Simest, 200 milioni per investimenti e formazione in Africa

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 21

Sbloccata la luce calmierata agli energivori

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 24

Ex Ilva, si accelera entro luglio il bando di vendita

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 26

Urso / Incentivi auto saranno triennali

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 27

Conti pubblici, allarme Fmi

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 28

Zes unica, molte richieste e il tax credit si riduce

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 30

Contratto ceramica, nel rinnovo il test sulla

rappresentanza

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 32

Crt, un mese per convincere il Mef

scritto da datiweb | Luglio 24, 2024
selezione articoli 24 lug 2024 35

SOSTENIBILITA’| ASVIS – Corso e-learning “Azienda 2030 – Le opportunità dello sviluppo sostenibile”

scritto da Maria Rosaria Zappile | Luglio 24, 2024
Segnaliamo che, ASVIS ha realizzato il nuovo corso e-learning *“Azienda 2030: Le opportunità dello sviluppo sostenibile – versione 2.0”*, *ch*e ha l’obiettivo di approfondire le sfide e le opportunità di una trasformazione del modello di business tenendo conto delle spinte alla transizione verso uno sviluppo economico più sostenibile, tra le quali hanno un ruolo di primo piano gli ultimi sviluppi della normativa europea (es. *CSRD – Corporate Sustainability*

Reporting Directive, Regolamento Tassonomia).

In particolare, il corso Azienda 2030 si compone di **4 moduli,** cui si aggiungono diversi approfondimenti: **il primo** introduce il concetto di sviluppo sostenibile, ripercorrendo le tappe principali, e descrive come la sostenibilità sta trasformando l'economia e il business; **il secondo** descrive le opportunità della trasformazione e i principali *driver* del cambiamento per le imprese verso la sostenibilità; **il terzo** approfondisce i nuovi modelli di produzione, consumo e offerta di beni e servizi a cui far riferimento per mettere in atto la trasformazione sostenibile; i**l quarto** ha l'obiettivo di indicare il cammino da seguire per avviare il cambiamento, evidenziando i fattori critici di successo della trasformazione e le principali normative europee che coinvolgono le imprese (quali, ad esempio, la *CSRD* e il Regolamento Tassonomia).

Alla fine di ogni modulo, un test di 5 domande aiuta a verificare la comprensione dei messaggi più importanti.

Il teaser del corso è disponibile al seguente indirizzo: https://youtu.be/Pi-gtw_mgQA

Per ulteriori informazioni, cfr. allegati.

AZIENDA 2030 e learning presentazione e-learning Azienda 2030_ASviS

LAVORO | La sicurezza sul lavoro, delle macchine e

delle persone e la sicurezza dei dati, tra intelligenza artificiale e cybersecurity

scritto da Francesco Cotini | Luglio 24, 2024

La valutazione di tutti i rischi, al fondamento degli obblighi di salute e sicurezza, si alimenta continuamente di nuove fattispecie legate all'evoluzione della tecnologia.

Prendere spunto dall'impianto normativo nazionale (che estende la valutazione dei rischi e la conseguente azione prevenzionale ad ogni tipo di rischio), dalle recenti e non ancora operative previsioni del Regolamento macchine (UE/2023/1230) con riferimento sia all'uso dell'intelligenza artificiale sia alla necessità di prevenire attacchi informatici dall'esterno consente di delineare un quadro, sia attuale che di prospettiva, alla luce del quale adottare i comportamenti più adeguati, sui versanti tecnologico, organizzativo e culturale.

Va osservato che il quadro legislativo (comunitario e nazionale) è in rapida evoluzione, alcune norme sono già vigenti, altre sono approvate ma entreranno in vigore nei prossimi anni, altre ancora sono in fase di adozione al livello comunitario. È essenziale, quindi, anticipare l'applicazione concreta del complessivo quadro regolatorio attraverso una analisi che consenta di integrare i vari elementi, accomunati da una rapidissima evoluzione tecnologica.

