KAN Brief
3/23
Kommission Arbeitsschutz und Normung


# LA SICUREZZA DELLE INFORMAZIONI

# Indice

© Suphakant - stock.adobe.com

## In primo piano



## Temi



© GordonGrand - stock.adobe.com

© M.Dörr & M.Frommherz - stock.adobe.com



**Ultimi aggiornamenti:**

www_kan_de

Kommission Arbeitsschutz und Normung (KAN)

KAN_Arbeitsschutz_Normung

KAN – Kommission Arbeitsschutz und Normung

**Benjamin Pfalz**
Presidente della KAN
Sindacato Industriale dei Metallurgici (IG Metall)

# Cibersicurezza: una sfida a livello sia regolamentare che aziendale

Oggi più che mai le imprese devono difendersi dagli attacchi informatici. Ormai si tratta anche di una questione di prevenzione. Data l'interazione tra uomo e macchina risultante dall'uso di mezzi di lavoro telecomandati, dagli impianti di produzione interconnessi e dal crescente ricorso all'apprendimento automatico, sempre più spesso si rende necessario tenere conto della cibersicurezza anche nel quadro della valutazione aziendale dei rischi. Le misure tese a garantire la sicurezza dei prodotti svolgono in generale un ruolo particolare.

I relativi aspetti sono stati ripresi sempre più nell'ambito della regolamentazione. Nel caso dei dispositivi di misurazione, controllo e regolazione rilevanti ai fini della sicurezza, p. es., la TRBS 1115 concretizza il regolamento sulla sicurezza degli impianti e della salute per quel che riguarda l'identificazione e la definizione delle necessarie misure di cibersicurezza. Il tema è contemporaneamente trattato dal nuovo regolamento UE in materia di macchine e dal futuro regolamento sull'IA. Per disciplinare la messa in circolazione di prodotti e prodotti semilavorati con elementi digitali, è stata avviata la messa a punto della cosiddetta legge sulla ciberresilienza (Cyber Resilience Act).

La normazione deve ora supportare adeguatamente i regolamenti. L'incarico di normazione relativo alla bozza del regolamento sull'IA affronta chiaramente il tema della cibersicurezza. Gli organismi di normazione europei stanno già reagendo prendendo in esame il patrimonio normativo esistente e assegnando i vari temi alle loro strutture.

A tal proposito è fondamentale che il settore della prevenzione si faccia sentire! La KAN sta pertanto affrontando il tema a tutti i livelli, p. es. tramite un colloquio specialistico in programma per quest'anno e dedicato alla normazione rilevante per la prevenzione contestualmente al regolamento sull'IA. **«**

# Regolamento UE per una maggiore sicurezza del mondo degli apparecchi e macchinari interconnessi

In futuro i fabbricanti di prodotti con “elementi digitali” dovranno garantirne la cibersicurezza per tutto il ciclo di vita: questo è quanto intende ottenere la Commissione UE con la legge sulla ciberresilienza (Cyber Resilience Act).

A fronte del persistere degli attacchi online, p. es. con ransomware, la Commissione UE continua a premere affinché vengano colmate le lacune di sicurezza IT. Dopo leggi come quella sulla cibersicurezza (Cybersecurity Act) del 2019 – che getta le basi per uno schema di certificazione della sicurezza IT di apparecchi, sistemi e servizi interconnessi valevole in tutta l’UE – o il recente emendamento della direttiva sulla sicurezza delle reti e delle informazioni (NIS2), a settembre del 2022 ha approvato la bozza di una legge sulla ciberresilienza (Cyber Resilience Act o CRA)[1]. Secondo il previsto regolamento sulla ciberresilienza, in futuro i prodotti “con elementi digitali” come hardware e software dovranno essere “immessi sul mercato con un minor numero di vulnerabilità”.

L’ambito di validità della bozza è ampio. La Commissione vuole p. es. coprire “qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto”, componenti compresi, anche se messi in circolazione separatamente. Particolare attenzione verrà probabilmente rivolta all’Internet delle cose o ai piccoli router (“plaste-router”) che, date le loro numerose falle di sicurezza, ad oggi sono spesso vulnerabili. Il regolamento non si applicherà invece a prodotti “sviluppati esclusivamente per scopi di sicurezza nazionale o militari” o specificamente progettati per trattare informazioni classificate. Lo stesso dicasi per settori come quelli dell’aviazione, dei dispositivi medici o delle auto, per i quali già valgono requisiti specifici.

Per quanto riguarda design, sviluppo e processo produttivo, in base alla proposta in futuro prima d’immettere un apparecchio sul mercato i fabbricanti interessati dovranno obbligatoriamente soddisfare dei requisiti essenziali di cibersicurezza. Saranno inoltre tenuti a monitorare eventuali vulnerabilità per tutta la durata del ciclo di vita dell’apparecchio e a porvi rimedio attraverso update automatici e gratuiti. A ciò si aggiungerà l’obbligo di segnalare entro appena 24 ore all’Agenzia dell’Unione europea per la cibersicurezza (ENISA) qualsiasi incidente con ripercussioni sulla sicurezza di hardware o software. In generale dovrà essere introdotta una linea coordinata per la divulgazione delle vulnerabilità.

La CRA prevede che vengano limitate le superfici di attacco degli apparecchi considerati e ridotte al minimo le ripercussioni degli incidenti. I prodotti a cui si applica dovranno garantire la riservatezza dei dati, p. es. mediante crittazione. Dovrà inoltre divenire obbligatorio proteggere l’integrità e l’elaborazione d’informazioni e valori misurati indispensabili ai fini del funzionamento di un articolo.

Al di là di queste disposizioni di base, la Commissione ha individuato una serie di settori critici ad alto rischio. I prodotti del caso sono stati suddivisi in due classi, per ciascuna delle quali è prevista l’introduzione di una specifica procedura di conformità. La categoria I comprende sistemi di gestione dell’identità, browser, sistemi di gestione delle password, programmi antivirus, firewall, reti private virtuali (VPN), sistemi di gestione della rete, sistemi IT di ampia portata, interfacce di rete fisiche, router e chip. A questi si aggiungono sistemi operativi, p. es. per smartphone o desktop, microprocessori e l’Internet of Things (IoT) nelle aziende, che non sono ritenuti particolarmente sensibili.

Nella classe di rischio più alta (classe II) rientrano invece dispositivi desktop e mobili, sistemi operativi virtualizzati e p. es. integrati in macchinari, emittenti di certificati digitali, microprocessori di uso generale, lettori di carte, sensori per robot e contatori intelligenti. A questi dovranno poi aggiungersi apparecchi IoT, router e firewall per l’industria, che è in generale considerata un “ambiente sensibile”. Le falle di sicurezza IT, infatti, si ripercuotono ormai pesantemente anche su macchinari e impianti – che oggi sono sempre più interconnessi e non più accessibili soltanto a partire dalle superfici aziendali – e dunque anche sulla prevenzione.

