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

Periodico di informazione per i CLIENTI dello STUDIO VIOLI

Indice delle NOTIZIE (N)

- N1) D.Lgs. 231/01: Whistleblowing, dal 15 luglio in vigore le nuove regole per le grandi aziende
- N2) Privacy: Data Privacy Framework. La lotta contro il nuovo accordo sui dati dell'UE
- N3) Privacy: Garante Privacy, triplicate le ispezioni con oltre 9 milioni di euro di sanzioni riscosse
- N4) Privacy: App per rimborso pedaggi: multa di un milione ad Aspi per uso illecito dei dati; È italiano il nuovo tool gratuito anti-ransomware che riesce a contrastare fino al 94% degli attacchi informatici
- N5) Sicurezza: La rettifica del regolamento macchine: le nuove date di applicazione
- N6) Sicurezza: La legge n. 85/2023 ha convertito il Decreto-Legge 48 (Decreto lavoro) del governo in materia di lavoro che all'articolo 14 modifica il D.Lgs. n. 81/2008

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

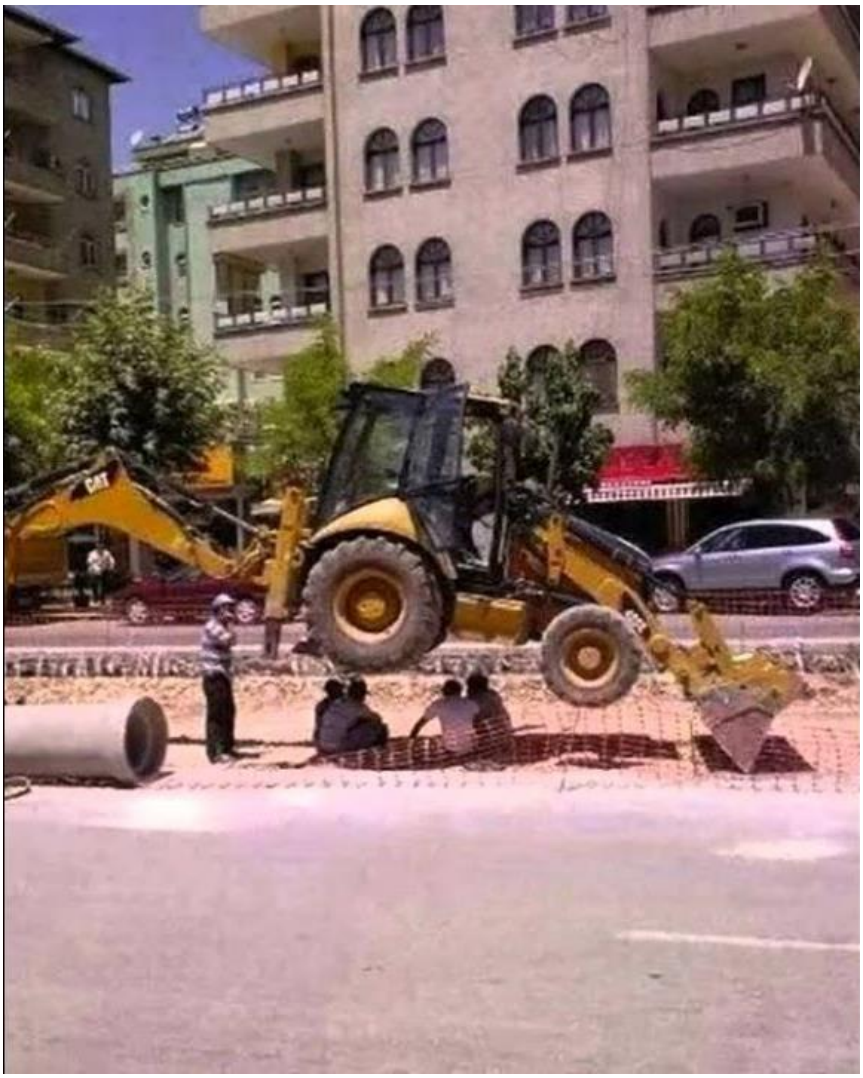
AFORISMA DEL MESE

"Se lo sviluppo economico non ci rende anche felici, allora è un falso sviluppo"