- **Individuazione dei rischi ai fini della direttiva comunitaria (89/391/CEE) e del sistema nazionale di salute e sicurezza nei luoghi di lavoro (Dlgs 81/2008).**

1. **Il diritto comunitario**. Il punto di partenza è la

sentenza emanata all'esito della causa C-49/00 con la quale si è affermato che "*i rischi professionali che devono essere oggetto di una valutazione da parte dei datori di lavoro non sono stabiliti una volta per tutte, ma si evolvono costantemente in funzione, in particolare, del progressivo sviluppo delle condizioni di lavoro e delle ricerche scientifiche in materia di rischi professionali.*"

2. **La lettura della normativa nazionale (Cass, 29 gennaio 2024, n. 3405**). L'ampia dizione dell'art. 28 del Dlgs 81/2008, letto alla luce della direttiva comunitaria sopra richiamata, legittima l'altrettanto ampio spettro assegnato dalla giurisprudenza nazionale ai contenuti della valutazione dei rischi. Il datore di lavoro è, infatti, "*tenuto a redigere e sottoporre ad aggiornamento il documento di valutazione dei rischi previsto dall'art. 28 del Lgs. n. 81 del 2008, all'interno del quale deve indicare in modo specifico i fattori di pericolo concretamente presenti all'interno dell'azienda, in relazione alla singola lavorazione o all'ambiente di lavoro e le misure precauzionali ed i dispositivi adottati per tutelare la salute e la sicurezza dei lavoratori*". Inoltre, "*la redazione del documento di valutazione dei rischi e l'adozione di misure di prevenzione non escludono la responsabilità del datore di lavoro quando, per un errore nell'analisi dei rischi o nell'identificazione di misure adeguate, non sia stata adottata idonea misura di prevenzione.*"
3. **L'impatto dell'art. 2087 cc sull'evoluzione tecnologica (Cass., 5 aprile 2024, n. 9120).** Con la sua logica di "norma aperta di chiusura dell'ordinamento", l'art. 2087 cc contiene una formulazione che, "*attraverso l'espresso riferimento alle misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie a tutelare la integrità fisica e la personalità morale dei prestatori di lavoro, correla l'obbligo di protezione alle concrete e indefinite situazioni di rischio a cui*

il lavoratore può trovarsi esposto e in tal modo impone al datore di lavoro l'adozione non solo delle misure cd. nominate ma anche di tutte quelle che, seppure non tipizzate, siano richieste dalle conoscenze tecniche e dall'esperienza riferite ad un determinato momento storico".

4. **Gli obblighi del datore di lavoro (art. 70 Dlgs 81/2008).** Secondo l'art. 70 del Dlgs 81/2008, "*le attrezzature di lavoro messe a disposizione dei lavoratori devono essere conformi alle specifiche disposizioni legislative e regolamentari di recepimento delle direttive comunitarie di prodotto".*

È, quindi, evidente come i temi dell'evoluzione tecnologica (le moderne macchine e attrezzature di lavoro), l'integrazione delle macchine con forme di intelligenza artificiale e l'esposizione delle stesse macchine (e di tutta l'azienda) all'attacco esterno sono temi che entrano di diritto all'interno della valutazione dei rischi prevista dall'art. 28 del Dlgs 81/2008.

- **Il regolamento macchine**

1. Per quanto concerne l'**intelligenza artificiale**al 12° considerando del Regolamento evidenzia che "di recente sono state immesse sul mercato macchine più avanzate, meno dipendenti dagli operatori umani. Tali macchine lavorano a compiti definiti e in ambienti strutturati, tuttavia possono imparare a svolgere azioni nuove in tale contesto e diventare più autonome. Tra gli ulteriori perfezionamenti alle macchine, già realizzati o attesi, figurano l'elaborazione in tempo reale di informazioni, la risoluzione di problemi, la mobilità, i sistemi di sensori, l'apprendimento, l'adattabilità e la capacità di funzionare in ambienti non strutturati (ad esempio cantieri). La relazione della Commissione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica del 19

febbraio 2020 in materia di sicurezza e di responsabilità afferma che l'emergere di nuove tecnologie digitali, quali l'intelligenza artificiale, l'Internet delle cose e la robotica, pone nuove sfide in termini di sicurezza dei prodotti. La relazione conclude che la vigente normativa in materia di sicurezza dei prodotti, compresa la direttiva 2006/42/CE, presenta una serie di lacune in merito che devono essere colmate. Di conseguenza il presente regolamento dovrebbe disciplinare i rischi di sicurezza derivanti da nuove tecnologie digitali".

