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

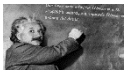
2023 Ottobre **Il nostro punto di vista su…** *Anno 16 – 2° sem*

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

"Ci sono abbastanza risorse per soddisfare i bisogni di ogni uomo, ma non l'avidità di ogni uomo"
Gandhi – politico, filosofo e avvocato indiano

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.

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

“Potatura autunnale: dov’è l’errore?” *risposta a fine pagina

* la scala con il taglialegna è appoggiata al ramo che viene tagliato e che cadrà... con la scala

Notizie

- N1) D.Lgs. 231/01: Sanzione "231" per l'infortunio sul lavoro

Scatta la sanzione ex "231" alla società anche se l'infortunio sul lavoro è successo perché l'impresa ha voluto risparmiare tempo più che soldi: la cautela necessaria non risulta adottata dall'azienda per evitare di rallentare l'attività in cantiere.

Il punto è che, dopo il reato di lesioni personali colpose contestato al datore, **la responsabilità amministrativa dell'ente si configura anche quando alla violazione delle norme antinfortunistiche corrisponde un modesto risparmio di spesa**: ciò che conta ai fini della responsabilità è che la società abbia un interesse o un vantaggio dalla condotta contro legge addebitata agli amministratori.

È quanto emerge dalla sentenza 39129/2023, pubblicata il 26 settembre dalla terza sezione penale della Cassazione.

Diventa definitiva la condanna inflitta all'impresa edile dopo che l'operaio è rimasto in parte schiacciato dal cancello scorrevole uscito dalle guide. Alla srl si imputa la violazione delle norme antinfortunistiche per non aver adottato le necessarie misure di sicurezza all'ingresso del cantiere. Non giova alla difesa dedurre che dall'omissione la società non ottiene alcun risparmio di spesa perché riparare il cancello le sarebbe costato solo qualche decina di euro. In realtà l'intervento di manutenzione era necessario da tempo e sull'accesso al cantiere non risultava installata la segnaletica informativa. La mancata riparazione, insomma, è dettata dalla necessità «di non incidere sui tempi delle attività».

Soprattutto la responsabilità dell'ente si configura anche quando risultano esigui il vantaggio ottenuto o l'interesse perseguito dalla società con la violazione antinfortunistica: anche la mancata adozione di cautele che comportano spese modeste può determinare reati colposi di evento in materia di sicurezza sul lavoro, anche con conseguenze serie.

La sanzione "231", infine, può scattare anche se la violazione delle norme antinfortunistiche non risulta sistematica ma integrata da una trasgressione isolata dovuta a un'iniziativa estemporanea, quando risulta provato che l'infrazione è legata all'interesse dell'ente.

- N2) Privacy: In Italia gli attacchi ransomware sono aumentati del 34,6% e l'80% delle vittime sono PMI

Nel secondo trimestre 2023, il fenomeno del ransomware è cresciuto del +34,6% in Italia e del +62% a livello globale rispetto al trimestre precedente. A rilevarlo è l'ultimo report "Threatland" curato dal Security Operation Center (SOC) e dal Team di Cyber Threat Intelligence di Swascan.

Il numero delle aziende vittime delle gang ransomware è aumentato del 185% dall'inizio dell'anno e del 105% rispetto al secondo trimestre del 2022.

In Italia, l'80% delle vittime colpite sono Pmi e il 91% sono aziende con fatturato inferiore ai 250 milioni di euro.

Secondo il report che analizza i principali rischi informatici (**ransomware, phishing e malware**) tra aprile e giugno scorsi in Italia si sono registrati numerosi attacchi informatici che hanno coinvolto soprattutto aziende di servizi. Circa 190 mila i dispositivi compromessi in Italia.

La cyber-gang "Monti" quella più attiva nel nostro Paese.

