (ad esempio: servizi di cloud gestiti da aziende aventi sede extra UE).

- Il periodo di conservazione (se è stato limitato e in ragione di quale scopo), tenendo in considerazione che i tempi di conservazione dei metadati devono in ogni caso essere proporzionati rispetto alle finalità perseguite.

In particolare, finalità connesse alla sicurezza informatica e alla tutela del patrimonio informatico giustificherebbero la conservazione dei metadati per un arco temporale congruo rispetto all'obiettivo di rilevare e mitigare eventuali incidenti di sicurezza, adottando tempestivamente le opportune contromisure.

Ove i tempi di conservazione non siano definiti in maniera proporzionata alle finalità del trattamento, il titolare del trattamento incorrerebbe nella violazione del principio di "limitazione della conservazione". Per l'applicabilità del "secondo comma dell'art. 4 Statuto dei lavoratori (L. n. 300/1970), **la conservazione non dovrebbe comunque superare i 21 giorni**, un tempo più ampio è possibile solo in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente, in applicazione del principio di accountability, le specificità della realtà tecnica e organizzativa del titolare del trattamento".

2) La disamina complessiva del trattamento

La suddetta analisi preliminare è propedeutica alla successiva disamina complessiva del trattamento, finalizzata all'implementazione di tutti i necessari adempimenti, anche nel rispetto delle normative che si intersecano con la disciplina di protezione dei dati, di talché andrebbero effettuate le seguenti verifiche, in ordine:

- alla sussistenza dei presupposti di liceità (stabiliti dall'art. 4 della l. 20 maggio 1970, n. 300), allorquando sussista la finalità di monitoraggio sistematico degli interessati, inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati"; in tal caso, andrebbe verificata la sussistenza dei suddetti presupposti di liceità, ovvero se sussistono le esigenze organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale che potrebbero legittimare, se del caso, l'uso degli strumenti dai quali possa derivare la possibilità di controllo a distanza dell'attività dei lavoratori, con le correlate garanzie procedurali (accordo sindacale o autorizzazione pubblica). Diversamente, andrebbero limitate le finalità del trattamento, in modo che venga effettuato, per impostazione predefinita, solo il trattamento strettamente necessario per conseguire le specifiche e lecite finalità, in tutte le fasi ed attività di trattamento;

- al rispetto delle disposizioni che vietano al datore di lavoro di acquisire e comunque trattare informazioni attinenti alla sfera privata del lavoratore (art. 8 della l. 20 maggio 1970, n. 300), ovvero: se tramite il trattamento in questione è possibile o meno acquisire informazioni riferite alla sfera personale o alle opinioni dell'interessato e quindi non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore. In tal caso, stante il divieto espresso di legge, la verifica dovrebbe essere orientata all'inibizione e limitazione di tale finalità del trattamento, nel senso che il titolare del trattamento dovrebbe adoperarsi affinché i metadati non siano trattati per tali finalità incompatibili con quelle determinate e legittime;

- alla sussistenza di rischi elevati per i diritti e le libertà delle persone fisiche (in ragione delle tecnologie impiegate e considerato il contesto e le finalità perseguite) che rendano necessaria una preventiva valutazione di impatto sulla protezione dei dati personali. Tale necessità ricorre, in particolare, in caso di raccolta e memorizzazione dei log della posta elettronica per finalità di "monitoraggio sistematico",

inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti";

- alle misure organizzative e tecniche interne per assicurare l'accessibilità selettiva ai metadati da parte dei soli soggetti autorizzati, adeguatamente istruiti, con tracciatura degli accessi effettuati;

- ai rapporti con i fornitori, giacché il titolare del trattamento/datore di lavoro dovrebbe impartire le necessarie istruzioni al fornitore di servizi e programmi di posta elettronica, finalizzate alla disattivazione delle funzioni non compatibili con le proprie finalità del trattamento o che si pongono in contrasto con specifiche norme di settore previste dall'ordinamento, ad esempio, commisurando adeguatamente anche i tempi di conservazione dei dati ovvero chiedendo al fornitore del servizio di anonimizzare i metadati raccolti nei casi in cui non si intenda effettuare una conservazione più prolungata degli stessi.

