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

2003-2023

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

2023 Maggio **Il nostro punto di vista su…** *Anno 16 – 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

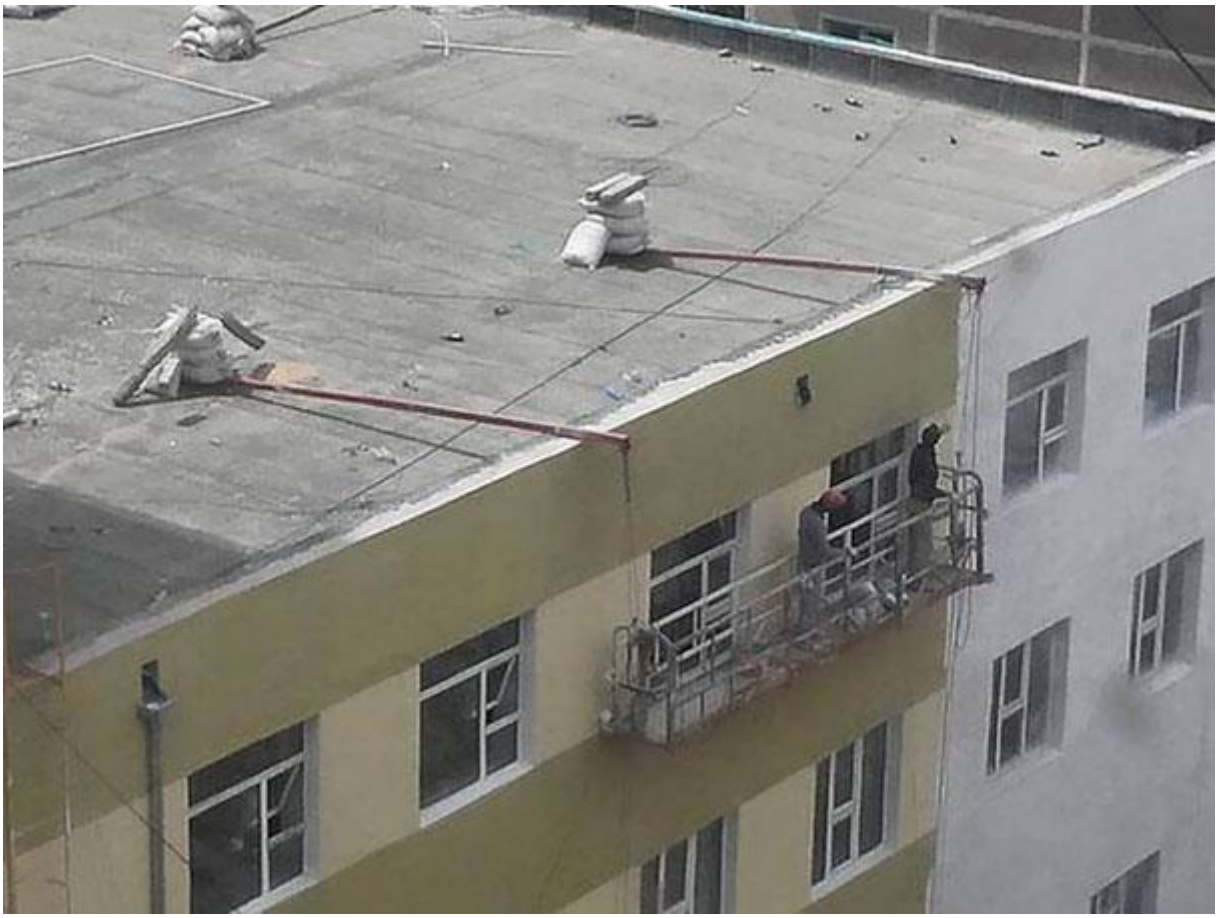
AFORISMA DEL MESE

"Il più grande pericolo per noi non è che miriamo troppo in alto e non riusciamo a raggiungere il nostro obiettivo ma che miriamo troppo in basso e lo raggiungiamo"

Michelangelo Buonarroti (pittore, scultore, architetto e poeta italiano)

Scadenziario di Maggio 2023 sul sito del Sole 24 Ore http://www.ilsole24ore.com/norme-e-tributi/scadenze.shtml

E-mail: info@studiovioli.com **SDI:** giorgiovioli@pec.it
Web: www.studiovioli.com **Fax:** 059 682304
Studio Violi Srl - Via per Capanna Tassone, 1156 41021 Ospitale - Fanano (MO)
P.I. e C.F. 02836380366 – REA 335410 CCIAA MO – Cap. Soc. € 10.000 I.V.