Stando al rapporto di Swascan, sono state 1451 le vittime (colpite e soggette a pubblicazione di dati rubati) a livello globale di questi attacchi, caratterizzati dalla diffusione di software malevoli che criptano dati per il cui ripristino si chiede il pagamento di un riscatto.
Si registra anche un incremento delle gang di cybercriminali dietro questi attacchi il cui numero di è salito da 36 a 43 (+19,4%). Lockbit si distingue come la più attiva, avendo orchestrato ben 245 attacchi nel corso del trimestre. Questi attacchi sembrano avere un obiettivo preciso: le aziende.
Le aziende di servizi sono state le più colpite, rappresentando il 47% degli attacchi, seguite da quelle del settore manufatturiero (16%) e tecnologico (6%).
Anche in Italia, il settore dei servizi è in cima alla lista con il 54% degli attacchi, seguito dal manufatturiero (11%) e dal sanitario (9%), più che raddoppiato rispetto al trimestre precedente. Tuttavia, la minaccia non ha risparmiato altri settori, tra cui il finanziario, il manifatturiero, l'immobiliare, ecc.

- N3) Privacy: Ispezioni del Garante Privacy, aziende e DPO pronti ad affrontarle con procedure interne e simulazioni

Lo scorso anno un rapporto dell'Osservatorio di Federprivacy ha rivelato che il 54% dei Data Protection Officer (DPO) vede una possibile ispezione del Garante della Privacy alla stregua di un'emergenza, e questo mette in evidenza che le aziende non possono stare alla sorte sperando che il Nucleo Privacy della Guardia di Finanza o la stessa Autorità non bussino mai alla loro porta, ma devono tenersi sempre pronte a una tale eventualità.

Procedure interne - Riguardo all'opportunità di farsi trovare pronti di fronte a una inaspettate ispezione, vi sono peraltro grandi aziende operanti in settori in cui i trattamenti di dati personali rivestono particolari criticità, che hanno incluso nelle proprie procedure interne manuali e documenti come "**Vademecum delle prassi per la cooperazione con Garante Privacy", in cui hanno stabilito in anticipo come affrontare tali situazioni, individuando ad esempio ruoli di responsabilità nel presidiare la PEC aziendale e nel ricevere i funzionari dell'autorità, come allertare le funzioni da coinvolgere sia per gli aspetti normativi che quelli relativi alla cybersecurity, verificare tempestivamente che tutta documentazione potenzialmente richiesta dagli ispettori sia pronta per essere messa a loro disposizione, e come cooperare diligentemente con essi per tutta la durata dell'attività ispettive**.
Questo approccio, oltre che a stabilire cosa fare e come fare per non farsi cogliere impreparati in tali circostanze, è sicuramente utile per evitare di andare nel panico se l'autorità si dovesse presentare all'ingresso dell'azienda con scarso o nessun preavviso.

Ruolo del DPO - In questo contesto, il Data Protection Officer ha un ruolo cruciale, in quanto trai principali compiti che gli sono assegnati dall'art. 39 b) del Regolamento UE 2016/679 egli deve sorvegliare l'osservanza dello stesso GDPR e delle altre disposizioni dell'UE o degli Stati membri relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento, "comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo", definizione quest'ultima che non a caso è resa "audit" nella versione inglese del Regolamento europeo.

Attività di Audit - E proprio l'audit è uno degli strumenti più efficaci che può aiutare un'azienda a svolgere una periodica attività di monitoraggio per verificare il livello della propria compliance al GDPR.
Tali audit possono essere svolti a più livelli, e nella prassi **quelli di prima parte** sono effettuati in modo indipendente dallo stesso DPO e/o dai suoi collaboratori, prestando attenzione a non incorrere in un potenziale conflitto d'interesse che potrebbe derivare ad esempio dal controllo di processi aziendali in cui egli stesso è coinvolto con il rischio di "controllare sé stesso". Naturalmente, un audit di prima parte presuppone che l'organizzazione esaminata disponga di un sistema di gestione della privacy aziendale che ne individui chiaramente requisiti, criteri ed altre regole che devono essere note alle funzioni sottoposte all'esaminazione.
Gli audit di seconda parte, sono invece svolti verso organizzazioni esterne su cui si hanno interessi particolari, e nell'ambito della compliance GDPR vi rientrano sicuramente quei fornitori in outsourcing che trattano dati personali per conto dell'azienda titolare, e che per questo devono essere designate come "responsabili del trattamento" ai sensi dell'art.28 del Regolamento europeo, con l'obbligo di "mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del suddetto articolo, consentendo e contribuendo alle attività di revisione, comprese le ispezioni realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato".
Vi sono infine gli audit di terza parte, che il titolare del trattamento può commissionare ad un organismo di certificazione esterno accreditato, il quale svolge attraverso propri esperti da esso incaricati la sua attività di audit in modo del tutto indipendente e con maggiori garanzie di poter avere poi risultanze finali obiettive senza il rischio che possano essere in qualche modo "autoreferenziali" oppure influenzate da compiacenze in cui si potrebbe scivolare quando gli audit vengono svolti "tra colleghi" che rispondono allo stesso management.