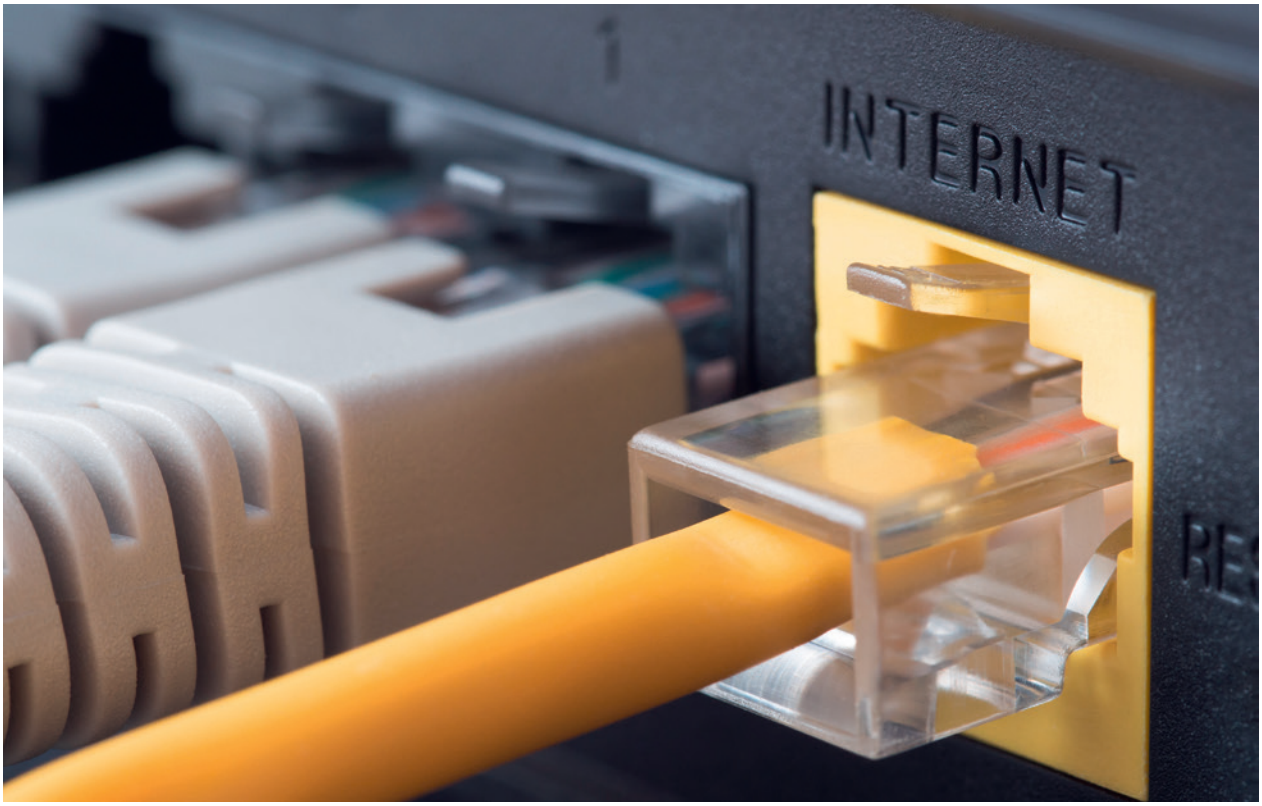
I fabbricanti sono chiamati a valutare la conformità dei loro prodotti mediante un'apposita procedura interna o tramite un esame da parte di enti riconosciuti. Laddove un produttore punti sulle norme armonizzate o abbia già ottenuto un certificato nel quadro di un sistema europeo di certificazione della cibersicurezza, si potrà dare per scontato che il suo hardware o software sia conforme al regolamento. Importatori e distributori saranno tenuti a verificare l'osservanza delle previste procedure da parte del produttore nonché la marcatura CE dell'apparecchio. Per i prodotti di scarsa criticità i fabbricanti saranno autorizzati a compilare da sé una dichiarazione di conformità. Per quanto riguarda la classe di rischio II, sarà invece necessaria una valutazione da parte di terzi.

La Commissione ritiene necessario intervenire, visto che fino al 2021 i crescenti episodi di cibercriminalità hanno causato costi il cui volume è stimato a 5500 miliardi di euro l'anno. In un ambiente interconnesso un incidente di cibersicurezza ai danni di un prodotto potrebbe avere ripercussioni negative su un'intera impresa o catena di fornitura e in molti casi – p. es. in quello del malware WannaCry – le conseguenze potrebbero farsi sentire nell'arco di pochi minuti anche al di là dei confini del mercato interno. Ciò comporterebbe un blocco delle attività economiche e sociali e potrebbe addirittura rappresentare un rischio per la vita.

### Critiche alla bozza del regolamento

In un suo commento[2] l'ente tedesco di assicurazione obbligatoria contro gli infortuni (DGUV) ha criticato il fatto che già il concetto chiave di cibersicurezza non sia definito in modo chiaro e ha fatto notare come, a seconda delle norme o dei regolamenti considerati, questo termine stia di volta in volta a indicare uno stato, un'attività o un prodotto. Più in generale, risulterebbero problematici i termini dal significato non chiaramente definito contenenti il prefisso "ciber". A seconda delle fonti considerate, p. es., il concetto di cibersicurezza non abbraccerebbe gli attacchi via radio o tramite interfacce USB.

La DGUV vede in modo critico anche l'obbligo dei fabbricanti di segnalare entro 24 ore grandi quantità di dettagli circa una falla di sicurezza. In molti casi, infatti, effettuare degli accertamenti in tempi così brevi non sarebbe realistico. Nello stesso tempo – così la DGUV – non sarebbe propriamente necessario divulgare dettagli utilizzabili ai fini di un attacco. Nel suo commento la DGUV sostiene l'importan-




© a_korn - stock.adobe.com

za di trasmettere soltanto quei dati di cui le autorità hanno davvero bisogno, p. es. per diramare un avvertimento circa un prodotto o stimare gli effetti di una vulnerabilità. Secondo l'ente tedesco di assicurazione obbligatoria contro gli infortuni, anche i due anni concessi per adeguarsi ai nuovi requisiti sarebbero troppo pochi per quei fabbricanti che dipendono da altri prodotti e devono p. es. attendere una valutazione della conformità.

Jonas Stein, responsabile del gruppo di lavoro "Security" della DGUV, fa anche notare che non è possibile svolgere adeguati accertamenti sui sistemi operativi, visto che si evolvono di continuo, e ricorda che in molti casi – basti ricordare Linux – sono di tipo open source. Nel caso dei software liberi, tuttavia, non vi sarebbe un unico produttore responsabile della procedura di conformità. Lo stesso settore open source, così Stein, teme di cadere nella trappola della responsabilità: i software liberi sono infatti opera di tanti singoli sviluppatori, i quali potrebbero essere chiamati a rispondere di potenziali falle. "Data la carenza dei mezzi finanziari e delle risorse che servono per svolgere le procedure proposte in merito alla conformità CE, alcuni progetti potrebbero dover essere completamente sospesi", lamenta la Free Software Foundation Europe (FSFE).