- N3) Privacy: Pubblicato in Gazzetta Ufficiale dell'UE il Regolamento sull'intelligenza artificiale

ISi tratta del primo provvedimento legislativo al mondo volto a regolare in maniera orizzontale gli utilizzi dell'intelligenza artificiale,

con l'obiettivo di istituire un quadro giuridico atto a garantire un'intelligenza artificiale antropocentrica, tutelando i diritti fondamentali degli individui dai potenziali effetti pregiudizievoli derivanti dall'utilizzo dell'IA, ma volendo comunque promuovere un contesto di fiducia nei consumatori per tali sistemi attraverso meccanismi, in modo da favorirne la diffusione, e prevedendo alcuni istituti per facilitarne l'implementazione.

Il Regolamento europeo sull'intelligenza artificiale stabilisce:

1. **regole armonizzate** per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione
2. **divieti** di talune pratiche di IA
3. **requisiti specifici** per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi
4. **regole di trasparenza** armonizzate per determinati sistemi di IA
5. **regole armonizzate per l'immissione sul mercato** di modelli di IA per finalità generali
6. **regole in materia di monitoraggio e vigilanza del mercato**, governance ed esecuzione
7. **misure a sostegno dell'innovazione**, con attenzione alle PMI, comprese le start-up.

L'entrata in vigore del regolamento UE 2024/1689 avviene il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea, e si applicherà a decorrere dal 2 agosto 2026, seguendo un cronoprogramma per l'operatività e per la regolarizzazione dei sistemi di intelligenza artificiale già in uso.
Il regolamento, salvo le varie eccezioni, si applicherà dopo 24 mesi dall'entrata in vigore, ma prevede una scaletta progressiva di inizio di operatività per i singoli capi dello stesso.

La prima fase è collocata **decorsi 6 mesi dall'entrata in vigore**.
La seconda fase è collocata **decorsi 12 mesi**.
La terza fase è collocata **decorsi 24 mesi** dall'entrata in vigore e segna l'entrata a regime nella sua integralità dell'AI Act.

Nel dettaglio lo scaglionamento delle tempistiche per l'acquisizione della piena efficacia delle disposizioni contenute nel Regolamento è il seguente:

1. I capi I e II (definizioni e pratiche vietate) si applicano a decorrere dal 2 febbraio 2025;
2. Il capo III, sezione 4 (autorità di notifica designate dagli stati membri), il capo V (modelli di AI per finalità generali), il capo VII (banca dati UE per i sistemi ad alto rischio), il capo XII (sanzioni) e l'art. 78 (riservatezza dei dati trattati in conformità al regolamento) si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'art. 101 (Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali);
3. L'art. 6, paragrafo 1 (classificazione dei sistemi ad alto rischio), e i corrispondenti obblighi di cui al Regolamento, si applicano a decorrere dal 2 agosto 2027

-N4) Privacy: Attenzione alla privacy con i siti di conversione dei file in pdf: trovati online migliaia di documenti d'identità, certificati, e contratti; Vinted, sanzione da 2,3 milioni di euro per violazione del Gdpr;