“Ponteggio mobile”

Notizie

- N1) D.Lgs. 231/01: Whistleblowing, obbligo di trattamento dei dati in ossequio al principio di accountability

La recente introduzione nel nostro ordinamento degli obblighi in materia di whistleblowing per i soggetti privati darà certamente un contributo importante all'emersione degli illeciti in ambito aziendale.

Ma le procedure interne di segnalazione ora richieste generano trattamenti di dati personali, anche particolari, che comportano l'adozione di cautele e misure di sicurezza da parte del titolare del trattamento.

Con il decreto legislativo 10 marzo 2023 n. 24 pubblicato sulla Gazzetta Ufficiale Serie Generale n. 63 del 15 marzo 2023 è stata data attuazione, all'interno del nostro ordinamento, alla direttiva (UE) 2019/1937 in materia di persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Quindi è stata introdotta, seppur con notevole ritardo rispetto al termine del 17 dicembre 2021 inizialmente previsto, la disciplina relativa alla protezione dei c.d. "whistleblower", termine anglosassone che letteralmente sta ad indicare i "suonatori di fischietto", ovvero i soggetti che denunciano la commissione di illeciti all'interno di organizzazioni o enti. E la ratio di questa normativa va individuata nell'evitare che questi soggetti abbiano conseguenze negative successive alla propria condotta virtuosa e che quindi desistano dai propri buoni propositi.

In effetti una normativa che spinga tutti gli operatori di mercato a segnalare e fare emergere gli illeciti in cui si imbattono non può che essere valutata positivamente e, magari nel nostro Paese più che in altri contesti, dare un contributo decisivo al miglioramento generale della cultura e dell'effettività della compliance normativa in ambito aziendale. Introdurre una tutela efficace dei diritti e delle libertà delle persone che, vincendo il timore di conseguenze negative, superino l'abitudine all'omertà in relazione a comportamenti antigiuridici fino ad oggi sottaciuti e nascosti, porterà a compiere passi in avanti, anche culturali, all'intero mondo del lavoro.

La via segnata dalla direttiva è quella di prevedere l'obbligo per i soggetti privati di introdurre delle procedure interne in grado di consentire all'interessato di effettuare le segnalazioni degli illeciti in modo da avere la certezza che queste rimangano riservate.

Il legislatore italiano ha però escluso la possibilità **che vengano effettuate segnalazioni completamente anonime, limitazione da ritenersi condivisibile in un'ottica di responsabilizzazione del segnalante e anche di trasparenza nei confronti del soggetto segnalato.**

E le tempistiche previste per l'adeguamento sono piuttosto stringenti, avendo la norma adottato un criterio dimensionale **che prevede il termine del 15 luglio 2023 per i soggetti del settore privato che abbiano impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, oltre le 249 unità.**

Sono invece tenuti all'adeguamento entro il **17 dicembre 2023 i soggetti che abbiano impiegato nell'ultimo anno la media di almeno 50 unità, o che rientrino in ambiti di attività definite "rilevanti" o che abbiano adottato i modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001 in tema di responsabilità amministrativa da reato delle società e degli enti.**

Le segnalazioni potranno avvenire attraverso i canali interni oggetto degli obblighi di cui al capoverso precedente oppure direttamente all'ANAC – Autorità Nazionale Anticorruzione in una serie di casi particolari,

ad esempio laddove il canale di segnalazione interno non sia stato attivato, non sia adempiente agli obblighi normativi o se la segnalazione interna sia già stata effettuata ma non abbia avuto seguito o possa presentarsi il rischio effettivo di ritorsioni a carico del segnalante.

I soggetti privati dovranno adottare procedure interne per le segnalazioni modellate sulle indicazioni del decreto ed effettivamente in grado di tutelare la riservatezza dei soggetti segnalanti, mettendoli al riparo da qualsiasi ingiusta conseguenza negativa.