A metà luglio il Consiglio dei ministri UE e la commissione competente per l'industria del Parlamento UE hanno preso posizione rispetto alla proposta della Commissione, cosicché a breve potranno prendere il via i negoziati circa un compromesso finale. Gli Stati membri sostengono l'importanza p. es. di una dichiarazione di conformità semplificata, di un maggiore sostegno per le piccole imprese e di un chiarimento della durata di vita dei prodotti attesa dai fabbricanti. Fanno inoltre notare che dovrebbe essere previsto l'obbligo di segnalare le vulnerabilità sfruttate e gli incidenti di sicurezza alle autorità nazionali competenti, e non all'ENISA. I deputati rivendicano a loro volta definizioni più circostanziate, tabelle di marcia osservabili e una più equa ripartizione delle responsabilità e premono nello stesso tempo affinché anche dispositivi per case intelligenti, smart watch e telecamere di sicurezza private trovino posto nella categoria ad alto rischio.

*Dr. Stefan Krempl*
*Freier Journalist*
*sk@nexttext.de*

[1] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:52022PC0454
[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Legge-sulla-ciberresilienza-nuove-norme-in-materia-di-cibersicurezza-per-i-prodotti-digitali-e-i-servizi-ausiliari/F3376532_it

# Conoscenze collaudate nelle nuove specifiche in materia d'industrial security

I componenti di sicurezza funzionale proteggono la vita e la salute delle persone, p. es. impedendo l'accesso a zone pericolose di macchine e impianti. A tal proposito è importante che la sicurezza non possa essere compromessa nemmeno da manipolazioni dall'esterno. Per questo occorre che lo stato dell'arte trovi coerente applicazione e che fabbricanti e utilizzatori reagiscano adeguatamente a eventuali falle di sicurezza.

Affinché le funzioni di sicurezza dei sistemi di comando possano intervenire in maniera affidabile occorre che gli stessi sistemi di comando siano sicuri, ossia protetti da avarie e manipolazioni. La crescente frequenza con cui vengono segnalate nuove catastrofi nel settore dell'industrial security fa paura. Ciò non di meno, vi sono motivi di speranza: grazie alle possibilità offerte dallo sviluppo tecnologico, infatti, quasi tutte le falle di sicurezza sono facilmente evitabili – come dimostra il seguente esempio tipico.

Già nel 1883 Auguste Kerckhoffs aveva enunciato sei presupposti fondamentali di una comunicazione riservata. In base al secondo di questi, il sistema di comunicazione "non deve essere segreto, deve poter cadere nelle mani del nemico senza inconvenienti". Evidentemente Guglielmo Marconi non era al corrente di questo scritto. La telegrafia – tecnologia da lui ideata per una comunicazione riservata – presupponeva infatti che nessun altro potesse entrare in possesso di uno degli apparecchi in uso o costruirne uno uguale per poi sintonizzarlo sulla stessa frequenza. Nel 1903 Nevil Maskelyne richiamò l'attenzione su questo problema disturbando una dimostrazione di Marconi con la trasmissione di una serie d'insulti in alfabeto Morse. Oggi Maskelyne è per questo considerato il primo hacker della storia. Benché quella della cifratura sicura con metodi crittografici sia una tecnica nota da molto tempo, oggi lo stesso errore di design si ritrova p. es. nei comandi radio per sistemi di semafori[1] e nelle gru industriali[2].

## Mancano definizioni unitarie

Ad oggi il tool per la ricerca di norme relative alla security messo a punto dall'università di Brema[3] ha registrato in una banca dati circa 800 norme e oltre 2000 occorrenze riguardanti disposizioni giuridiche. Il fatto che i documenti facciano uso di termini differenti e, almeno in parte, non definiti in maniera univoca rappresenta però un problema. Mentre in alcuni documenti si parla diffusamente di security o sicurezza delle informazioni, in altri si coniano composti contenenti il termine ciber. Non avendo di per sé un significato univoco, questi neologismi devono essere definiti in maniera esatta all'interno del testo. In alcuni casi per cibersicurezza s'intende un'attività, in altri una misura volta a contrastare attacchi via Internet e in altri ancora uno stato in cui un prodotto risulta protetto dagli attacchi via radio.

Anziché coniare neologismi, sarebbe meglio lavorare con due termini ben definiti come sicurezza delle informazioni o security. Laddove poi, p. es., il significato debba essere limitato agli attacchi via radio, questa limitazione andrebbe indicata con chiarezza. Una soluzione diversa e assai elegante è quella adottata dal regolamento UE in materia di macchine, che al punto 1.1.9 dell'allegato III richiede una "protezione dall'alterazione" risultando così anche più chiaro della direttiva Macchine UE finora in vigore. Con ciò il documento si concentra sull'obiettivo di protezione consistente nel far sì che, p. es. in caso di accesso remoto, non possano crearsi situazioni pericolose e si astiene dallo specificare da cosa venga esattamente provocata l'alterazione.

## Comunicazione rapida come fattore decisivo

Una comunicazione rapida ed efficace è la chiave di un'adeguata reazione a falle di sicurezza. Eppure la situazione sul fronte comunicazione non è affatto buona, come dimostra la falla di sicurezza della libreria software Log4J che ha fatto notizia nel dicembre del 2021. Questa libreria software è parte integrante non solo di molti servizi server, ma anche di numerosi componenti industriali. Mentre all'epoca qualcuno puntava il dito contro un uso errato della libreria facendo presente che i problemi di sicurezza avrebbero potuto essere evitati se solo si fosse letta la documentazione, molti produttori si chiedevano se fossero interessati da falle di sicurezza. E in non pochi casi hanno dovuto attendere parecchi mesi per riuscire a sapere se questo problema riguardasse i loro prodotti.

In sintesi, mancavano
- un contatto di emergenza per la security all'interno dell'azienda,
- un formato unitario per raccomandazioni operative e
- uno standard secondo il quale i fabbricanti potessero segnalare anche che un determinato prodotto non era interessato da una lacuna di sicurezza.

Alla mancanza d'informazioni e interfacce unitarie viene posto rimedio con una serie di specifiche aperte che sono state messe a punto da varie associazioni d'imprese, autorità e organizzazioni e possono essere immediatamente attuate da ciascuna azienda (vedi tabella). Un contatto d'emergenza come da specifica IETF RFC 9116 viene archiviato in un semplice file security.txt all'interno del sito web [4]. Qui un fabbricante può anche rimandare alla sua lista di raccomandazioni operative (CSAF). A ciascun prodotto hardware o software viene assegnato un identificatore univoco a livello mondiale (CPE), in modo che gli avvisi internazionali (CVE) possano essere associati automaticamente ai prodotti giusti e alle relative versioni. La criticità della lacuna di sicurezza viene classificata il meglio possibile attraverso un indice univoco a livello mondiale (CVSS). Sulla base della specifica aperta SPDX per ogni progetto è possibile documentare in formato leggibile a macchina quali librerie sono state utilizzate. Attraverso un apposito programma, per ciascun prodotto gli utilizzatori hanno la possibilità di verificare regolarmente se vi sono avvisi di sicurezza e di visualizzare le raccomandazioni operative del caso.