Attenzione alla privacy con i siti di conversione dei file in pdf: trovati online migliaia di documenti d'identità, certificati, e contratti.
Ogni giorno milioni di utenti utilizzano servizi online per la conversione dei file PDF per lavoro o per svago, ignari che alcuni di questi siti potrebbero essere dei veri e propri colabrodo per i dati sensibili, facendo trapelare online migliaia di documenti. Ci sono infatti molti strumenti online gratuiti per creare file PDF e per la maggior parte funzionano bene e risultano molto utili in svariate situazioni. Come spesso accade però ci può essere il risvolto della medaglia, ovvero può accedere che questi convertitori possano rappresentare una minaccia in termini di privacy e sicurezza dei dati degli utenti. Un esempio è il caso emerso in questi giorni di oltre 89.000 file PDF che sono stati scoperti in un bucket Amazon S3, liberamente accessibile a chiunque, dal team di ricerca di Cybernews. I file che sono finiti nel contenitore digitale di Amazon Web Services provengono dai servizi PDF Pro e Help PDF e comprendono copie e scansioni di passaporti, patenti, certificati e contratti. Contengono quindi informazioni sensibili, alcune delle quali possono essere utilizzate da malintenzionati per commettere azioni illecite. I ricercatori hanno sottolineato come l'accesso a questi documenti possa permettere ai criminali di commettere frodi finanziarie, come la richiesta di prestiti, l'affitto di proprietà o l'acquisto di beni costosi utilizzando l'identità delle vittime. Ma le conseguenze possono essere ancora più gravi: le informazioni contenute nei documenti possono essere utilizzate per creare false identità, ottenere accesso a conti bancari e condurre altre attività illegali. Questa situazione sottolinea l'importanza di essere cauti quando si utilizzano servizi online per la gestione di documenti sensibili. Ci si augura ovviamente che si intervenga sulla questione per la sicurezza degli utenti. Nonostante le segnalazioni e i tentativi di contatto da parte di Cybernews, i responsabili dei servizi PDF Pro e Help PDF non hanno risposto né preso provvedimenti per risolvere la falla di sicurezza. Questi due servizi, molto simili per design e probabilmente gestiti dalla stessa entità, continuano a mettere a rischio la riservatezza degli utenti, poiché i file caricati diventano immediatamente pubblici. Nel frattempo c'è chi, ignaro della falla, continua a utilizzare i due servizi per convertire file che, una volta caricati, diventano immediatamente pubblici. Vanno quindi ad ampliare la portata di un problema che mette in evidenza l'importanza di prestare molta attenzione a questo tipo di attività, gratuite e per questo allettanti, ma spesso poco attente alla privacy degli utenti.

Vinted, sanzione da 2,3 milioni di euro per violazione del Gdpr. Vinted, la nota piattaforma online di abbigliamento di seconda mano con oltre 100 milioni di utenti in tutto il mondo avrebbe violato il Gdpr, **e per questo è stata condannata a pagare una multa di € 2.385.276.**
Il provvedimento sanzionatorio è stato adottato dal Garante per la protezione dei dati personali della Lituania (VDAI), dove ha sede la società di e-commerce, a conclusione di un'indagine aperta a seguito dei reclami che erano stati presentati dall'autorità francese (CNIL) e da quella polacca (UODO) nel 2021 e nel 2022. Le autorità avevano denunciato delle "difficoltà incontrate da parte degli interessati nell'esercizio del loro diritto alla cancellazione dei dati", a cui Vinted avrebbe omesso di dare seguito senza fornire specifiche motivazioni, e senza chiarire perché in certi ambiti il trattamento dei dati degli utenti sarebbe proseguito anche dopo la loro richiesta di cancellazione. Inoltre, la piattaforma avrebbe implementato illecitamente un sistema di "shadow ban", ovvero una strategia per limitare la visibilità di contenuti specifici degli utenti a loro insaputa, che agisce essenzialmente come una forma di moderazione occulta, in cui i post o gli elenchi di un utente che non avrebbe rispettato le regole della community vengono nascosti alla vista del pubblico, impedendo le interazioni con i potenziali con acquirenti. Secondo quanto accertato dall'autorità, gli utenti sottoposti a questa tecnica subdola sarebbero stati costretti ad abbandonare la piattaforma senza che fossero mai stati informati di un trattamento dei loro dati personali per tale finalità, e così facendo Vinted avrebbe quindi violato i princìpi di legalità, correttezza