Simulazione di ispezione - Se da una parte, delle procedure che indicano a tutte le funzioni coinvolte come comportarsi in tali casi contribuiscono ad attivarsi in modo ordinato e coerente, non possono però tenere conto del fattore umano, e non è possibile sapere come il team e lo stesso DPO reagiranno di fronte all'improvvisa apertura di uno stato di crisi, come è un'ispezione sulla privacy, almeno fino al momento in cui non si troveranno effettivamente a tu per tu con le fiamme gialle o con i funzionari del Garante.
L'unico strumento che può realisticamente rivelarlo, e che per certi versi può superare addirittura l'utilità degli audit, è plausibilmente uno "stress test" che si può effettuare attraverso una simulazione più rassomigliante possibile a quello che sarebbe lo scenario di una vera ispezione del Garante.
Nessun audit, seppur realizzato in modo ineccepibile, **può infatti testare quale può essere la reazione se il team riceve una PEC che avverte l'arrivo di una ispezione del Nucleo Privacy al mattino seguente, o se un ufficiale delle fiamme gialle suona al campanello dell'azienda, e se durante l'ispezione i funzionari del Garante interrogano e mettono sotto pressione il DPO**, il CISO, ed altre persone interessate da potenziali violazioni, chiedendo loro di esibire valutazioni d'impatto ed altri documenti, e forse osservando senza troppe galanterie le non conformità riscontrate.

-N4) Privacy: Garante Privacy, il piano delle attività ispettive per il secondo semestre 2023; Videocamere, email, e investigazioni: la privacy del lavoratore non è un diritto assoluto

Garante Privacy, il piano delle attività ispettive per il secondo semestre 2023: nel mirino riconoscimento facciale, telemarketing, e cookies Il Garante per la protezione dei dati personali ha varato il piano delle proprie attività ispettive relative al secondo semestre del 2023. Sotto la lente dell'autorità vi saranno in particolare il settore della statistica e della ricerca scientifica, il telemarketing, il riconoscimento facciale, i gestori ed i fornitori di servizi che utilizzano lo SPID e la carta d'identità elettronica (CIE) nell'ambito di servizi online offerti anche tramite app, nonché i cookie e gli altri strumenti di tracciamento. Come previsto del Regolamento del n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio del Garante per la protezione dei dati personali (doc. web. n. 1098801), l'autorità ha infatti pubblicato la Deliberazione del 3 agosto 2023 rendendo note quelle che saranno le attività ispettive a cui sarà data la priorità nella seconda parte dell'anno, che nel dettaglio sono le seguenti:

a) accertamenti nel settore della statistica e della ricerca scientifica con specifico riferimento alle misure di cui all'art. 89 del Regolamento UE 2016/679 (GDPR) e in particolare alla tematica della pseudonimizzazione;

b) accertamenti sui trattamenti di dati personali da parte di operatori del settore energetico con specifico riferimento all'attivazione di contratti non richiesti e allo svolgimento di attività di telemarketing, nell'attuale contesto di superamento del c.d. mercato tutelato;

c) accertamenti riferiti ai trattamenti di dati biometrici mediante riconoscimento facciale, (anche) nell'ambito del rapporto di lavoro;

d) prosecuzione delle ispezioni sui gestori dell'identità digitale (SPID) e sui soggetti di cui essi si avvalgono per il rilascio di servizi fiduciari (SPID e firma digitale) nonché sui fornitori di servizi che utilizzano SPID e CIE nell'ambito di servizi online (offerti anche tramite APP);

e) prosecuzione delle verifiche in ordine alla corretta implementazione delle Linee guida sui cookie e gli altri strumenti di tracciamento anche attraverso lo strumento degli accertamenti on line;

f) altri accertamenti nei confronti di soggetti pubblici e privati, al fine di verificare l'osservanza delle disposizioni in materia di protezione dei dati personali, ivi incluse le istruttorie relative a reclami e segnalazioni formali proposti all'Autorità ed in istruttoria presso i relativi Dipartimenti e Servizi.