José Pepe Mujica – ex Presidente dell'Uruguay

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

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



“Protezione solare”

Notizie

- N1) D.Lgs. 231/01: Whistleblowing, dal 15 luglio in vigore le nuove regole per le grandi aziende

È entrato in vigore il 15 luglio 2023 il dlgs. n.24/2023 che dà attuazione alla direttiva (Ue) 2019/1937 in materia di whistleblowing, fatto salvo il termine più ampio del 17 dicembre 2023 per i soggetti del settore privato che abbiano impiegato fino a 249 lavoratori nell'ultimo anno.

La nuova normativa, che racchiude in un unico testo la disciplina del settore pubblico e privato, **ha definito in maniera organica un complesso regime di obblighi e tutele che ampliano le garanzie per i «segnalanti» (e le persone legate al whistleblower da stabili rapporti affettivi o di parentela entro il quarto grado, nonché ai c.d. «facilitatori» e agli enti di proprietà di tutti questi soggetti), al fine di incentivare il sistema di segnalazione che pregiudichi l'integrità dell'ente o l'interesse pubblico.**

Insomma, per le imprese, e di ritorno gli studi legali, la partita si fa sempre più complessa. «I gruppi multinazionali si stanno predisponendo ad aggiornare i propri sistemi whistleblowing conciliando la nuova normativa con esigenze interne di efficienza e temi cross-border; l'affinamento dei sistemi di segnalazione elettronici richiede conoscenza accurata delle tecnologie disponibili sul mercato – tema al momento prioritario per le aziende - e di quali soluzioni siano migliori e più adatte per l'organizzazione aziendale di riferimento; è in corso di formazione una best practice su come ottimizzare la scelta di chi debba essere costituito destinatario delle segnalazioni», spiega Federico Busatta, partner del dipartimento contenzioso e arbitrati dello studio legale Gianni & Origoni.

Secondo Alessandro Musella, partner e leader del Focus Team corporate compliance & investigations di BonelliErede, «gli adempimenti a carico delle aziende sono significativi e molte non sembrano avere una struttura interna adeguata a farvi fronte. I più complessi da attuare, soprattutto per le aziende di minori dimensioni, **sono la necessità di attivare canali di segnalazione che devono garantire il requisito di protezione dell'identità del segnalante e di avere una persona o ufficio interno che sia autonomo, dedicato, con personale specificamente formato oppure affidare la gestione a una persona o un ufficio esterno che garantisca i medesimi requisiti.**

Quanto alle sanzioni dell'Autorità nazionale anticorruzione (Anac), si tratta di sanzioni di tipo amministrativo che variano dai 10.000 ai 50.000 euro e che si applicano se non sono stati istituiti canali di segnalazione conformi ai requisiti del decreto o non sono state adottate le procedure indicate dal decreto. Tuttavia il vero rischio per le società che non implementano un sistema di segnalazione conforme ai requisiti è quello di subire segnalazioni «pubbliche», cioè indirizzate direttamente all'Anac (che poi può attivare indagini sull'azienda) o addirittura segnalazioni oggetto di «divulgazione pubblica» secondo le modalità previste dal decreto.

«Maggiori difficoltà interpretative, allo stato attuale della disciplina e in attesa di eventuali chiarimenti da parte delle Autorità, emergono nei punti di contatto con il modello di gestione 231. Nello specifico, la scelta di deferire la gestione delle segnalazioni ad un ufficio interno lascia irrisolto il problema del raccordo tra l'ufficio «gestore» della segnalazione e l'OdV, che non può rimanere totalmente escluso dalla notizia circa l'invio di una segnalazione, la sua indagine e la relativa conclusione, soprattutto quando questa riguardi condotte rilevanti ai sensi del d.lgs. 231/2001 o evidenzi una o più violazioni del Modello organizzativo. **Tra le problematiche più complesse ed impellenti vi è, in primo luogo, l'adempimento relativo all'attivazione del canale interno, per il quale assume rilevanza fondamentale una corretta valutazione circa le misure di sicurezza idonee a garantire la riservatezza dell'identità del segnalante e del segnalato, nonché il contenuto della segnalazione. Il tema**