e trasparenza richiesti dall'art. 5, par.1, lett. a) del GDPR, creando un impatto negativo sulla capacità degli interessati di esercitare i propri diritti. In aggiunta a tali infrazioni, il Garante della privacy lituano ha inoltre ritenuto che la piattaforma non avesse adottato misure organizzative e tecniche, sufficienti a garantire l'attuazione del principio di accountability, relative al diritto di accesso. Nello specifico, l'autorità ha riscontrato che Vinted si è rifiutata di dare riscontro a una richiesta di accesso di un interessato perché quest'ultimo non era riuscito a identificare un motivo specifico per la richiesta, e pertanto l'autorità ha ritenuto che fossero stati violati anche l'art.5, par. 2 del Regolamento europeo sulla protezione dei dati e l'art. 12, commi 1 e 4, in relazione alla mancata fornitura di informazioni, comunicazioni e condizioni trasparenti per l'esercizio dei diritti degli interessati. Tutto questo ha portato l'autorità all'irrogazione di quella che in Lituania è di fatto la più elevata multa che sia mai stata comminata fin dall'introduzione del Gdpr, il cui calcolo complessivo è stato basato sulle Linee Guida 04/2022 emanate dall'European Data Protection Board con l'obiettivo di armonizzazione le metodologie di calcolo delle sanzioni amministrative pecuniarie connesse alle violazioni del Regolamento UE 2016/679 all'interno dell'area UE. Trovandosi in totale disaccordo con la decisione assunta dal Garante, dal canto suo Vinted ha già annunciato le proprie intenzioni di fare ricorso, affermando che "i casi a cui fa riferimento l'autorità lituana per la protezione dei dati non sono in alcun modo correlati alla sicurezza degli account né comportano alcun uso improprio o violazione dei dati personali degli utenti", e sostenendo di aver investito molto nella conformità e nella protezione dei propri membri, collaborando con l'autorità durante tutto il procedimento. **In Italia Vinted era stata già sanzionata nel 2022 dall'Antitrust con una multa di 1,5 milioni di euro per aver dato informazioni "ingannevoli e scorrette" agli utenti.**

Scoperto in un forum di hacking un file contenente quasi 10 miliardi di password uniche in chiaro. I ricercatori di Cybernews hanno scoperto la più grande compilation di password del mondo, denominata RockYou2024. **Un utente con nickname ObamaCare ha pubblicato su un forum di hacking un file di testo contenente quasi 10 miliardi di password uniche in chiaro**. Una precedente raccolta del 2021 aveva dimensioni inferiori.

Il file rockyou2024.txt condiviso sul forum contiene 9.948.575.739 password uniche. Il team di Cybernews ha esaminato la collezione, scoprendo che le password provengono da un mix di vecchi e nuovi data breach. Una simile raccolta, nota come RockYou2021, era stata individuata tre anni fa. In quel caso, il numero di password era circa 8,4 miliardi. È probabile che la compilation del 2024 sia stata creata dopo aver effettuato l'accesso ad oltre 4.000 database durante gli ultimi 20 anni. Non è noto se è stata messa in vendita o distribuita in forma gratuita. Una simile collezione di password rappresenta una miniera d'oro per i cybercriminali. Combinando le password con altre informazioni (ad esempio gli indirizzi email) è possibile effettuare un attacco di forza bruta per tentare di accedere agli account dei servizi online. Un'altra tecnica molto utilizzata è nota come credential stuffing. I cybercriminali possono prendere il controllo degli account, sfruttando una cattiva e pericolosa abitudine di molti utenti, ovvero l'uso delle stesse credenziali per diversi account. Per evitare rischi è necessario adottare alcune misure preventive.

Innanzitutto deve essere verificata la presenza delle credenziali nei data breach, usando strumenti sicuri, come ad esempio il sito Have I Been Pwned.

Per prudenza, è invece sempre meglio evitare di utilizzare siti web e tool che per effettuare la verifica richiedono l'inserimento delle proprie password. Se si scopre che la sicurezza delle proprie credenziali può essere compromessa, si devono cambiare le password in tutti gli account in cui sono utilizzate, scegliendo combinazioni robuste e uniche, e se possibile è anche fortemente consigliata l'attivazione dell'autenticazione a due fattori.