Ulteriore elemento di interesse del decreto **è l'ampia estensione delle categorie dei soggetti segnalanti**, a partire naturalmente dai lavoratori subordinati, soggetti per definizione in una posizione di subordinazione nei confronti del datore di lavoro e dell'organizzazione per cui operano, ma anche **tutte le categorie di lavoratori parasubordinati e lavoratori autonomi, consulenti esterni o fornitori.**

In effetti anche questi soggetti che non possono considerarsi "organici" all'ente potrebbero da un lato utilmente effettuare delle segnalazioni di illeciti in cui si siano imbattiti nel corso della propria attività di outsourcer o di fornitore, dall'altro potrebbero essere anch'essi soggetti a conseguenze negative in termini di risoluzione del contratto di collaborazione o fornitura o anche di denigrazione sul mercato con danno alla propria immagine professionale. L'ampio respiro della norma che mira all'emersione degli illeciti a 360° emerge chiaramente anche da questo aspetto specifico.

Venendo al tema del trattamento dei dati personali che la novella normativa porta con sé, l'art. 13 del decreto offre una serie di indicazioni molto puntuali sull'argomento.

Innanzitutto viene sottolineato il fatto che tutti i trattamenti di dati personali conseguenti alla segnalazione degli illeciti siano soggetti alla normativa obbligatoria in materia di trattamento dati personali e quindi non sia prevista deroga alcuna. L'ente che ha adempiuto agli obblighi in materia di whistleblowing tratterà i dati relativi in qualità di titolare del trattamento e quindi di tali trattamenti sarà chiamato a rispondere.

Alla luce di questo e in ossequio al principio **dell'accountability previsto dal GDPR quindi l'azienda dovrà organizzarsi internamente e adottare le misure di sicurezza previste per garantire la riservatezza e la sicurezza dei dati trattati all'interno delle segnalazioni raccolte**.

Quindi in primo luogo i dati del segnalante, ma anche i dati degli interessati oggetto delle segnalazioni e di eventuali terzi coinvolti, fornendo adeguante informazioni circa i trattamenti di cui siano oggetto, come esplicitamente indicato al comma 4.

Il titolare del trattamento, nell'elaborazione del proprio modello organizzativo interno finalizzato alla corretta gestione delle segnalazioni, **dovrà adottare tutte le misure organizzative, informatiche e fisiche per garantire che i dati personali trattati non siano soggetti a rischi di accesso abusivo, di perdita o di trattamento illecito, facendo riferimento alle prescrizioni del GDPR e, in particolare, a quanto prescritto dall'art. 32**.

Inoltre il comma 6 del Decreto in esame fa esplicitamente riferimento alla **valutazione di impatto sulla protezione dei dati (DPIA)** regolata dall'art. 35 del Regolamento, che dovrà essere effettuata analizzando i rischi a cui sono soggetti i dati personali riferiti a tutti gli interessati coinvolti, progettando misure di sicurezza specifiche finalizzate alla riduzione del rischio in termini di probabilità e di gravità. **Un'attività di analisi molto approfondita che certamente ciascun ente dovrà portare a termine in modo accurato, essendo un obbligo esplicitamente previsto, valutando di fare ricorso al supporto di professionisti esterni specializzati in privacy, qualora tali risorse non siano presenti all'interno della propria organizzazione.**

Gli obiettivi di riservatezza delle segnalazioni saranno **in molti casi raggiunti attraverso l'utilizzo di software dedicati, già presenti sul mercato ed offerti da anni da molte aziende di servizi IT, visto che gli obblighi in termini**

di whistleblowing erano già stati introdotti per il settore pubblico dal 2001. Il Titolare del trattamento dovrà prestare la massima attenzione nella scelta dei fornitori di questi servizi informatici e valutare nel dettaglio il loro livello di affidabilità, anche dal punto di vista della privacy compliance.

In termini di qualificazione giuridica a fini privacy delle parti infatti il fornitore dovrà essere nominato responsabile del trattamento ai sensi dell'art. 28 del GDPR, come peraltro esplicitato dal comma 6 dell'art. 13 del Decreto. Diventerà così centrale la redazione del c.d. Data Protection Agreement, l'accordo di nomina a responsabile, che dovrà prevedere i diritti e i doveri delle parti e soprattutto espliciterà le misure di sicurezza con cui il fornitore proteggerà i trattamenti di dati personali svolti "per conto" del Titolare.