solleva evidenti punti di contatto con la disciplina in materia di protezione dei dati personali, per cui, in ottica del principio di accountability e di privacy by design, il datore di lavoro dovrà, non solo procedere con il compimento di una valutazione del rischio (cd. «DPIA» dall'inglese: Data Protection Impact Assessment) di cui all'art. 35 del Gdpr, ma anche mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio già nella fase di progettazione.»

Appare invece sicuramente «propizio» il momento di emanazione del d.lgs. 24/2023: difatti, l'ennesima revisione del d.lgs. 50/2016 (il cd. codice degli appalti pubblici) e la parziale deregolamentazione degli affidamenti saranno senz'altro un interessante banco di prova per la nuova disciplina.

È importante ricordare che un funzionale raccordo tra «modello 231», registri in materia di data protection e canali per il whistleblowing sono elementi fondamentali per tutelare non solo i diritti dei singoli dipendenti, ma anche per evitare di esporre amministratori e il management a rischi inutili.

- N2) Privacy: Data Privacy Framework. La lotta contro il nuovo accordo sui dati dell'UE

Cosa succede a tutti i dati che Google, Amazon, Facebook e altre aziende tecnologiche americane raccolgono nel Vecchio Continente?

È una domanda che riguarda milioni di persone in Europa: cosa succede a tutti i dati che Google, Amazon, Facebook e altre aziende tecnologiche americane raccolgono nel Vecchio Continente? Possono trasferirli negli Stati Uniti?

L'UE adesso si fida

L'UE adesso pensa di sì. La Commissione ha approvato il cosiddetto Data Privacy Framework. È un accordo che consente il libero flusso di dati personali attraverso l'Atlantico. Le piattaforme online americane saranno così autorizzate a memorizzare le informazioni degli utenti europei sui propri server nazionali. I due quadri normativi precedenti, entrambi predecessori di questo accordo erano stati dichiarati invalidi dalla Corte di giustizia europea (ECJ). Il tentativo numero tre avrà successo? Ci sono diversi motivi di scetticismo.

Fattore Schrems

Privacy Shield e Safe Harbor erano stati bloccati dall'avvocato austriaco Max Schrems. Ora vuole anche fare causa contro il Data Privacy Framework, come dice al quotidiano tedesco WELT. "Abbiamo già diverse opzioni legali nel cassetto". Ha detto che si aspetta che il caso finisca davanti alla CGE all'inizio del prossimo anno. I giudici potrebbero sospendere il nuovo accordo sui dati tra Bruxelles e Washington per la durata del procedimento. I giganti tecnologici americani avrebbero quindi un problema. Sottolineano ripetutamente che vale la pena fare affari nell'UE solo se sono autorizzati a trattare le informazioni degli utenti di Internet negli Stati Uniti. Qualche tempo fa, Facebook ha persino minacciato di lasciare l'Europa se non fosse più consentito inviare dati a casa. Ma quella era probabilmente una trovata pubblicitaria; un tentativo di fare pressioni sulla Commissione.

I precedenti Schrems I e Schrems II

Le precedenti sentenze della Corte di giustizia sono note come Schrems I e Schrems II. Presto seguirà probabilmente Schrems III. E ancora una volta la posta in gioco è alta. Alla fine, sono in gioco il futuro delle