- N5) Sicurezza: Emergenza Caldo 2024: confermata la cassa integrazione e nuove misure in arrivo

Anche per l'estate 2024 si prevede il rinnovo degli strumenti e degli ammortizzatori sociali adottati nel 2023 per fronteggiare l'emergenza caldo. Tra le principali misure vi è la possibilità di richiedere la cassa integrazione in caso di temperature percepite superiori ai 35°, ma anche in situazioni particolari in cui la temperatura reale non raggiunge tale soglia.

Riattivazione del numero di pubblica utilità 1500

Il Ministero della Salute e l'INAIL hanno annunciato la riattivazione del numero di pubblica utilità 1500, attivo fino al 20 settembre. Questo servizio telefonico gratuito fornisce indicazioni sui comportamenti da adottare per proteggersi dalle ondate di calore e informazioni sui servizi socio-sanitari disponibili sul territorio nazionale. Quest'anno, il servizio è stato esteso anche a imprese e lavoratori, con un focus particolare sui rischi legati al caldo nei luoghi di lavoro, soprattutto per chi svolge attività all'aperto come in agricoltura e edilizia.

Incontro tra Ministero e parti sociali

Il 21 giugno si è svolto un incontro tra il Ministero e le parti sociali, sindacali e datoriali, per discutere la gestione dell'emergenza climatica. Nonostante non sia stato raggiunto un accordo definitivo, è stato confermato l'interesse a rinnovare gli strumenti e gli ammortizzatori sociali previsti la scorsa estate. Il Decreto Legge n. 98/2023 aveva già introdotto misure per i mesi tra luglio e dicembre 2023, come la neutralizzazione dei periodi di cassa integrazione per emergenza caldo e l'estensione della CIGO ai settori edile, lapideo e delle escavazioni.

Le misure previste per il 2024 includono:

1. Neutralizzazione dei periodi di cassa integrazione per emergenza caldo ai fini del calcolo dei limiti.
2. Estensione della CIGO ai settori edile, lapideo e delle escavazioni.
3. CISOA per eventi eccezionali fino al 31 dicembre, con esclusione dal calcolo dei giorni.
4. Incentivi all'adozione di linee guida e procedure per la sicurezza nei luoghi di lavoro.
5. Rinvio al 30 novembre della scadenza del versamento del contributo di solidarietà.

La cassa integrazione potrà essere adottata quando la temperatura percepita supera i 35°, ma anche in caso di temperature inferiori, a seconda del tipo di attività svolta e delle condizioni di lavoro.

Novità dalla legge di conversione del Decreto Agricoltura

Il Ministro per i Rapporti con il Parlamento, Luca Ciriani, ha annunciato che ulteriori novità potrebbero arrivare con la legge di conversione del Decreto Agricoltura (DL n. 63/2024). Durante il suo intervento alla Camera il 26 giugno, Ciriani ha spiegato che è in corso la presentazione di un pacchetto di misure per incentivare il lavoro agricolo di qualità, contrastare lo sfruttamento della manodopera e tutelare la salute dei lavoratori dall'emergenza caldo. Tra gli interventi previsti vi sono anche misure in tema di ammortizzatori sociali. Per le conferme definitive, si attende la conclusione dell'iter parlamentare del disegno di legge.