Da ultimo l'art. 14 del Decreto esplicita le regole in termini di conservazione delle segnalazioni e quindi anche di conservazione dei dati personali ivi contenuti.

Viene indicato come parametro il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito della segnalazione.

La previsione è coerente con il principio della privacy by default e della minimizzazione del trattamento dei dati personali, che non ammette la conservazione perpetua. Il Titolare del trattamento dovrà quindi prevedere all'interno delle procedure interne per la gestione delle segnalazioni anche delle policy interne di cancellazione dei dati personali trattati, con l'impostazione informatica all'interno degli applicativi utilizzati e la distruzione di eventuale documentazione cartacea raccolta.

Dall'esame della normativa in materia di whistleblowing emerge chiaramente come questa sia strettamente connessa al tema privacy, sia per quanto attiene al profilo della riservatezza dei dati, non solo personali, ma anche dei numerosi adempimenti specifici che l'ente dovrà adottare per trattare correttamente le informazioni raccolte. Ma soprattutto perché anche gli illeciti in materia di privacy sono ricompresi all'interno dell'elenco delle fattispecie che potranno essere oggetto di segnalazione, come indicato esplicitamente all'interno dell'art. 2 comma 1 numero 3) del Decreto, e questo aspetto potrebbe dare una notevole spinta anche alla diffusione e miglioramento della cultura della privacy compliance su tutto il territorio nazionale.

- N2) Privacy: modifiche al Decreto Trasparenza in CdM il 1/5/2023 con semplificazioni e riduzione per gli oneri dei datori di lavoro

Nel decreto Lavoro sul tavolo del Cdm del 1° maggio sono entrati una serie di semplificazioni (e chiarimenti).

In particolare, per tutta una serie di informazioni, ad esempio, **durata del periodo di prova, congedo per ferie, importo iniziale della retribuzione, programmazione dell'orario normale di lavoro, è previsto che il datore assolve all'obbligo informativo con l'indicazione del riferimento normativo o della contrattazione, anche aziendale, che disciplina queste materie**.
Inoltre, sempre per sgravare i datori, s**i stabilisce che l'azienda è tenuta a consegnare o a mettere a disposizione del personale, anche sui siti web, contratti collettivi e regolamenti aziendali applicabili al rapporto di lavoro**.

Con una novità dell'ultima ora si interviene anche **sui controlli sui lavoratori "automatizzati".**
La nuova norma chiarisce che il datore è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio **«integralmente» automatizzati** deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti su sorveglianza, valutazione, prestazioni e adempimento delle obbligazioni contrattuali dei lavoratori.

Il passo avanti è significativo. «L'inserimento della parola «integralmente» automatizzati chiarisce un delicato problema interpretativo in ordine all'individuazione dei lavoratori per i quali operano obblighi di informazione molto più complessi ed estesi – ha sottolineato il professor Arturo Maresca (diritto del Lavoro, università la Sapienza di Roma) -. Con la nuova disposizione si chiarisce che questi lavoratori sono solo quelli che sono integralmente automatizzati (vedi ad es. le "piattaforme"). E non anche quelli che operano attraverso sistemi che solo parzialmente gestiscono la loro prestazione».
In sostanza la società deve informare i lavoratori sull'utilizzo di sistemi di monitoraggio "integralmente automatizzati" deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o cessazione del rapporto di lavoro nonché indicazioni incidenti su sorveglianza, valutazione prestazioni e adempimento delle obbligazioni contrattuali dei lavoratori.

- N3) Privacy: ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei

OpenAI, la società statunitense che gestisce ChatGPT, ha fatto pervenire al Garante per la protezione dei dati personali una nota nella quale illustra le misure introdotte in ottemperanza alle richieste dell'Autorità contenute nel provvedimento dello scorso 11 aprile,

spiegando di aver messo a disposizione degli utenti e non utenti europei e, in alcuni casi, anche extra-europei, una serie di informazioni aggiuntive, di aver modificato e chiarito alcuni punti e riconosciuto a utenti e non utenti soluzioni accessibili per l'esercizio dei loro diritti. Alla luce di questi miglioramenti OpenAI ha reso nuovamente accessibile ChatGPT agli utenti italiani.