Alcune grandi imprese puntano già adesso su queste specifiche. È ora fondamentale che a breve il loro esempio venga seguito da tutte le altre aziende, in modo che le informazioni su problemi di sicurezza vengano diramate rapidamente e con risparmio sui costi.

Per cominciare, le aziende dovrebbero ora almeno garantire la reperibilità in caso d'incidenti di sicurezza e rendere noto un contatto di emergenza. Con le istruzioni riportate su https://cert.dguv.de ciò è fattibile in una manciata di minuti.

### Specifiche aperte sulla sicurezza delle informazioni

| Informazione in entrata | A cura di | Specifica |
|---|---|---|
| Contatto di emergenza proprio | Produttore, utilizzatore | "security.txt" RFC 9116 |
| Identificatore del prodotto / ID (nome produttore, nome prodotto, versione, lingua...) | Produttore | CPE |
| Distinta base del software (Software Bill of Materials - SBOM) | Produttore | SPDX |
| Avviso di lacuna di sicurezza | Autorità di numerazione CVE | CVE |
| Security Advisory (raccomandazione operativa sulle CVE) | Produttore | CSAF |
| Caratteristiche per la valutazione della criticità | Produttore | CVSS |

Serie delle specifiche aperte che, insieme, contribuiranno in modo decisivo all'industrial security. Nei prossimi anni produrranno quell'accelerazione della comunicazione in caso di falle di sicurezza della quale allo stato attuale vi è urgente bisogno.

*Jonas Stein*

*Responsabile del laboratorio di prova per l'industrial security e del gruppo di lavoro "Security" della DGUV*

*Jonas.Stein@dguv.de*

[1] Servizio televisivo (canale ARD) "Quando i semafori diventano verdi grazie all'hacking" 2021 (in tedesco), https://ardmediathek.de Hacker Ampeln
[2] Andersen et al, 2019 « A Security Analysis of Radio Remote Controllers for IndustrialApplications » https://documents.trendmicro.com/assets/white_papers/wp-a-securityanalysis-of-radio-remote-controllers.pdf
[3] https://cybersecurity-navigator.de
[4] Falle di sicurezza critiche in macchine e installazioni e sicurezza.txt https://cert.dguv.de

# Il nuovo regolamento in materia di macchine – conseguenze per la normazione armonizzata

In nessun altro settore industriale le norme rivestono un'importanza simile a quella attribuita loro nel campo dell'ingegneria meccanica. Il nuovo regolamento UE in materia di macchine pone i comitati di normazione dinnanzi all'arduo compito di verificare la conformità delle norme alle nuove basi giuridiche e, se necessario, adottare dei provvedimenti per un loro adeguamento.

Nel corso degli anni le elevate esigenze di sicurezza degli utilizzatori di macchinari – insieme alla grande varietà di questi ultimi – hanno fatto sì che venissero elaborate oltre 800 norme armonizzate facenti capo alla direttiva Macchine europea. Chi applica tali norme può dare per scontato che le soluzioni e le misure in esse descritte sono adatte a soddisfare i requisiti legali stabiliti dai regolamenti o dalle direttive di riferimento. Tra queste oltre 800 norme figurano circa 100 cosiddette norme di tipo B, le quali trattano determinati aspetti di sicurezza o dispositivi di protezione che si ritrovano in numerose macchine. Oltre 700 norme descrivono invece requisiti e soluzioni tecniche per tipi di macchine ben precisi (norme di tipo C). Negli anni dall'interazione tra direttiva Macchine e norme armonizzate è scaturito un sistema ben rodato che garantisce un alto livello di sicurezza delle macchine riconosciuto in tutto il mondo.

## Compito titanico per la normazione

Con il nuovo regolamento (UE) 2023/1230 in materia di macchine pubblicato sulla Gazzetta Ufficiale dell'UE in data 29 giugno 2023, la Commissione UE ha inaugurato un nuovo capitolo giuridico. A decorrere dalla data di riferimento del 20 gennaio 2027 – dunque senza periodo di transizione – detto regolamento sostituirà la direttiva Macchine 2006/42/CE attualmente in vigore. Oltre a numerosi adeguamenti formali e concettuali del testo giuridico sono intervenute importanti modifiche dell'allegato I della direttiva Macchine, nel quale sono descritti requisiti di sicurezza fondamentali (EHSR – Essential Health and Safety Requirements). Nel regolamento in materia di macchine gli EHSR sono riportanti nel nuovo allegato III. La funzione principale delle norme armonizzate consiste nel soddisfare questi requisiti di sicurezza. Sulla scia dei cambiamenti intervenuti vanno innegabilmente ponendosi i seguenti quesiti:

Quali sono le ripercussioni immediate degli EHSR nuovi e modificati sui contenuti delle odierne norme armonizzate? Con l'entrata in vigore del regolamento in materia di macchine le norme armonizzate facenti capo alla direttiva Macchine possono continuare a essere applicate? E continuano a dare luogo alla presunzione di conformità?

Rispondere alla prima domanda è tutt'altro che semplice. È infatti ancora in corso un intenso dibattito circa l'attuazione pratica e normativa dei nuovi EHSR "protezione dall'alterazione", "funzione di supervisione di macchine mobili autonome" e "prevenzione del rischio di contatto con linee elettriche aeree sotto tensione".

Da una panoramica approssimativa degli ambiti di validità delle norme emerge però che gli EHSR – nuovi o profondamente modificati che siano – andranno probabilmente a tangere in qualche modo quasi tutti i tipi di macchine. Tutte le norme armonizzate andrebbero dunque sottoposte a un esame volto ad appurare la rilevanza dei nuovi EHSR e, se interessate, dovrebbero essere adattate, sia dal punto di vista dei contenuti che da quello formale, secondo le regole procedurali stabilite dalla Commissione UE (allegato ZA sotto forma di tabella, rimandi datati). A questo scopo sarebbe teoricamente necessaria una revisione di quasi tutte le circa 800 norme armonizzate – e dei relativi approfonditi assessment effettuati dagli HAS consultant. Affrontare questo compito nei tre anni e mezzo che rimangono prima che il regolamento in materia di macchine venga applicato in maniera vincolante non è però assolutamente realistico.

### Pubblicazione limitata come possibile soluzione temporanea

Per tutte le norme europee (sia EN che EN ISO) che risulteranno armonizzate secondo la direttiva Macchine a una data ancora da definirsi della prima metà del 2026, la Commissione UE ha perciò in programma (dato aggiornato all'agosto 2023) un'iniziativa straordinaria per il trasferimento in blocco come norme armonizzate sotto il nuovo regolamento in materia di macchine. Unica limitazione: queste norme possono naturalmente garantire un'armonizzazione solo per gli EHSR da esse già trattati sotto la direttiva Macchine. Per evidenziare questa circostanza nel quadro della pubblicazione sulla Gazzetta UE in modo che gli utilizzatori delle norme possano prenderne atto, i comitati tecnici (TC) competenti dovranno per forza esaminare (ma NON necessariamente revisionare) tutto il rispettivo portafoglio di norme, così da identificare le lacune esistenti rispetto al nuovo regolamento in materia di macchine. Nello stesso tempo CEN e CENELEC inizieranno a lavorare alla messa a punto di soluzioni normative relativamente agli EHSR nuovi o sottoposti a modifiche significative, in maniera tale da colmare a livello normativo le lacune identificate.
Attualmente, con l'aiuto del forum settoriale coordinante "Machinery" del CEN/CENELEC, si sta mettendo a punto una guida intesa ad agevolare i TC chiamati ad affrontare questa ambiziosissima impresa. Il documento dovrebbe essere disponibile al più tardi verso la fine del 2023.