- N6) Sicurezza: Infortuni: più morti di lavoro che di mafia

Tra il 1983 e il 2018 gli omicidi riferibili alla criminalità organizzata sono stati 6.681. Nello stesso periodo i morti sul lavoro sono stati oltre 55.000

Negli ultimi 10 anni la media è stata quasi di 1.200 vittime annue sul lavoro. Secondo gli ultimi dati pubblicati dall'Inail, nel solo 2023, a fronte di 585.356 denunce totali, 1041 hanno riguardato infortuni mortali.
Il sindacato chiede al ministero della Giustizia di rendere noti i dati sui procedimenti penali in materia di incidenti sul lavoro. Nella ricerca della UIL si denuncia il fatto che 'pur a fronte di una mole straordinaria di dati statistici in materia di infortuni e decessi sul lavoro, è incredibile dover constatare come non si disponga di dati open source che possano consentire l'analisi del fenomeno dal punto di vista giudiziario e sanzionatorio penale'. Viene quindi chiesto al ministero della Giustizia di comunicare 'il numero dei procedimenti penali iscritti negli ultimi 10 anni e quelli attualmente pendenti (con distinzione per singoli uffici giudiziari) inerenti ai reati di omicidio colposo e lesioni colpose aggravati dalla violazione delle norme a tutela della salute e sicurezza sul lavoro; il numero dei procedimenti penali iscritti negli ultimi 10 anni e quelli attualmente pendenti per i reati a carico di società ed enti; il numero dei procedimenti penali iscritti negli ultimi 10 anni inerenti alle violazioni in materia di salute e sicurezza sui luoghi di lavoro; e, per tutti questi procedimenti penali, il numero e il dettaglio per ufficio giudiziario di quelli definiti con archiviazione, con condanna, con assoluzione con altre formule di proscioglimento, con prescrizione e per improcedibilità, nonché la durata media degli stessi'.
Elevata è l'incidenza dei casi mortali sul lavoro che hanno riguardato stranieri: oltre il 65% degli infortuni mortali avvenuti in occasione del lavoro nel 2023. Il dato considera solo i lavoratori regolari. Nel 2023 i sinistri mortali sul lavoro sono stati maggiori nel Mezzogiorno (sud e isole), rispetto a Centro e Nord.

- N7) D.Lgs. 231/01: le novità e modifiche al decreto 231 nei primi 6 mesi del 2024

Nel corso dei primi 6 mesi del 2024 sono intervenute varie novità e modifiche al D.Lgs. 231/01 da recepire all'interno del proprio MOG aziendale.

Di seguito si riportano le novità e modifiche:

1) Provvedimento Legge n. 90 del 28 Giugno 2024

Introduzione, abrogazione e modifica articoli del codice penale facenti parte del:

- Art. 24 del D.Lgs 231/01 (Indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture) e
- Art. 24-bis del D.Lgs 231/01 (Delitti informatici e trattamento illecito di dati). Quest'ultima fattispecie di reato è stato interamente modificato anche il testo con l'inserimento del comma 1-bis e la modifica dei commi esistenti.

2) Provvedimento D.Lgs. n. 87 del 14 Giugno 2024

Modifica testo Art. 10-quater D.Lgs n.74/2000 (Indebita compensazione) che ha interessato la fattispecie dei reati previsti dall'Art. 25-quinquiesdecies (Reati tributari) D.Lgs 231/01

3) Provvedimento D.L. n.19 del 2 Marzo 2024 coordinato con la Legge di conversione 29 aprile 2024, n. 56

Modifiche all'Art. 512-bis c.p. (Trasferimento fraudolento di valori) ha interessato la fattispecie dei reati previsti dall' 25-octies.1 (Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori) D.Lgs 231/01

4) Provvedimento Legge n.6 del 22 Gennaio 2024

Modifiche all'Art.518-duodecies p. (Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici) che ha interessato la fattispecie dei reati previsti dall'Art. 25-septesdecies (Delitti contro il patrimonio culturale) D.Lgs 231/01

La chiusura dello Studio Violi è prevista da giovedì 1 agosto a domenica 18 agosto compresi.

Per urgenze contattare l'ing. Violi al 338/6132605 o givioli@gmail.com
da lunedì 29 luglio a mercoledì 1 agosto e da lunedì 19 a venerdì 23 agosto

Buone ferie a tutti

Voglia gradire i nostri più cordiali saluti

ing. Giorgio Violi ing. Alberto Sant'Unione