OpenAI, in particolare, ha:

- predisposto e pubblicato **sul proprio sito un'informativa rivolta a tutti gli utenti e non utenti**, in Europa e nel resto del mondo, per illustrare quali dati personali e con quali modalità sono trattati per l'addestramento degli algoritmi e per ricordare che chiunque ha diritto di opporsi a tale trattamento;
- **ampliato l'informativa sul trattamento dei dati riservata agli utenti del servizio rendendola ora accessibile anche nella maschera di registrazione** prima che un utente si registri al servizio;
- **riconosciuto a tutte le persone che vivono in Europa, anche non utenti, il diritto di opporsi a che i loro dati personali siano trattati per l'addestramento degli algoritmi** anche attraverso un apposito modulo compilabile online e facilmente accessibile;
- **ha introdotto una schermata di benvenuto alla riattivazione di ChatGPT in Italia**, con i rimandi alla nuova informativa sulla privacy e alle modalità di trattamento dei dati personali per il training degli algoritmi;
- **ha previsto per gli interessati la possibilità di far cancellare le informazioni ritenute errate** dichiarandosi, allo stato, tecnicamente impossibilitata a correggere gli errori;
- **ha chiarito, nell'informativa riservata agli utenti**, che mentre continuerà a trattare taluni dati personali per garantire il corretto funzionamento del servizio sulla base del contratto, tratterà i loro dati personali ai fini dell'addestramento degli algoritmi, salvo che esercitino il diritto di opposizione, sulla base del legittimo interesse;
- **ha implementato per gli utenti già nei giorni scorsi un modulo che consente a tutti gli utenti europei di esercitare il diritto di opposizione** al trattamento dei propri dati personali e poter così escludere le conversazioni e la relativa cronologia dal training dei propri algoritmi;
- ha **inserito nella schermata di benvenuto riservata agli utenti italiani già registrati al servizio un pulsante attraverso il quale, per riaccedere al servizio, dovranno dichiarare di essere maggiorenni o ultratredicenni** e, in questo caso, di avere il consenso dei genitori;
- **ha inserito nella maschera di registrazione al servizio la richiesta della data di nascita prevedendo un blocco alla registrazione per gli utenti infratredicenni** e prevedendo, nell'ipotesi di utenti ultratredicenni ma minorenni che debbano confermare di avere il consenso dei genitori all'uso del servizio.

L'Autorità garante esprime soddisfazione per le misure intraprese e auspica che OpenAI, nelle prossime settimane, ottemperi alle ulteriori richieste impartitele con lo stesso provvedimento dell'11 aprile con particolare riferimento all'implementazione di un sistema di verifica dell'età e alla pianificazione e realizzazione di una campagna di comunicazione finalizzata a informare tutti gli italiani di quanto accaduto e della possibilità di opporsi all'utilizzo dei propri dati personali ai fini dell'addestramento degli algoritmi.
L'Autorità garante riconosce i passi in avanti compiuti per coniugare il progresso tecnologico con il rispetto dei diritti delle persone e auspica che la società prosegua lungo questo percorso di adeguamento alla normativa europea sulla protezione dati.
L'Autorità garante proseguirà dunque nell'attività istruttoria avviata nei confronti di OpenAI e nel lavoro che porterà avanti la apposita task force costituita in seno al Comitato che riunisce le Autorità per la privacy dell'Unione europea.
Commento: vedremo gli sviluppi operativi e concreti su questo pericolo potenziale per tutti noi dopo le prese di posizioni negative di Musk e di premi Nobel sullo sviluppo incontrollato e sulle problematiche sul diritto di autore per i testi redatti dalla intelligenza artificiale.

- N4) Privacy: Videosorveglianza: non basta l'ok dei dipendenti per installare le telecamere in azienda

Sul controllo a distanza, i lavoratori non possono sostituirsi al sindacato.

Anche se fossero tutti d'accordo a far installare, ad esempio, le telecamere nell'azienda, in mancanza del placet della rappresentanza sindacale (Rsa o Rsu) l'installazione sarebbe illegittima e il datore di lavoro penalmente responsabile.