aziende tecnologiche americane in Europa e la privacy dei cittadini dell'UE. Il Data Privacy Framework è una copia del Privacy Shield, afferma Schrems. E Privacy Shield, a sua volta, una copia di Safe Harbor. "L'ultimo accordo non si basa su cambiamenti materiali", afferma Schrems, "ma su un pensiero politico a breve termine".
Per la Ue l'aria è cambiata
Nel 2015, la Corte di giustizia aveva dichiarato per la prima volta l'invalidità di Safe Harbor, seguita dal suo successore Privacy Shield nel 2020. Ogni volta, le promesse dei due accordi suonavano buone: un porto sicuro per i dati personali e uno scudo per la privacy. Ma la realtà era diversa: i giudici hanno ritenuto che gli accordi non proteggessero adeguatamente i dati degli europei. Soprattutto, la Corte di giustizia ha criticato il fatto che le agenzie di intelligence americane potessero sottrarre informazioni in massa senza sospetti. Ora, nell'accordo numero tre, Bruxelles ha certificato che gli Stati Uniti dispongono di una protezione dei dati "adeguata". Ciò significa che il livello di protezione negli Stati Uniti soddisfa gli standard europei. Le agenzie di intelligence americane, afferma la Commissione, dovrebbero essere autorizzate a intercettare le informazioni dei cittadini dell'UE solo se necessario per la sicurezza nazionale e proporzionato.

Ma Schrems non si fida

Schrems non la vede così. Pensa che le agenzie di intelligence statunitensi abbiano ancora troppo accesso ai dati degli europei. Potrebbero continuare a spiare persone in Germania, Austria e altri paesi dell'UE, proprio così, come vogliono, senza sospetti concreti o autorizzazione giudiziaria. L'America, afferma Schrems, attribuirà un significato diverso alla parola "proporzionato" rispetto alla Corte di giustizia.
L'ultima parola alla Corte di Giustizia Ue
Schrems non è solo in questa valutazione. Un rapporto del Parlamento europeo afferma inoltre che agli Stati Uniti non può essere garantita l'adeguatezza nella protezione dei dati. La scorsa settimana il commissario europeo per la giustizia Didier Reynders ha difeso il Data Privacy Framework. Secondo il ministro, questa volta l'accordo resisterà al vaglio della Corte di giustizia. Questo perché questo terzo tentativo differisce in modo significativo da Privacy Shield e Safe Harbor, ha affermato Reynders. Ad esempio, crea un tribunale che consente agli europei di intentare causa negli Stati Uniti se ritengono che non sia stato effettuato un accesso ai loro dati in modo "proporzionato". Vedremo presto se tutto ciò soddisferà la Corte di giustizia europea.

- N3) Privacy: Garante Privacy, triplicate le ispezioni con oltre 9 milioni di euro di sanzioni riscosse

In un momento storico caratterizzato da un ricorso sempre più massiccio alle piattaforme on line e dallo sviluppo dell'intelligenza artificiale, è un Garante per la Privacy impegnato su numerosi fronti quello che emerge dalla presentazione della Relazione annuale delle attività svolte lo scorso anno dall'Autorità presieduta da Pasquale Stanzione.

Come emerge dalla Relazione annuale, il 2022 ha infatti visto il Garante alle prese con una serie di interventi centrati sulle grandi questioni legate alla tutela dei diritti fondamentali delle persone nel mondo digitale, in particolare, **quelle riguardanti le implicazioni etiche della tecnologia, l'economia fondata sui dati, le grandi piattaforme e la tutela dei minori, i sistemi di age verification, i big data, l'intelligenza artificiale generativa, il Metaverso e le problematiche poste dagli algoritmi, gli scenari tracciati dalle neuroscienze, la sicurezza dei**

sistemi e la protezione dello spazio cibernetico, la monetizzazione delle informazioni personali, i fenomeni del revenge porn, del cyberbullismo, dello sharenting, e del social scoring.

Particolare attenzione dell'Authority è stata rivolta all'uso dei dati biometrici e al diffondersi di sistemi di riconoscimento facciale, come nel caso di Clearview che ha portato ad una sanzione da 20 milioni di euro inflitta alla società statunitense, a cui è stato vietato l'uso dei dati biometrici e il monitoraggio degli italiani.