Va da sé che nel caso di revisioni di norme o di nuovi progetti in programma è già ora possibile nonché consigliabile puntare alla conformità al nuovo regolamento in materia di macchine. Si spera così che entro l'inizio del 2027 una certa percentuale di norme sia stata adattata ad esso. Per buona parte delle norme armonizzate, tuttavia, ciò sarà possibile soltanto quando già vi sarà l'obbligo di applicare il nuovo regolamento in materia di macchine.

Una più precisa finestra temporale per le future revisioni delle norme dovrebbe essere definita in concomitanza con il nuovo incarico di normazione della Commissione UE per il regolamento in materia di macchine. Tale incarico – che sarà disponibile il prossimo anno e, a differenza dei mandati precedenti, avrà una durata limitata (probabilmente tra i 5 e i 10 anni) – costituisce la base giuridica dell'elaborazione di norme armonizzate facenti capo al nuovo regolamento in materia di macchine. Una prima bozza dell'incarico di normazione è stata pubblicata a fine giugno. I commenti dei gruppi interessati verranno discussi in seno agli organi della Commissione probabilmente in autunno.

Per finire, per gli utilizzatori delle norme il passaggio delle norme armonizzate dalla direttiva Macchine al regolamento in materia di macchine dovrà essere reso più agevole. Le norme pubblicate tra il 2024 e la prima metà del 2026 avranno due allegati ZA – uno per la direttiva Macchine e uno per il regolamento in materia di macchine – in cui sarà specificato quali disposizioni giuridiche sono coperte e da quali sezioni della rispettiva norma. Anche in questo caso i TC di normazione interessati verranno informati entro tempi ristretti.

Tutte le misure descritte contribuiranno a far sì che il passaggio delle norme armonizzate dalla vecchia direttiva Macchine al nuovo regolamento in materia di macchine si svolga nel modo più agevole possibile.

*Dr. Frank Wohnsland*

*VDMA (Associazione tedesca dei costruttori di macchine e impianti)*

*Presidente del forum di settore "Machinery" del CEN/CENELEC*

*frank.wohnsland@vdma.org*

# Ergonomia digitale: un progetto KAN getta luce sullo stato della ricerca

**Dietro incarico della KAN la BioMath GmbH ha svolto un'indagine volta a chiarire a che punto è la ricerca in fatto d'interfacce e formati di dati nel campo dei modelli umani digitali e dei sistemi per la registrazione di movimenti.**

Nel settore della prevenzione si fa uso di modelli digitali e metodi di progettazione e valutazione di prodotti e processi. I modelli umani digitali simulano aspetti fisici del lavoro. Esistono inoltre sistemi che registrano i movimenti sulla scorta delle coordinate delle articolazioni umane in uno spazio tridimensionale. Successivamente i dati così raccolti possono essere fatti confluire in un modello umano digitale a partire dal quale gli esperti definiranno delle misure per una progettazione sicura e sana dei luoghi di lavoro.

© berCheck - stock.adobe.com

Enti di ricerca e imprese dispongono di metodi e strumenti per l'analisi, la valutazione e la rappresentazione dei dati forniti da modelli umani digitali e sistemi di registrazione dei movimenti. Non di rado, tuttavia, si tratta di soluzioni isolate e che, date le differenze di formato, non sono compatibili tra loro. Dagli anni '60 in poi sono stati messi a punto circa 150 modelli umani digitali per svariate finalità (non tutti vengono però ancora usati).

La standardizzazione delle interfacce
- tra modelli umani digitali,
- tra sistemi per la registrazione dei movimenti e
- tra modelli umani digitali e sistemi per la registrazione dei movimenti

sarebbe utile ai fini della prevenzione, poiché permetterebbe di ottenere una base di dati più attendibile, a partire dalla quale definire misure per una progettazione del lavoro a misura d'uomo. Con interfacce e formati di dati unitari diverrebbe possibile unire dati di movimento provenienti da fonti diverse e utilizzarli per valutazioni esaustive.

## Il progetto KAN rivela la varietà dei modelli

Nel quadro di un progetto KAN la BioMath GmbH ha raccolto e valutato delle pubblicazioni sull'ergonomia digitale. L'obiettivo era, non da ultimo, quello di evidenziare quali conoscenze vadano considerate affidabili tra quelle maturate nell'ambito delle scienze del lavoro relativamente a modelli umani digitali e rilevamento digitale, valutazione e rappresentazione di dati sui movimenti.

Il resoconto[1] fornisce una panoramica dei modelli umani digitali e delle loro proprietà e possibilità. Dallo studio emerge come questi attingano a misure antropometriche di banche dati differenti e che riflettono caratteristiche di gruppi di popolazione differenti. I dati, inoltre, sono raggruppati e/o ripartiti in modi talvolta molto diversi tra loro. La loro qualità incide anche sulla qualità dei modelli umani digitali.

È stato anche analizzato quali sistemi per la registrazione dei movimenti siano già stati esaminati nel quadro di studi. Particolare attenzione è stata a tal proposito dedicata alle possibilità di scambio di dati. Come rivelato dalla ricerca, su questo fronte non vi sono per ora procedure unitarie.

Nei futuri progetti di ricerca occorrerà pertanto concentrarsi meglio non da ultimo sui seguenti punti:
- Ai fini dello scambio di dati tra modelli umani digitali sarebbe opportuno disporre di un formato standardizzato, non proprietario e ben documentato.
- Servirebbero inoltre delle definizioni concettuali e andrebbero stabiliti dei possibili livelli di dettaglio, p. es. per determinate parti di un modello umano digitale.
- Poiché per quanto riguarda caratteristiche e configurazione dei modelli umani esistono diversi approcci, sarebbe importante stabilire delle disposizioni sulla struttura dei modelli che favoriscano la comparabilità.

## E ora?

L'azienda che ha curato il progetto ha riepilogato gli esiti della ricerca in un resoconto che descrive l'attuale situazione e gli approcci per l'armonizzazione di interfacce e formati di dati unitari. I contenuti del resoconto verranno resi disponibili sotto forma di rapporto tecnico (DIN/TR). A tal proposito la KAN provvederà a elaborare il testo e a presentare un'istanza presso il DIN. Nel lungo termine l'obiettivo è quello di creare delle norme di base per modelli umani digitali, interfacce e formati di dati. Secondo la KAN, tuttavia, per ora l'armonizzazione completa dei requisiti non è possibile.