2. Per quanto concerna la **cibersicurezza**, al 25° considerando si ribadisce che "*altri rischi relativi a nuove tecnologie digitali sono quelli provocati da terzi malintenzionati che incidono sulla sicurezza dei prodotti rientranti nell'ambito di applicazione del presente regolamento. A tale proposito i fabbricanti dovrebbero essere tenuti ad adottare misure proporzionate che si limitano alla protezione della sicurezza dei prodotti rientranti nell'ambito di applicazione del presente regolamento. Ciò non preclude l'applicazione ai prodotti rientranti nell'ambito di applicazione del presente regolamento di altri atti giuridici dell'Unione che affrontano specificamente aspetti di cibersicurezza*".
3. Più in concreto, il tema delle forme di **intelligenza artificiale**, anche autoevolutiva, viene in considerazione nella valutazione dei rischi da parte del produttore, laddove si prevede che
4. (art. 8) "*le macchine o i prodotti correlati sono messi a disposizione sul mercato o messi in servizio soltanto se, quando debitamente installati, sottoposti a manutenzione e utilizzati conformemente al loro uso previsto o in condizioni ragionevolmente prevedibili, soddisfano i requisiti essenziali di sicurezza e di tutela della salute di cui all'allegato III*".
5. (art. 10) "*all'atto dell'immissione sul mercato o della*

messa in servizio di una macchina o di un prodotto correlato, i fabbricanti garantiscono che siano stati progettati e fabbricati conformemente ai requisiti essenziali di sicurezza e di tutela della salute di cui all'allegato III".

- (art. 3) definisce i requisiti essenziali di sicurezza e di tutela della salute come "*le disposizioni obbligatorie, di cui all'allegato III, relative alla progettazione e alla costruzione di prodotti rientranti nell'ambito di applicazione del presente regolamento, intese ad assicurare un livello elevato di tutela della salute e di sicurezza delle persone*" e, dove, quindi, "*la documentazione tecnica deve specificare i mezzi utilizzati dal fabbricante per assicurare la conformità della macchina o del prodotto correlato ai requisiti essenziali di sicurezza e di tutela della salute applicabili*".

1. Quanto alle problematiche di **cibersicurezza**, l'art. 20 del Regolamento evidenzia che "*le macchine e i prodotti correlati che sono stati certificati o per i quali è stata emessa una dichiarazione di conformità nell'ambito di un sistema di certificazione della cibersicurezza adottato conformemente al regolamento (UE) 2019/881 e i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea, sono considerati conformi ai requisiti essenziali di sicurezza e di tutela della salute di cui all'allegato III, punti 1.1.9 e 1.2.1, per quanto concerne la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo nella misura in cui tali requisiti siano contemplati dal certificato di cibersicurezza o dalla dichiarazione di conformità o da loro parti*."

Il Regolamento UE 2019/881 è stato tradotto nel Dlgs 3 agosto 2022, n. 123.

Il medesimo Regolamento 2023/1230, all'allegato III, prevede – tra l'altro – che

- (punto 1.1.9) "l*a macchina o il prodotto correlato devono essere progettati e costruiti in modo tale da fare sì che il collegamento ad essi di un altro dispositivo, tramite qualsiasi caratteristica del dispositivo connesso stesso o tramite qualsiasi dispositivo remoto che comunica con la macchina o il prodotto correlato, non determini una situazione pericolosa*".
- (punto 1.2.1) "*i sistemi di comando devono essere progettati e costruiti in modo tale che: a) riescano a resistere, se del caso, a circostanze e rischi, a previste sollecitazioni di servizio e ad influssi esterni intenzionali o meno, compresi tentativi deliberati ragionevolmente prevedibili da parte di terzi che conducono a una situazione pericolosa*".
- **Intelligenza artificiale e gestione del rischio (Regolamento sull'intelligenza artificiale del 13 giugno 2024)**