Anche se in linea di principio le ispezioni del Garante vengono effettuate fisicamente presso le sedi dei soggetti interessati, l'autorità potrà svolgere la propria attività anche da remoto con accertamenti online in riferimento a trattamenti di dati personali effettuati tramite siti internet da parte di titolari del trattamento pubblici e privati.

Le ispezioni del Garante consistono nella verifica della correttezza di tutti i sistemi di acquisizione, archiviazione, protezione, gestione e cancellazione dei dati personali trattati da un'azienda, e non si tratta di controlli puramente formali o documentali, ma sono volte ad accertare che i trattamenti di dati personali avvengano in conformità al Gdpr e alla normativa correlata in materia di protezione dei dati personali.

Come previsto dal protocollo di intesa con la Guardia di finanza del 30 marzo 2021, le ispezioni saranno effettuate in collaborazione con il Nucleo Speciale Tutela privacy e frodi informatiche delle fiamme gialle, e oltre alle attività programmate il Garante ed il Nucleo Speciale potranno naturalmente condurre ulteriori attività ispettive a seguito di segnalazioni o di reclami da parte degli interessati.

Videocamere, email, e investigazioni: la privacy del lavoratore non è un diritto assoluto La privacy del lavoratore non è un diritto assoluto. Negli anni la giurisprudenza ha dettato precisi confini per bilanciare da un lato la tutela alla riservatezza e la dignità dei dipendenti; dall'altro la protezione del patrimonio e dell'immagine aziendale.

Non sempre i contorni sono chiari e definiti, dando luogo a un contenzioso che negli ultimi anni ha riguardato soprattutto:

- l'uso delle videocamere di sorveglianza;
- il controllo delle email aziendali;
- l'impiego di agenzie investigative per rilevare e contestare condotte illecite dei dipendenti.

I controlli - Intanto occorre distinguere tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti o gruppi di dipendenti nello svolgimento della loro prestazione di lavoro, che dovranno necessariamente essere realizzati nel rispetto dell'articolo 4 dello Statuto dei Lavoratori e "controlli difensivi" in senso stretto, diretti ad accertare specifiche condotte illecite ascrivibili – in base a concreti indizi – a singoli dipendenti.vQuesti ultimi controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, possono essere effettuati dal datore di lavoro anche senza le garanzie previste dall'articolo 4 dello Statuto dei lavoratori, cioè senza l'autorizzazione dell'ispettorato nazionale del lavoro o dei sindacati e senza informare preventivamente il lavoratore.

Così il datore di lavoro potrà installare telecamere nascoste nel caso di ripetuti ammanchi di cassa o furti e ragionevoli sospetti in capo a determinati lavoratori. Il controllo dovrà essere mirato e giustificato, non potendo in ogni caso legittimare un controllo costante e preventivo rispetto al fatto illecito.

La posta elettronica - Applicando gli stessi principi è lecito il controllo delle email aziendali, a condizione che il lavoratore sia stato adeguatamente informato, che il controllo sia proporzionato alle finalità e non sia un controllo massivo. In via generale non possono invece essere controllate le email personali, ma potrà essere sanzionato un utilizzo illecito delle mail personali o dei social network