*Katharina von Rymon Lipinski*
*vonrymonlipinski@kan.de*

[1] www.kan.de/fileadmin/Redaktion/Dokumente/KAN-Studie/de/2023_KAN-Projekt_Digitale_Ergonomie_bf_final.pdf

# ASGA – un nuovo comitato per affrontare aspetti trasversali della prevenzione

Nel 2021 ai comitati per la prevenzione preesistenti in seno al Ministero federale per il lavoro (BMAS) si è aggiunto il comitato statale per la sicurezza e salute sul lavoro ("Ausschuss für Sicherheit und Gesundheit bei der Arbeit" o "ASGA"). Che compiti ha? E perché è stato istituito?

In Germania i comitati statali[FN1] hanno il compito di elaborare delle regole (tecniche) volte a concretizzare gli obiettivi di protezione generali dei singoli regolamenti facenti capo alla legge sulla prevenzione. Coordinati dall'ente federale per la prevenzione e la medicina del lavoro (BAuA), si occupano di potenziali fattori di rischio del sistema di lavoro, p. es. sostanze pericolose, sostanze biologiche nonché luoghi e mezzi di lavoro. Le regole forniscono ai datori di lavoro dei requisiti di processo e progettazione la cui osservanza permette di soddisfare le disposizioni dei singoli regolamenti in materia di prevenzione (presunzione di conformità).

Sulla scia della diversificazione delle forme di lavoro, della digitalizzazione e degli influssi climatici sull'ambiente lavorativo, l'impostazione finora rigorosamente verticale del processo di regolamentazione non basta più laddove si debbano valutare in maniera approfondita le ripercussioni presenti e future sugli occupati e definire delle misure adeguate. Anche per quanto riguarda temi classici come quelli della valutazione del rischio e dell'addestramento, i requisiti da soddisfare non dipendono da singoli fattori di rischio, ragion per cui vanno considerati da diverse prospettive (orizzontalmente).

Questa esigenza è emersa in modo eclatante con la pandemia di Coronavirus e le nuove sfide che questa ha sollevato in termini di prevenzione aziendale e salute sul posto di lavoro. Quella sul SARS-CoV è stata la prima regola definita di proposito secondo un approccio interfattoriale e il successo della sua attuazione nelle aziende ha evidenziato l'opportunità di verificare per quali altri campi tematici sia utile elaborare delle regole orizzontali in materia di prevenzione aziendale e salute sul posto di lavoro.

Per questa ragione, con l'integrazione del § 24 a pubblicata nel dicembre del 2020, l'ASGA[FN2] ha trovato un suo posto direttamente nella legge sulla prevenzione. Tra i compiti del nuovo comitato vi è quello di elaborare – a patto che ciò non ricada nelle competenze di un altro comitato statale – regole e constatazioni circa le modalità di adempimento dei requisiti fissati dalla legge sulla prevenzione.

Un'altra ragione dell'istituzione del nuovo comitato consiste nella scarsa coerenza dell'attuale corpus di regole, che a sua volta è legata all'impostazione rigorosamente verticale dei comitati preesistenti. Già nel 2011 il documento guida sul riassetto del corpus di disposizioni e regole in materia di prevenzione aveva evidenziato la necessità di un miglior coordinamento, a livello di contenuti, tra lo statuto autonomo degli enti assicurativi contro gli infortuni e il corpus di regole statali nonché tra i rispettivi ambiti di regolamentazione. Per quanto riguarda i campi d'azione centrali – p. es. quello della valutazione del rischio – ad oggi in tal senso è stato fatto molto poco. I membri dell'ASGA concordano circa la necessità di rivolgere l'attenzione a questo aspetto.

## Composizione e modus operandi

La composizione dell'ASGA non differisce da quella di altri comitati per la prevenzione. L'ASGA è infatti costituito da esperti convocati dal BMAS in rappresentanza di datori di lavoro pubblici e privati, sindacati, autorità dei Länder tedeschi, assicurazione tedesca obbligatoria contro gli infortuni e scienza. Del comitato fanno parte 15 membri e 15 membri supplenti.

Oltre alla direzione, la presidente dell'ASGA coordina la cooperazione tra tutti i comitati per la prevenzione compresi in un gruppo direttivo. Questo organo riveste una funzione centrale per quel che riguarda l'elaborazione di regole orizzontali multidisciplinari. Tramite i loro incaricati, i comitati fanno confluire il loro know-how direttamente nei rispettivi gruppi di progetto. Sono pertanto immediatamente coinvolti in tutto il processo che dall'elaborazione di una bozza di progetto conduce all'approvazione di una nuova regola – e ciò rappresenta una novità.

L'ASGA si riunisce due volte l'anno. Il gruppo direttivo riepiloga le sue argomentazioni e i suoi voti in apposite raccomandazioni che vengono sottoposte all'attenzione del gruppo di coordinamento. Quest'ultimo esamina i temi e i compiti del momento e prepara le proposte di delibera per le sedute dell'ASGA.

### Progetti e priorità

Come tutti i comitati, l'ASGA ha definito un programma di lavoro per l'attuale periodo di convocazione. Tra i temi cardine figurano valutazione del rischio, carichi mentali, addestramento efficace e al passo con i tempi, lavoro flessibile in termine di mobilità con videoterminale al di fuori del luogo di lavoro e ripercussioni del cambiamento climatico sulla sicurezza e la salute sul lavoro. L'obiettivo consiste nel mettere a punto delle regole statali che s'inseriscano in modo coerente nell'attuale corpus di regole.

Al momento le sfide non mancano: difficilmente, infatti, un processo di cambiamento si svolge senza intoppi. L'intento è quello d'impostare l'operato del comitato in maniera positiva e rispettosa, così da poter affrontare l'ambizioso programma di lavoro sulla base di un consenso. Per favorire questo sviluppo, la presidenza dell'ASGA deve inoltre promuovere l'elaborazione di guide applicative e processi adeguati e trasparenti.

Il gruppo di progetto per la valutazione del rischio sta già lavorando all'ideazione e all'impostazione dei contenuti di una regola ASGA, mentre il gruppo di progetto per i carichi mentali darà il via ai lavori probabilmente nel corso di quest'anno.

*Prof. Dr. Anke Kahl*

*Cattedra per la sicurezza sul lavoro della Bergische Universität Wuppertal.*

*Presidente dell'ASGA*

[1] www.bmas.de/DE/Arbeit/Arbeitsschutz/Arbeitsschutzausschuesse/arbeitsschutzausschuesse.html
[2] www.baua.de/EN/Tasks/Committee-administration/ASGA/ASGA_node.html

# Riforma della legislazione UE sulla responsabilità per danno da prodotti difettosi

**Nell'autunno del 2022 la Commissione UE ha dato il via all'ammodernamento dei regimi UE sulla responsabilità per danno da prodotti difettosi. Dopo la pubblicazione delle bozze di un emendamento della direttiva sulla responsabilità per danno da prodotti difettosi e di una nuova direttiva sulla responsabilità da IA, il Consiglio dei ministri UE e il Parlamento si stanno ora concentrando maggiormente sulla questione.**

L'ingresso nell'era digitale rende necessario un adeguamento non solo delle disposizioni giuridiche sulla messa in circolazione, ma anche del diritto sulla responsabilità. La vecchia direttiva sulla responsabilità per danno da prodotti difettosi – che è pur sempre datata 1985 e in Germania è stata attuata nel 1989 con l'approvazione della legge sulla responsabilità da prodotto – non è ormai più idonea a coprire tutti i danni provocati da prodotti. Ciò si traduce in incertezza per le imprese e in un crescente numero di prodotti relativamente ai quali, in caso di danni da essi provocati, non è previsto alcun diritto di compensazione per il consumatore.[FN1] La direttiva necessita inoltre di un allineamento con il regolamento sulla sicurezza dei prodotti di recente aggiornato e con quello sulla vigilanza del mercato.