Sul fronte della tutela on line dei minori l'anno scorso è proseguita in modo intenso l'azione di vigilanza sull'età di iscrizione ai social, anche attraverso sistemi di age verification, ed anche altre criticità che riguardano direttamente i minori, come nella vicenda di Tik Tok, che a seguito dell'intervento dell'autorità italiana ha sospeso l'invio di pubblicità personalizzata ai minori basata sul legittimo interesse, ritenuta una base giuridica inadeguata con seri rischi che la pubblicità potesse raggiungere i giovanissimi con contenuti non appropriati.

Di recente, l'intervento del Garante su ChatGpt ha poi consentito di indirizzare lo sviluppo dell'intelligenza artificiale generativa in una direzione compatibile con la tutela delle persone, specie se minori.

Per contrastare il fenomeno del revenge porn e aiutare le persone che temono la diffusione di foto e video a contenuto sessualmente esplicito il Garante ha inoltre introdotto un modello di segnalazione sicuro che ha visto circa 150 segnalazioni ricevute, le quali sono state trattate tempestivamente, e che nella maggior parte dei casi hanno portato a provvedimenti diretti alle piattaforme coinvolte per ottenere il blocco preventivo della diffusione delle foto e dei video.

Significativo anche il numero dei data breach notificati nel 2022 al Garante da parte di soggetti pubblici e privati: 1351. Nel settore pubblico (31,2% dei casi), le violazioni hanno riguardato soprattutto comuni, istituti scolastici e strutture sanitarie, nel settore privato (68,8% dei casi) sono stati coinvolte sia PMI e professionisti che grandi società del settore delle telecomunicazioni, energetico bancario e dei servizi. Nei casi più gravi sono stati adottati provvedimenti di tipo sanzionatorio.

Il processo di digitalizzazione della P.a. ha subìto una forte accelerazione, soprattutto per la necessità di dare attuazione al Pnrr, e il Garante è intervenuto, tra l'altro, sullo Spid per i minori, sulla Cield, sul Sistema di gestione delle deleghe, sulla Piattaforma dei benefici economici erogati da soggetti pubblici, sui Siti web della Pubblica Amministrazione.

Sempre per quanto riguarda la pubblica amministrazione, il Garante ha richiamato Ministeri, Enti locali e Regioni ad evitare diffusioni illecite di dati personali e a contemperare obblighi di pubblicità degli atti e dignità delle persone, e ha bloccato sul nascere iniziative locali volte all'erogazione di benefici basati su meccanismi di scoring associati a comportamenti "virtuosi" dei cittadini in vari settori.

Sotto la lente del Garante anche il cosiddetto spoofing, ossia l'effettuazione di chiamate promozionali indesiderate realizzate attraverso il camuffamento del numero chiamante.

Per quanto riguarda l'attività di relazione con il pubblico, nel 2022 l'Autorità ha dato riscontro a oltre 16.400 quesiti, che hanno riguardato, in maniera preponderante, gli adempimenti connessi all'applicazione del GDPR.

I provvedimenti correttivi e sanzionatori sono stati 317, mentre le sanzioni riscosse ammontano a circa 9,5 milioni di euro. Le ispezioni effettuate nel 2022, svolte anche con il contributo del Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza, sono state 140, quasi triplicate rispetto a quelle dell'anno precedente in cui ancora si subiva l'impatto dell'emergenza pandemica.

-N4) Privacy: App per rimborso pedaggi: multa di un milione ad Aspi per uso illecito dei dati; È italiano il nuovo tool gratuito anti-ransomware che riesce a contrastare fino al 94% degli attacchi informatici