durante l'orario di lavoro. L'informativa al lavoratore non deve essere necessariamente scritta, ma può diventare difficile in sede processuale dimostrare con testimoni l'avvenuta informazione circa i limiti e le modalità dei controlli tecnologici.
Tra i comportamenti più gravi ascrivibili al lavoratore e accertabili tramite i controlli periodici delle email aziendali rientra sicuramente la violazione dell'obbligo di fedeltà nei confronti del datore di lavoro prescritto dall'articolo 2105 del Codice civile.
Così è stato ritenuto legittimo il licenziamento della dipendente che trafuga informazioni riservate per svolgere attività concorrenziale (Tribunale di Roma, Sezione lavoro, sentenza 4032, pubblicata il 5 maggio 2023).
Investigazioni private - Altrettanto lecite sono le riprese effettuate dall'investigatore privato incaricato di sorvegliare il dipendente che effettuava attività di pulizie per una piscina privata durante l'assenza per malattia. Come specificato più volte dalla giurisprudenza, infatti, in questi casi il trattamento dei dati personali, ammesso di norma in presenza del consenso dell'interessato, può essere eseguito anche in assenza perché serve a far valere o difendere un diritto in sede giudiziaria o per svolgere le investigazioni difensive. Ovviamente anche in questi casi i dati devono essere trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento (Tribunale di Perugia, sezione lavoro sentenza 129 pubblicata il 30 luglio 2022).
Il casellario giudiziale - Una questione controversa riguarda la possibilità del datore di lavoro di chiedere i carichi pendenti e il casellario giudiziale in fase di selezione. In realtà la Corte di cassazione con un orientamento più recente ha sdoganato tali richieste, anche quando non previsto dal contratto collettivo nazionale applicabile al rapporto di lavoro. Anche in fase precontrattuale, infatti, il datore di lavoro è libero di determinare criteri rigidi che prevedano, ad esempio, l'assenza di processi penali in corso, potendo legittimamente procedere ad una verifica dei requisiti di affidabilità dei lavoratori da assumere ai sensi dell'articolo 41 della Costituzione (Tribunale di Roma, Sezione lavoro, sentenza 6030 pubblicata il 23 giugno 2023).
In alcuni casi poi è addirittura obbligatorio richiedere il certificato del casellario giudiziale per il datore di lavoro, ad esempio nelle attività professionali o volontarie che comportino contatti diretti e regolari con minori, così come previsto dal Dlgs. 39/2014.

- N5) Sicurezza: Infortuni e malattie professionali: i dati dei primi otto mesi del 2023

Le denunce di infortunio sul lavoro presentate all'INAIL entro il mese di agosto sono state 383.242 (-20,9% rispetto ad agosto 2022), 657 delle quali con esito mortale (-3,0%). In aumento le patologie di origine professionale denunciate (+23,2%).

Nella sezione "Open data" del sito Inail sono disponibili i dati analitici delle denunce di infortunio– nel complesso e con esito mortale – e di malattia professionale presentate all'Istituto entro il mese di agosto. Nella stessa sezione sono pubblicate anche le tabelle del "modello di lettura" con i confronti "di mese" (agosto 2022 vs agosto 2023) e "di periodo" (gennaio-agosto 2022 vs gennaio-agosto 2023). Il confronto effettuato su un medio periodo, tuttavia, potrebbe rivelarsi poco attendibile rispetto al trend che si delineerà nei prossimi mesi. Per un'analisi più indicativa dell'andamento infortunistico, infatti, sarà necessario attendere un lasso di tempo maggiore, anche per tener conto di eventuali ritardi nelle denunce di infortunio, in particolare di quelle con esito mortale, pervenute all'Inail.
Ciò premesso, nei primi otto mesi di quest'anno si registra, rispetto all'analogo periodo del 2022, una decisa riduzione delle denunce di infortunio in complesso (dovuta quasi esclusivamente al notevole minor peso dei casi di contagio da Covid-19), un calo di quelle mortali e una crescita delle malattie professionali.

DENUNCE DI INFORTUNIO

Le denunce di infortunio presentate all'Inail entro il mese di agosto 2023 sono state 383.242, in calo rispetto alle 484.561 dei primi otto mesi del 2022 (-20,9%), in aumento rispetto alle 349.449 del 2021 (+9,7%) e alle 322.132 del 2020 (+19,0%), e in diminuzione rispetto alle 416.894 del 2019 (-8,1%).
A livello nazionale i dati rilevati al 31 agosto di ciascun anno evidenziano, per i primi otto mesi del 2023 rispetto all'analogo periodo dell'anno precedente, un decremento dei casi avvenuti in occasione di lavoro, passati dai 429.161 del 2022 ai 323.946 del 2023 (-24,5%), mentre quelli in itinere, occorsi cioè nel tragitto di andata e ritorno tra l'abitazione e il posto di lavoro, hanno fatto registrare un aumento del 7,0%, da 55.400 a 59.296.

L'analisi territoriale evidenzia una diminuzione delle denunce di infortunio in tutte le aree del Paese: più consistente al Sud (-27,3%) e nelle Isole (-26,7%), seguite da Nord-Ovest (-24,3%), Centro (-20,7%) e Nord-Est (-12,9%). Tra le regioni con i maggiori decrementi percentuali si segnalano la Campania, la Liguria, il Molise e il Lazio.