Lo precisa l'Inl nella nota 2572/2023 in cui fornisce indicazioni sul rilascio del provvedimento di autorizzazione all'installazione di strumenti di controllo diretto o indiretto dei lavoratori, in considerazione anche degli orientamenti del Garante Privacy. **L'Inl precisa, inoltre, che la disciplina vale anche per rider e co.co.co. di terza generazione, ma non per i volontari.**

Le nuove indicazioni riguardano, dunque, il divieto fissato all'art. 4 dello Statuto dei lavoratori (legge 300/1970) dei c.d. "controlli a distanza" dei lavoratori, in base al quale non è possibile far "uso d'impianti audiovisivi e altri strumenti che abbiano quale finalità esclusiva il controllo a distanza dell'attività dei lavoratori". Se l'installazione non ha queste finalità, ma dall'utilizzo è comunque possibile il controllo dei lavoratori, la stessa norma detta le modalità attraverso cui il datore di lavoro può essere autorizzato.

Due le procedure dell'autorizzazione, necessariamente prioritaria all'installazione di impianti. **La prima è di tipo sindacale: sottoscrizione d'intesa tra azienda e sindacati (Rsa o Rsu). Se tale accordo sindacale non è raggiunto, l'azienda può far ricorso alla seconda modalità: richiesta di autorizzazione all'ispettorato.**

Tenuto conto che il bene giuridico tutelato ha natura collettiva e non individuale, **precisa l'Inl, la mancanza di accordo tra datore di lavoro e rappresentanze sindacali o del provvedimento di autorizzazione non può essere supplita dall'eventuale consenso, seppur informato, di tutti i singoli lavoratori; in tal caso, l'installazione resta illegittima e penalmente sanzionata.**

Poiché la disciplina si applica alle aziende con lavoratori, spiega ancora l'Inl, gli ispettori possono e devono intervenire soltanto in realtà con presenza di lavoratori. **Tuttavia, si può verificare il caso di un'azienda di nuova costituzione che, alla presentazione dell'istanza di autorizzazione, non ancora abbia in forza lavoratori, che prevede di assumere una volta avviata l'attività. In tal caso, precisa l'Inl, è possibile richiedere l'autorizzazione indicando il numero dei lavoratori da assumere.** Oppure si può verificare che un'azienda già in esercizio, con un impianto legittimamente installato ma senza lavoratori, proceda ad assunzioni ricadendo, così, negli obblighi dell'art. 4. In tal caso, pur avendo l'azienda già installato e messo in funzione l'impianto, può fare istanza producendo, contestualmente, attestazione che l'impianto è disattivato e che, non appena il personale sarà adibito al lavoro, sarà messo di nuovo in funzione solo dopo eventuale provvedimento di autorizzazione.

Campo di applicazione. Infine, l'Inl precisa che la disciplina dell'art. 4 si applica anche alle co.co.co. che si concretano in prestazioni prevalentemente personali, continuative ed eseguite secondo modalità etero organizzate, anche se organizzate su piattaforme digitali e pure ai lavoratori autonomi tramite piattaforme digitali. **Ne restano esclusi, invece, i volontari per l'incompatibilità della qualità di volontario con qualsiasi forma di rapporto di lavoro, subordinato o autonomo**.

-N5) Privacy: Garante privacy, no all'uso di modalità ingannevoli - Sanzionata una digital company