Nella Gazzetta Ufficiale della UE del 12 luglio 2024 è stato pubblicato il **Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate sull'intelligenza artificiale.**

Secondo il **considerando 50**, "*per quanto riguarda i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione elencata nell'allegato al presente regolamento, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto interessato è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione. Tali prodotti sono, in particolare, macchine, giocattoli,*

ascensori, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici, dispositivi medico-diagnostici in vitro, veicoli automobilistici e aeronautici".

Secondo il **considerando 64, "***al fine di attenuare i rischi derivanti dai sistemi di IA ad alto rischio immessi sul mercato o messi in servizio e per garantire un elevato livello di affidabilità, è opportuno applicare determinati requisiti obbligatori ai sistemi di IA ad alto rischio, tenendo conto della finalità prevista e del contesto dell'uso del sistema di IA e conformemente al sistema di gestione dei rischi che deve essere stabilito dal fornitore. Le misure adottate dai fornitori per conformarsi ai requisiti obbligatori del presente regolamento dovrebbero tenere conto dello stato dell'arte generalmente riconosciuto in materia di IA ed essere proporzionate ed efficaci per conseguire gli obiettivi del presente regolamento. Sulla base del nuovo quadro legislativo, come chiarito nella comunicazione della Commissione "La "Guida blu" all'attuazione della normativa UE sui prodotti 2022″, di norma più di un atto giuridico della normativa di armonizzazione dell'Unione può essere applicabile a un prodotto, poiché quest'ultimo può essere messo a disposizione o messo in servizio solo se risulta conforme a tutta la normativa di armonizzazione dell'Unione applicabile. I pericoli dei sistemi di IA disciplinati dai requisiti del presente regolamento riguardano aspetti diversi rispetto alla vigente normativa di armonizzazione dell'Unione e pertanto i requisiti del presente regolamento completerebbero il corpus esistente della normativa di armonizzazione dell'Unione. Ad esempio, le macchine o i dispositivi medici in cui è integrato un sistema di IA potrebbero presentare rischi non affrontati dai requisiti essenziali di sicurezza e di tutela della salute stabiliti nella pertinente normativa armonizzata dell'Unione,*

in quanto tale normativa settoriale non affronta i rischi specifici dei sistemi di IA".

- **Cibersicurezza e gestione del rischio (direttiva 2022/2555 del 14 dicembre 2022 e Cyber resilience act)**

La Direttiva (art. 21) prevede che i soggetti rilevanti (le aziende appartenenti ai settori ad alta criticità) "*adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi*".

Il tema della valutazione dei rischi e dell'interconnessione con l'IA è oggetto di attenzione anche nell'ambito del Regolamento europeo che punta a definire i requisiti di cyber security per i prodotti con componenti digitali immessi sul mercato europeo, il Cyber Resilience Act (CRA), approvato dal Parlamento europeo il 12 marzo 2024.

Il considerando 53 evidenzia che "i *fabbricanti di prodotti che rientrano nell'ambito di applicazione del regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio che sono anche prodotti con elementi digitali ai sensi del presente regolamento (CRA) dovrebbero rispettare sia i requisiti essenziali di cui al presente regolamento sia i requisiti essenziali di sicurezza e di tutela della salute di cui al regolamento (UE) 2023/1230. I requisiti essenziali di cui al presente regolamento e alcuni requisiti essenziali del regolamento (UE) 2023/1230 potrebbero affrontare rischi di cibersicurezza simili. La conformità ai requisiti essenziali di cui al presente regolamento (CRA) potrebbe pertanto facilitare la conformità ai requisiti essenziali che coprono anche determinati rischi di cibersicurezza di cui al regolamento (UE) 2023/1230, in particolare quelli riguardanti la protezione contro la corruzione e la sicurezza e*

l'affidabilità dei sistemi di controllo di cui all'allegato III, sezioni 1.1.9 e 1.2.1, di tale regolamento".