Il calo che emerge dal confronto del periodo gennaio-agosto 2022 e 2023 è legato sia alla componente femminile, che registra un -34,5% (da 204.383 a 133.898 casi denunciati), sia a quella maschile, che presenta un -11,0% (da 280.178 a 249.344). Il decremento ha interessato sia i lavoratori italiani (-24,2%) sia quelli comunitari (-17,0%) ed extracomunitari (-1,4%). Dall'analisi per classi di età emergono diminuzioni in tutte le fasce tranne quella degli under 20, che registra un +12,6% dovuto principalmente all'aumento infortunistico degli studenti.

CASI MORTALI

Le denunce di infortunio sul lavoro con esito mortale presentate all'Istituto nei primi otto mesi 2023 sono state 657, 20 in meno rispetto alle 677 registrate nel periodo gennaio-agosto 2022, 115 in meno rispetto al 2021, 166 in meno rispetto al 2020 e 28 in meno rispetto al 2019.

A livello nazionale i dati rilevati al 31 agosto di ciascun anno evidenziano per i primi otto mesi del 2023 rispetto al pari periodo del 2022, pur nella provvisorietà dei numeri, un decremento solo dei casi mortali in itinere, scesi da 181 a 157, mentre quelli avvenuti in occasione di lavoro passano da 496 a 500. Il calo ha riguardato sia l'Industria e servizi (da 573 a 564 decessi) sia l'Agricoltura (da 83 a 73) e il Conto Stato (da 21 a 20).
Dall'analisi territoriale emerge un calo nel Nord-Est (da 152 a 141 casi), al Centro (da 142 a 126) e nelle Isole (da 59 a 57), un incremento al Sud (da 142 a 151) e una stabilità nel Nord-Ovest (182 in entrambi i periodi). Le regioni che presentano i maggiori aumenti sono Friuli Venezia Giulia (+11 casi mortali), Abruzzo (+10), Liguria (+9), Lombardia e Campania (+5 ciascuna), mentre i cali più evidenti sono quelli di Toscana (-14), Emilia Romagna e Piemonte (-8 ciascuna), e Valle d'Aosta (-6).

DENUNCE DI MALATTIA PROFESSIONALE

Le denunce di malattia professionale protocollate dall'Inail nei primi otto mesi del 2023 sono state 48.514, oltre novemila in più rispetto allo stesso periodo del 2022 (+23,2%). L'incremento è del 32,9% rispetto al 2021, del 74,8% sul 2020 e del 18,2% rispetto al 2019.
I dati rilevati al 31 agosto di ciascun anno mostrano un aumento del 24,1% nella gestione Industria e servizi (da 32.298 a 40.080 casi), del 18,8% in Agricoltura (da 6.723 a 7.986) e del 29,5% nel Conto Stato (da 346 a 448). L'incremento delle denunce interessa tutte le aree del Paese, a partire dal Sud (+27,6%), seguito da Nord-Ovest (+26,2%), Isole (+25,4%), Nord-Est (+21,2%) e Centro (+20,2%).
In ottica di genere si rilevano 6.469 denunce di malattia professionale in più per i lavoratori, da 29.087 a 35.556 (+22,2%), e 2.678 in più per le lavoratrici, da 10.280 a 12.958 (+26,1%). L'aumento ha interessato sia le denunce dei lavoratori italiani, che sono passate da 36.365 a 44.590 (+22,6%), sia quelle dei comunitari, da 991 a 1.197 (+20,8%), e degli extracomunitari, da 2.011 a 2.727 (+35,6%).
Le patologie del sistema osteo-muscolare e del tessuto connettivo, quelle del sistema nervoso e dell'orecchio continuano a rappresentare, anche nei primi otto mesi del 2023, le prime tre malattie professionali denunciate, seguite dai tumori e dalle patologie del sistema respiratorio.

- N6) Sicurezza: Proroga dei termini di qualificazione per manutentori presidi antincendio

Tra le ragioni addotte le oggettive difficoltà organizzative rispetto al previgente quadro normativo e l'impegno richiesto ai Comandi dei VVF per fronteggiare il ripristino di ampie aree nazionali colpite dagli eventi meteorologici sfavorevoli del 2023.