## Più prodotti ed eventi dannosi in primo piano

Si prevede che la nuova direttiva sulla responsabilità per danno da prodotti difettosi sarà applicabile a tutti i tipi di prodotti – anche a quelli che finora non venivano considerati. Tra questi vi sono p. es. anche prodotti smart, update di software, sistemi di IA e servizi digitali, ma anche prodotti rifabbricati o modificati in maniera sostanziale. Nell'ambito dell'economia circolare i produttori non saranno però chiamati a rispondere di danni provocati da parti di prodotto non modificate.

Nel caso dei prodotti provenienti da Stati terzi che vengono importati nell'UE direttamente dai consumatori – p. es. mediante acquisto online – i diritti di responsabilità verranno ampliati: oltre che nei confronti degli importatori attualmente chiamati a rispondere di eventuali danni da prodotto, in futuro potranno essere fatti valere nei confronti dei rappresentanti dei produttori e di altri attori, p. es. piattaforme online, con sede all'interno dell'UE. Sono inoltre previsti dei cambiamenti a livello processuale. Allo scopo di ridurre l'asimmetria informativa tra produttori e consumatori, agli operatori economici potrà essere imposto l'obbligo di divulgazione delle prove. Nel complesso si avrà una notevole semplificazione probatoria a favore delle parti danneggiate, ma non si arriverà a un'inversione dell'onere della prova. Nella bozza vengono meno i limiti finora previsti per il massimale di responsabilità e la franchigia.

## Modifica dei regimi di responsabilità

Sulla base della bozza della direttiva sulla responsabilità per danno da prodotti difettosi il diritto al risarcimento è dato solo in caso di danni a persone (danni alla salute psichica inclusi), danni materiali e perdita di dati. Si tratta di una responsabilità da prodotto severa, che può essere fatta valere contro il produttore e altri operatori economici a prescindere da una loro eventuale colpa. Le rivendicazioni del caso possono essere sollevate solo da persone fisiche e solo laddove il prodotto in questione non venga utilizzato esclusivamente a scopi professionali.

## Nuova direttiva sulla responsabilità da IA a integrazione del quadro giuridico

La nuova direttiva sulla responsabilità per danno da prodotto difettoso verrà accompagnata da una direttiva sulla responsabilità da IA. Lo scopo di quest'ultima è quello di rendere molto più semplice, per chi ha subito danni provocati da sistemi di IA, far valere i propri diritti rifacendosi a una base giuridica diversa dalla legislazione sulla responsabilità per danno da prodotti. Ciò vale p. es. nel caso di violazioni di diritti fondamentali o legislazioni sulla responsabilità civile.

Onde evitare una frammentazione giuridica tra gli Stati membri dell'UE, dovrà essere definito un quadro giuridico armonizzato in materia di responsabilità di produttori, operatori o utilizzatori d'intelligenza artificiale. È previsto che, in caso di evento dannoso, si supponga che a causare quest'ultimo sia stata l'IA. La parte danneggiata dovrà solo dimostrare che il fornitore, operatore o utilizzatore dell'IA ha omesso colposamente di osservare un obbligo rilevante e che sussiste probabilmente un nesso causale. In caso di processo, inoltre, i produttori o fornitori di sistemi di IA ad alto rischio dovranno essere tenuti a mettere a disposizione tutte le informazioni di rilievo sul prodotto.

La direttiva sulla responsabilità da IA non attribuisce ancora diritti legali di risarcimento, bensì integra i regimi nazionali di responsabilità per colpa in caso di violazioni del diritto da parte dell'IA. I nuovi regimi di responsabilità per colpa rendono possibile la rivendicazione semplificata di pretese di risarcimento da parte di tutte le persone fisiche e giuridiche.

## Negoziati in seno alle istituzioni UE

Il Consiglio dei ministri UE ha già esaminato e approvato senza riserve la bozza della direttiva sulla responsabilità per danno da prodotti difettosi presentata dalla Commissione. Anche il dibattito in seno al Parlamento UE è già iniziato, ma durerà ancora qualche mese. La direttiva sulla responsabilità da IA verrà negoziata solo in un secondo momento.

*Freeric Meier*
*meier@kan.de*

[1] Studio di valutazione e proposte di direttiva: https://ec.europa.eu/commission/presscorner/detail/it/ip_22_5807

## Il Regno Unito proroga la validità della marcatura CE

Il Ministero dell'economia e del commercio del Regno Unito ha annunciato che, per quanto riguarda i prodotti immessi sul mercato britannico (ossia di Inghilterra, Scozia e Galles), il riconoscimento della marcatura CE verrà prorogato a tempo indeterminato oltre il dicembre del 2024. Per l'Irlanda del Nord ciò era già avvenuto. La regola si applica a 18 regolamenti rientranti nella sfera di competenze del ministero e riguardanti, non da ultimo, macchine, dispositivi di protezione individuale, attrezzature a pressione, apparecchi a bassa tensione, apparecchi Atex e apparecchi a gas.

In origine in Gran Bretagna la marcatura CE avrebbe dovuto cessare di essere riconosciuta a fine 2024 ed essere rimpiazzata da una marcatura UKCA (UK Conformity Assessed) obbligatoria. Con il nuovo regolamento in futuro le imprese potranno scegliere tra le due marcature. Ciò conviene sia alle imprese con sede nell'UE che a quelle britanniche: i loro prodotti non dovranno infatti più essere provvisti di una doppia certificazione per essere esportati nell'altrui spazio economico.

Maggiori informazioni (in inglese): www.gov.uk/government/news/uk-government-announces-extension-of-ce-mark-recognition-for-businesses

## Nuova campagna dell'EU-OSHA

A ottobre del 2023 l'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA) darà il via a una campagna della durata di due anni intitolata "Salute e sicurezza sul lavoro nell'era digitale". Per l'occasione l'EU-OSHA e i suoi punti di contatto nazionali organizzeranno una lunga serie di eventi a livello europeo e nazionale volti a sensibilizzare lavoratori, imprese e decisori politici nei confronti della salute e sicurezza sul lavoro.

Tra i temi cardine della campagna figurano il lavoro sulle piattaforme digitali, l'automatizzazione di compiti, il lavoro mobile e ibrido, la gestione del personale con l'ausilio dell'intelligenza artificiale e i sistemi digitali intelligenti. L'obiettivo è quello di rendere disponibili dati e fatti su questi temi che possano favorire la messa a punto di disposizioni giuridiche, linee guida, misure di sensibilizzazione e sostegno nonché nuovi prodotti e servizi rilevanti.