Garante privacy, no all'uso di modalità ingannevoli - Sanzionata una digital company Il Garante privacy ha sanzionato una società che offre servizi di digital marketing **con una multa di 300mila euro** per aver trattato in modo illecito dati personali a fini di marketing. La digital company veicolava agli utenti presenti nel proprio database i messaggi ricevuti dalle società sue clienti (tutte di medio-grande dimensione e alcune molto conosciute) per effettuare campagne promozionali via sms, email e attraverso chiamate automatizzate. Il database era costituito da dati raccolti direttamente dalla società attraverso i propri portali online (di notizie, concorsi a premi, curiosità, ricette di cucina), ma anche da informazioni personali acquistate da broker di dati. Dalle verifiche effettuate dall'Autorità, è emerso che in alcuni dei portali di proprietà della società, venivano utilizzati i cosiddetti "modelli oscuri" (dark patterns) che, attraverso interfacce grafiche opportunamente realizzate e altre modalità potenzialmente ingannevoli, invogliavano l'utente a prestare il consenso al trattamento dei dati per finalità di marketing e alla comunicazione dei dati a terzi sempre per la stessa finalità. Negli stessi portali, l'Autorità ha rinvenuto una serie di altre violazioni, a partire dalla incapacità della società di dimostrare, in alcuni casi, l'acquisizione del consenso per l'invio di messaggi promozionali, fino all'obbligo per l'utente di fornire risposte sulle sue abitudini di acquisto o alla richiesta di inserire i dati di contatto (nome, email) di amici potenzialmente interessati ai servizi offerti. Da ultimo, anche l'invito a cliccare su un link che conduceva ad un altro sito per scaricare un e-book, con i dati di profilo dell'utente già riconosciuti e i consensi privacy già tutti selezionati. L'Autorità inoltre, ricordando le verifiche da effettuare nel caso di acquisizione di banche dati da terzi, si è pronunciata in merito alla corretta ripartizione dei ruoli in ordine al trattamento dei dati personali tra le parti commerciali coinvolte nella filiera del marketing digitale.

- N6) Sicurezza: Inail, nei primi tre mesi infortuni in calo ma aumentano gli incidenti mortali

Per il presidente Inail, Franco Bettoni, «il quadro è drammatico e va contrastato con ogni mezzo». Il ministro del Lavoro Marina Calderone: «Agire insieme giorno per una cultura condivisa»

Nel primo trimestre 2023 diminuiscono gli infortuni sul lavoro, **grazie al calo delle denunce da contagio da Covid**, mentre crescono gli incidenti mortali.

Secondo quanto riferisce l'Inail, le denunce di infortunio sul lavoro presentate all'Istituto entro il mese di marzo sono state 144.586 (-25,5% rispetto allo stesso periodo del 2022), mentre sono state 196 quelle che hanno riguardato incidenti con esito mortale (+3,7%). **Sono in aumento le patologie di origine professionale denunciate, che sono state 18.164 (+25,1%).** I dati diffusi in occasione della Giornata mondiale per la salute e la sicurezza sul lavoro, come spiega il presidente dell'Inail, Franco Bettoni, si tratta di «un andamento drammatico che va contrastato con ogni mezzo. È dunque indispensabile insistere per consolidare ulteriormente la sinergia tra istituzioni, parti sociali, lavoratrici, lavoratori e imprese, sollecitando un confronto costante con l'obiettivo di diffondere la cultura della prevenzione per la crescita sociale ed economica del Paese». A questo proposito il ministro Marina Calderone ha sottolineato che «dobbiamo parlare quotidianamente di salute e sicurezza sul lavoro, in tutti i luoghi di formazione e di lavoro». Per il ministero meritano un plauso i progetti di legge per l'introduzione dell'insegnamento del diritto del lavoro e della sicurezza nei luoghi di lavoro nelle scuole secondarie all'esame di Montecitorio, perché, spiega il ministro «permettono al Parlamento di essere protagonista in una materia che non può avere colore politico. Salute e sicurezza nei luoghi di lavoro sono stati, sono e saranno temi fondanti del diritto dei lavoratori».

Voglia gradire i nostri più cordiali saluti *ing. Giorgio Violi* *ing. Alberto Sant'Unione*

PregandoLa di scusarci per il disturbo eventualmente arrecato, Le comunichiamo che i Suoi dati sono registrati nel Database Studio Violi srl e questo messaggio Le è stato inviato confidando che i temi trattati potessero essere di Suo interesse. In ottemperanza al Reg. 679/2016/UE, qualora non desiderasse più ricevere questo mensile dallo Studio Violi srl (titolare del trattamento dei dati), può comunicarcelo via mail all'indirizzo info@studiovioli.com. Garantiamo in ogni momento il rispetto di tutti i diritti di cui al Reg. 679/2016/UE.
Credits:si ringraziano le società che hanno facilitato la stesura del presente con la fornitura di parte del materiale, in particolare garante privacy, punto sicuro, ats, ipsoa, il sole24ore, tuttoambiente, iae, quotidiano sicurezza.it, privacylawconsulting, la repubblica, italia oggi, epc, postilla, necsi. Può inoltre contare sulla ns disponibilità ad approfondire i temi qui trattati