Il Ministero dell'Interno con Decreto 31 agosto 2023 (GU dell'11 settembre 2023, n. 212) ha apportato modifiche al Decreto 1° settembre 2021, recante: "Criteri generali per il controllo e la manutenzione degli impianti, attrezzature ed altri sistemi di sicurezza antincendio, ai sensi dell'articolo 46, comma 3, lettera a), punto 3, del D.Lgs. 9 aprile 2008, n. 81", **disponendo lo slittamento al 25 settembre 2024 del termine per la qualificazione dei manutentori dei presidi antincendio**, inizialmente posto al 25 settembre 2023.

- N7) Responsabilità ESG: La Commissione UE adotta gli standard europei di sostenibilità ESRS

La Commissione Europea ha adottato in via definitiva gli Standards Europei sul Rapporto di Sostenibilità (European Sustainability Reporting Standards - ESRS) applicabili a tutte le imprese che devono redigere la relazione di sostenibilità ai sensi della direttiva n. 2013/34/EU del 26 giugno 2013 in materia di bilanci d'esercizio e bilanci consolidati.

La Commissione europea ha approvato gli standards dopo avere raccolto i commenti a seguito della diffusione in pubblica consultazione, fino al 7 luglio 2023, della versione in bozza.

I principi entreranno in vigore dal 1° gennaio 2024 con riferimento ai rendiconti dei bilanci che iniziano dal 1° gennaio 2024 in avanti.

L'emanazione degli standards da parte della Commissione Europea era richiesta dall'art. 29-ter della direttiva n. 2013/34/EU, la quale quindi doveva adottare (entro il 30 giugno 2023) i principi di rendicontazione di sostenibilità (c.d. European Sustainability Reporting Standard - ESRS) i quali specificano le informazioni che le imprese sono tenute a comunicare.

Seppur con un mese di ritardo la Commissione europea ha approvato gli standards che costituiscono - a detta del Commissario per i servizi finanziari, la stabilità finanziaria e i mercati dei capitali - il giusto equilibrio tra:

- da un lato, il minore impatto possibile di maggiori oneri in capo alle imprese obbligate al reporting e,
- dall'altro lato, la rappresentazione da parte delle medesime imprese degli sforzi sostenuti al fine di soddisfare gli obiettivi del Green Deal e, conseguentemente, avere accesso a finanziamenti di sostenibilità.

I principi di rendicontazione di sostenibilità hanno lo scopo di assicurare la qualità delle informazioni comunicate, richiedendo che esse siano comprensibili, pertinenti, verificabili, comparabili e rappresentate fedelmente.

I principi di rendicontazione di sostenibilità, inoltre, **tengono in considerazione anche del confronto con l'International Sustainability Standards Board (ISSB) e la Global Reporting Initiative (GRI) al fine di garantire un grado molto elevato di interoperabilità tra gli standard dell'UE e quelli mondiali ed evitare, quindi, inutili doppie segnalazioni da parte delle imprese.**

Gli standard proposti sono 12 e sono suddivisi in 3 categorie:

1) comuni e trasversali

2) specifici (indicati con le lettere E - Environmental, S - Social e G - Governance);

3) relativi a particolari settori (questi ultimi ancora da pubblicare).

Gli standard sono i seguenti:

- ESRS 1 Requisiti generali
- ESRS 2 Informativa generale

Informazioni ambientali

- ESRS E1 Cambiamento climatico
- ESRS E2 Inquinamento
- ESRS E3 Acqua e risorse marine
- ESRS E4 Biodiversità ed ecosistemi
- ESRS E5 Risorse ed economia circolare

Informazioni sociali

- ESRS S1 Forza lavoro utilizzata
- ESRS S2 Lavoratori nella catena del valore
- ESRS S3 Comunità interessate
- ESRS S4 Consumatori ed utenti finali

Informazioni di governance

- ESRS G1 Conduzione dell'attività

Valutazione di materialità

L'ESRS 1 ("Requisiti generali") stabilisce i principi generali da applicare nella rendicontazione secondo l'ESRS e non stabilisce di per sé specifici requisiti di informativa.

L'ESRS 2 ("Informazioni generali") specifica le informazioni essenziali da divulgare indipendentemente dall'aspetto della sostenibilità preso in considerazione. È obbligatorio per tutte le società.

Tutti gli altri standards sono soggetti a una valutazione di materialità: la società riporterà solo le informazioni rilevanti e potrà omettere le informazioni che non sono rilevanti per il proprio modello di business e/o attività.