Informazioni sulla campagna: https://healthy-workplaces.osha.europa.eu/it

## Alla A+A 2023 c'è anche la KAN!

Dal 24 al 27 ottobre 2023 a Düsseldorf si terrà la fiera specialistica A+A. La KAN vi attende presso lo stand comune della DGUV, che quest'anno si troverà nel padiglione 5 (stand 5C06). Saremo lieti di fornirvi informazioni sui nostri attuali campi di attività – p. es. macchine semoventi senza guidatore, maschere anticontagio e grill a gas – presentarvi le nostre pubblicazioni e rispondere alle vostre domande sulla prevenzione e la normazione.

"Esseri umani normati – evoluzione delle misure corporee" – è questo il tema proposto dalla KAN in occasione della sua "Ora di ricevimento prevenzione", in programma giovedì 26 ottobre alle ore 10:00 presso il palco dello stand comune della DGUV.

Nel quadro del congresso A+A, che si svolge in parallelo, la KAN proporrà le seguenti relazioni:

- 25.10.2023: "VISION ZERO versus Standardization: A Position Statement"
- 26.10.2023: Norme sulla gestione rilevanti per la prevenzione al di là della ISO 45001

Trovate maggiori informazioni sul programma all'indirizzo Internet. www.aplusa-online.com. Vi aspettiamo!

## Seminari sull'attività di normazione nel campo della prevenzione

In collaborazione con l'istituto per il lavoro e la salute della DGUV (IAG) la KAN propone due seminari sull'attività di normazione nel campo della prevenzione.

Il seminario di base è rivolto ai membri attivi dei gruppi di normazione e a chiunque desideri affrontare il tema della normazione a beneficio di sicurezza e salute. Nel corso del seminario scoprite i processi di elaborazione delle norme e le possibilità di cui e altri esperti ed esperte di normazione di lungo corso e, insieme, riflettete su quali strategie potete adottare per ottimpotete avvalervi nelle varie fasi per esercitare la vostra influenza. I consigli e trucchi svelati in sede di seminario e lo scambio con i presenti vi aiutano a partecipare con successo all'attività di normazione. Il seminario di base si tiene a Dresda dal 25 al 27 ottobre 2023.

Conoscete a fondo le basi dell'attività di normazione e volete ampliare le vostre competenze? Nel seminario di approfondimento incontratizzare la vostra partecipazione ai lavori. Condividete inoltre esperienze in fatto di processo di normazione e possibilità d'influenza e ricevete informazioni aggiornate provenienti dal settore della normazione.

La fase in presenza del seminario di approfondimento si tiene a Dresda il 5 e 6 dicembre 2023. Le altre parti del seminario si svolgono online o in modalità di auto-apprendimento.

Informazioni e iscrizione:
https://asp.veda.net/webgate_dguv_prod, numero dell'evento: 570044 (seminario di base) e 570139 (seminario di apprendimento)

## Modifiche europee delle norme IEC

In base all'Accordo di Francoforte le norme elettrotecniche dovrebbero essere elaborate di preferenza a livello internazionale dallo IEC e nello stesso tempo essere recepite dal CENELEC come norme identiche (EN IEC). In alcuni casi, tuttavia, nel quadro del recepimento di norme IEC occorre apportare delle modifiche ai documenti, in modo che soddisfino i requisiti delle direttive o dei regolamenti europei sul mercato interno.

La presenza di modifiche è riconoscibile dal fatto che il CENELEC pubblica le norme interessate non come EN IEC 6xxxx bensì come EN 6xxxx – mantenendo però il numero attribuito loro dallo IEC.

# Eventi

**18.-20.10.23** » Dresden

Seminar
**Manipulation an Maschinen und Anlagen: Risiken erkennen, Maßnahmen ergreifen**
IAG
https://asp.veda.net/webgate_dguv_prod
🔎 570089

**19.10.23** » Bern

Tagung
**Schweizerische Tagung für Arbeitssicherheit**
SUVA
www.suva.ch 🔎 Tagung

**24.-27.10.23** » Düsseldorf

Messe und Kongress / Trade fair and Congress
**A+A 2023**
Messe Düsseldorf
www.aplusa-online.com

**25.10.23** » Online

Informationsveranstaltung
**Dresdner Treffpunkt „Kollege Roboter – Mensch-Roboter Interaktion in der betrieblichen Praxis“**
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Kollege Roboter

**25.-27.10.23** » Dresden

Seminar
**Grundlagen der Normungsarbeit im Arbeitsschutz**
IAG/KAN
https://asp.veda.net/webgate_dguv_prod
🔎 570044

**26.10.23** » Düsseldorf

Kongress
**GfA-Herbstkongress 2023 „Nachhaltige Sicherheit und Gesundheit bei der Arbeit“**
Gesellschaft für Arbeitswissenschaft (GfA)
www.gesellschaft-fuer-arbeitswissenschaft.de

**02.11.23** » Berlin

Nationaler Kick-off der EU-OSHA-Kampagne 2023-25
**Sicher und gesund arbeiten in Zeiten der Digitalisierung**
BAuA/DGUV/EU-OSHA
www.baua.de 🔎 Nationaler Kick-off

**13.11.23 – 18.01.24** » Dresden/Online

Seminar
**Normungsarbeit im Arbeitsschutz weiterdenken – Aufbauseminar**
IAG/KAN
https://asp.veda.net/webgate_dguv_prod 🔎 570139

**15.11.23** » Online

Informationsveranstaltung
**Dresdner Treffpunkt „Die neue europäische Maschinenverordnung“**
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Maschinenverordnung

**27.-28.11.23** » Bonn

Seminar
**Maschinenanlagen/Technische Anlagen**
MBT
www.maschinenbautage.eu/seminare/seminarmaschinenanlagen

**29.11.-01.12.23** » Dresden

Seminar
**Sicherer Einsatz von kollaborierenden Robotern**
Institut für Arbeit und Gesundheit der DGUV (IAG)
https://asp.veda.net/webgate_dguv_prod
🔎 570164

**04.-07.12.23** » Sankt Augustin

Seminar
**Sicherheitstechnik von Maschinen**
Institut für Arbeitsschutz der DGUV (IFA)
https://dguv.converia.de/frontend/index.php?sub=94

## Pubblicazioni della KAN

www.kan.de/en » Publications » KANBrief » KANBrief subscriptions (gratis)

Gefördert durch: Bundesministerium für Arbeit und Soziales aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

**Editore**
Verein zur Förderung der Arbeitssicherheit in Europa e.V. (VFA)
con supporto finanziario del Ministero Federale di Lavoro e degli Affari Sociali

**Redazione**
Kommission Arbeitsschutz und Normung, Segreteria KAN
Sonja Miesner, Michael Robert
Tel. +49 2241 231 3450 · www.kan.de · info@kan.de

**Responsabile**
Angela Janowitz, Alte Heerstr. 111, D – 53757 Sankt Augustin

**Traduzione**
Simona Rofrano

**Pubblicato trimestralmente, gratis**

**ISSN:** 2702-4024 (Print) · 2702-4032 (Online)