App per rimborso pedaggi: multa di un milione ad Aspi per uso illecito dei dati Una sanzione di un milione di euro è stata comminata dal Garante privacy ad Autostrade per l'Italia spa (ASPI) per avere trattato in modo illecito i dati di circa 100mila utenti registrati alla app per il rimborso del pedaggio, denominata Free to X. Le criticità del servizio – che consente la restituzione, totale o parziale, del costo del biglietto autostradale per i ritardi dovuti ai cantieri di lavoro – erano state segnalate al Garante da una associazione di consumatori. L'Autorità ha accertato che Autostrade riveste il ruolo di titolare del trattamento e non di responsabile, come invece indicato nella documentazione che regola i rapporti tra Aspi e la società Free to X che ha realizzato e gestisce la app, nonché nell'informativa resa al riguardo agli utenti. È stata Aspi infatti, in qualità di concessionario della rete autostradale, ad aver individuato il meccanismo di rimborso, la natura delle misure compensative, le modalità di adempimento, la tipologia del ritardo correlato alla presenza dei cantieri, attribuendo a Free to X solamente compiti di attuazione del servizio. La errata qualificazione dei ruoli privacy rivestiti dalle due società – sottolinea il Garante – ha immediate ripercussioni sull'informativa resa agli utenti che pertanto non è stata correttamente formulata. L'informativa avrebbe dovuto infatti riportare l'effettiva identità del titolare, ossia Aspi, nonché tutte le ulteriori informazioni per assicurare un trattamento corretto e trasparente, come previsto dal Regolamento. Aspi è incorsa, inoltre, in una ulteriore violazione per non aver designato Free to X quale responsabile del trattamento. Il Garante non ha indicato ad Aspi misure correttive poiché la società nel corso del procedimento si è conformata alla normativa privacy.

È italiano il nuovo tool gratuito anti-ransomware che riesce a contrastare fino al 94% degli attacchi informatici Arriva dall'Università di Bologna e di Arpae Emilia-Romagna un nuovo tool gratuito e open-source per contrastare i ransomware con un potenziale di protezione dagli attacchi informatici che arriva fino al 94%. Si chiama Ranflood, ed è stato messo a punto da un gruppo di ricercatori dell'ateneo emiliano. Il software funziona per Windows, macOs e Linux, ed agisce come una "trappola dinamica" che insegue il virus e gli somministra dei file-esca, guadagnando così tempo per svelare l'attacco in corso ed essendo in grado di prendere contromisure e di salvare i propri file su un dispositivo diverso. In pratica, Ranflood contrasta gli attacchi ransomware inondando cartelle specifiche (ad esempio, dove il ransomware sta crittografando i file, le cartelle dell'utente) con file esca, come spiega Saverio Giallorenzo, ricercatore al Dipartimento di Informatica - Scienza e Ingegneria dell'Università di Bologna, che è tra gli autori dello studio: "Questo progetto parte da una nuova interpretazione di una tecnica di contrasto ai virus già nota, basata sul predisporre delle 'trappole', o file-esca, che svelano la presenza di malintenzionati nel sistema. Da questa base di partenza, con Ranflood siamo riusciti a rendere la trappola 'dinamica': il sistema, cioè, insegue il virus per somministrargli i file-esca, che quindi non servono più solo per svelare un attacco, ma anche per sviarlo e salvare i dati reali della vittima". In questo modo, questo software può così anche aiutare gli utenti a recuperare i propri file una volta che il ransomware è stato fermato. La soluzione è stata testata in ambiente controllato su alcuni dei ransomware più noti, tra cui WannaCry (che mise in ginocchio la sanità inglese nel 2017) e LockBit (il virus usato nel 2021 per disabilitare i servizi della Regione Lazio). I risultati, pubblicati su Computer & Security, tra le riviste più prestigiose nel campo della sicurezza informatica, sono molto positivi, con un elevatissimo potenziale di protezione dagli attacchi. Attualmente, i ransomware sono tra i virus informatici più pericolosi e insidiosi che agiscono entrando nel computer della vittima e sequestrando i dati dell'utente, rendendoli inservibili se non dietro il pagamento di un riscatto che in certi casi può raggiungere anche cifre elevatissime: infatti secondo quanto riportato dal rapporto Sophos "State of Ransomware 2022", un'indagine indipendente condotta su 5.600 responsabili IT di 31 Paesi, in Italia il riscatto medio è di 709.746 dollari. Ma ora il nuovo software anti-ransomware made in Italy sviluppato dai ricercatori dall'Università di Bologna e di Arpae Emilia-Romagna potrebbe segnare una svolta, fornendo agli utenti un'efficace arma per contrastare un fenomeno che secondo le stime nel 2021 ha fruttato ai cybercriminali oltre 20 miliardi di dollari in tutto il mondo, a cui si sommano costi sommersi incalcolabili che utenti e imprese devono sostenere, dovuti ai disservizi causati dall'attacco e ad apparati informatici resi inservibili, nonché gli adempimenti legati al GDPR, comprese le notifiche di data breach da effettuare al Garante della Privacy, che in certi casi può anche infliggere anche pesanti sanzioni ai titolari che non sono in grado di dimostrare aver attuato tutte le misure tecniche ed organizzative necessarie per proteggere i dati.