L'articolo 13 – nel declinare gli obblighi degli operatori economici (in particolare, i fabbricanti) – prevede che "*fabbricanti effettuano una valutazione dei rischi di cibersicurezza associati a un prodotto con elementi digitali e tengono conto dei risultati di tale valutazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto con elementi digitali, allo scopo di ridurre al minimo i rischi di cibersicurezza, prevenire gli incidenti e ridurne al minimo l'impatto, anche in relazione alla salute e alla sicurezza degli utilizzatori…*"

"*…La valutazione dei rischi di cibersicurezza è documentata e aggiornata, se del caso, durante un periodo di assistenza da determinare conformemente al paragrafo 8 del presente articolo. Tale valutazione comprende almeno un'analisi dei rischi di cibersicurezza basata sulla finalità prevista e sull'uso ragionevolmente prevedibile del prodotto con elementi digitali, nonché sulle sue condizioni d'uso, quali l'ambiente operativo o gli attivi da proteggere, tenendo conto della durata di utilizzo del prodotto prevista".*

Da notare, che – tra i prodotti con elementi digitali importanti, e quindi soggetti alle procedure di valutazione della conformità – rientrano, tra l'altro, i *prodotti indossabili personali da indossare o collocare sul corpo umano a fini di monitoraggio della salute* (come il tracciamento) e ai quali non si applica il regolamento (UE) 2017/745 o il regolamento (UE) 2017/746, gli *ipervisori e sistemi di runtime container che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili.*

- **Rapporto tra IA e cibersicurezza**

Secondo l'**art. 15 del Regolamento europeo sull'intelligenza artificiale del 13 giugno 2024**, "*i sistemi di IA ad alto*

rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso, gli output o le prestazioni sfruttando le vulnerabilità del sistema. Le soluzioni tecniche volte a garantire la cibersicurezza dei sistemi di IA ad alto rischio sono adeguate alle circostanze e ai rischi pertinenti. Le soluzioni tecniche finalizzate ad affrontare le vulnerabilità specifiche dell'IA includono, ove opportuno, misure volte a prevenire, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare il set di dati di addestramento (data poisoning – "avvelenamento dei dati") o i componenti preaddestrati utilizzati nell'addestramento (model poisoning – "avvelenamento dei modelli"), gli input progettati in modo da far sì che il modello di IA commetta un errore (adversarial examples – "esempi antagonistici", o model evasion, – "evasione dal modello"), gli attacchi alla riservatezza o i difetti del modello".

Il sopra richiamato **Cyber Resilience Act,** all'art. 12 si preoccupa di coordinare la ciberisucrezza con l'IA prevedendo che *"prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento e sono classificati come sistemi di IA ad alto rischio ai sensi dell'[articolo 6] di tale regolamento sono considerati conformi ai requisiti relativi alla cibersicurezza di cui all'[articolo 15] di tale regolamento qualora:*

1. *a) tali prodotti soddisfino i requisiti essenziali di cui all'allegato I, parte I;*
2. *b) i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cui all'allegato I, parte 2;*
3. *c) il conseguimento del livello di protezione della cibersicurezza richiesta a norma dell'[articolo 15] del regolamento … [il regolamento sull'IA] sia dimostrato nella dichiarazione di conformità UE rilasciata a norma del presente regolamento."*

- **Conclusioni**

Già da queste prime indicazioni, di natura squisitamente normativa (alle quali si aggiungono aspetti applicativi legati alla normativa tecnica (es. ISO/IEC 27001:2022) è del tutto evidente come tra sicurezza sul lavoro, intelligenza artificiale e cibersicurezza occorra valorizzare l'elemento comune e centrale della valutazione dei rischi e della conseguente adozione di un adeguato sistema di gestione.

RELAZIONI INDUSTRIALI:

Giuseppe Baselice 089200829 g.baselice@confindustria.sa.it

Francesco Cotini 089200815 f.cotini@confindustria.sa.it