Gli obblighi di informativa soggetti alla materialità non sono discrezionali e quindi le informazioni devono essere divulgate se sono rilevanti; il processo di valutazione della rilevanza (o meno) dell'informazione è soggetto a verifica da parte dei soggetti esterni in conformità con le disposizioni della direttiva n. 2013/34/EU.

A titolo esemplificativo: Se un'azienda conclude che il cambiamento climatico non è un tema materiale e pertanto non effettua la rendicontazione in conformità a tale standard, deve fornire una spiegazione dettagliata delle conclusioni della sua valutazione di materialità in relazione al cambiamento climatico e non può quindi limitarsi a non fornire la rendicontazione.

Gli aggiornamenti futuri

L'EFRAG - quale consulente tecnico della Commissione (giusta la sua definizione nella direttiva n. 2013/34/EU) - pubblicherà periodicamente ulteriori orientamenti tecnici non vincolanti sull'applicazione dell'ESRS.

Il calendario dei prossimi mesi

Gli standards saranno ora trasmessi al Parlamento europeo e al Consiglio per il loro esame. Il termine per la verifica da parte del Parlamento e del Consiglio degli standards è di due mesi, prorogabile di altri due mesi. Il Parlamento europeo e/o il Consiglio possono approvare o respingere gli Standards, senza quindi poterli modificare.

Le imprese dovranno adottare gli Standards secondo il seguente calendario:

- società precedentemente soggette alla direttiva sulla dichiarazione non finanziaria - NFRD (grandi società quotate, grandi banche e grandi imprese assicurative - tutte se con più di 500 dipendenti), nonché grandi società quotate extra UE con più di 500 dipendenti: **esercizio 2024, con prima dichiarazione di sostenibilità pubblicata nel 2025;**
- altre grandi imprese, comprese altre grandi imprese quotate extra UE: **esercizio 2025, con prima dichiarazione di sostenibilità pubblicata nel 2026;**
- PMI quotate, comprese le PMI quotate non UE: **esercizio 2026, con le prime dichiarazioni di sostenibilità pubblicate nel 2027**;
- le società extra UE che generano oltre 150 milioni di euro all'anno di ricavi nell'UE e che hanno nell'UE una succursale con un fatturato superiore a 40 milioni di euro o una controllata che è una grande impresa o una PMI quotata dovranno dichiarare sugli impatti di sostenibilità a livello di gruppo di tale società extra UE a partire **dall'esercizio 2028, con prima dichiarazione di sostenibilità pubblicata nel 2029**.

- N8): Conferma della qualifica di "Privacy Officer e Consulente della Privacy" secondo lo schema CDP di TUV Italia in conformità alla norma ISO/IEC 17024:2012 certificazione delle professioni

In data 24 luglio 2023 l'ing. Violi ha confermato la propria qualifica di "Privacy Officer e Consulente della Privacy" secondo lo schema CDP di TUV Italia in conformità alla norma ISO/IEC 17024:2012 certificazione delle professioni. **La qualifica iniziale è stata conseguita il 10 giugno 2014 e sarà valida fino al 9 giugno 2026**.

- SINTESI DELLE SCADENZE

1. **Qualifica del tecnico manutentore antincendio**: settembre 2024
2. **Bilancio di sostenibilità**:
    a. società già soggette alla direttiva sulla dichiarazione non finanziaria - NFRD: esercizio 2024, con prima dichiarazione di sostenibilità pubblicata nel 2025;
    b. altre grandi imprese: esercizio 2025, con prima dichiarazione di sostenibilità pubblicata nel 2026;
    c. PMI quotate: esercizio 2026, con le prime dichiarazioni di sostenibilità pubblicate nel 2027;
3. **Ispezioni garante privacy** (estratto): entro fine 2023
    a. prosecuzione delle verifiche in ordine alla corretta implementazione delle Linee guida sui cookie e gli altri strumenti di tracciamento anche attraverso lo strumento degli accertamenti on line;
    b. altri accertamenti nei confronti di soggetti pubblici e privati, al fine di verificare l'osservanza delle disposizioni in materia di
    c. protezione dei dati personali, ivi incluse le istruttorie relative a reclami e segnalazioni formali proposti all'Autorità

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