- N5) Sicurezza: La rettifica del regolamento macchine: le nuove date di applicazione

La nascita di questo regolamento, che, rispetto alla direttiva macchine 2006/42/CE, ha un diverso impatto sulle normative nazionali (è un atto legislativo vincolante che deve essere applicato in modo uniforme nell'intera Unione europea), è tuttavia un po' "travagliata".

Dopo il Regolamento è stata pubblicata una rettifica che cambia, ad esempio, buona parte delle date di applicazione e che effettivamente, pur tratte dal Regolamento, apparivano, in qualche caso, inusuali tenendo conto dell'entrata in vigore dell'intero Regolamento.

Ci soffermiamo oggi sulla Rettifica del Regolamento, sulle date di entrata in vigore e di applicazione, rivedute e corrette, ricordando anche **i primi articoli che possono applicarsi dal 19 luglio 2023 (e non più dal 13 luglio 2023).**

Nella Gazzetta Ufficiale (GUUE) 169/35 del 4 luglio 2023 è stata dunque pubblicata la Rettifica del regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio, del 14 giugno 2023, relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio.

Riprendiamo tutte le varie modifiche apportate al Regolamento:

1. Pagina 17, articolo 6, paragrafo 9: anziché: «14 luglio 2025», leggasi: «20 luglio 2025».
2. Pagina 17, articolo 6, paragrafo 10, quarto comma: anziché: «14 luglio 2024», leggasi: «20 luglio 2024».
3. **Pagina 36, articolo 47, paragrafo 2: anziché: «13 luglio 2023», leggasi: «19 luglio 2023».**
4. Pagina 38, articolo 50, paragrafo 2: anziché: «14 ottobre 2026», leggasi: «20 ottobre 2026».
5. Pagina 38, articolo 51, paragrafo 2, primo comma: anziché: «14 gennaio 2027», leggasi: «20 gennaio 2027».
6. Pagina 38, articolo 52, paragrafo 1, prima frase: anziché: «14 gennaio 2027», leggasi: «20 gennaio 2027».
7. **Pagina 38, articolo 52, paragrafo 1, seconda frase: anziché: «13 luglio 2023», leggasi: «19 luglio 2023».**
8. Pagina 38, articolo 53, paragrafo 1: anziché: «14 luglio 2028», leggasi: «20 luglio 2028».
9. Pagina 38, articolo 53, paragrafo 3, primo comma: anziché: «14 luglio 2026», leggasi: «20 luglio 2026».
10. Pagina 39, articolo 54, secondo paragrafo: anziché: «14 gennaio 2027», leggasi: «20 gennaio 2027».
11. Articolo 54, terzo paragrafo, lettera a): anziché: «14 gennaio 2024», leggasi: «20 gennaio 2024».
12. Articolo 54, terzo paragrafo, lettera b): anziché: «14 ottobre 2023», leggasi: «20 Ottobre 2026».
13. **Articolo 54, terzo paragrafo, lettera c): anziché: «13 luglio 2023», leggasi: «19 luglio 2023».**
14. Articolo 54, terzo paragrafo, lettera d): anziché: «14 luglio 2024», leggasi: «20 luglio 2024**».**

- N6) Sicurezza: La legge n. 85/2023 ha convertito il Decreto-Legge 48 (Decreto lavoro) del governo in materia di lavoro che all'articolo 14 modifica il D.Lgs. n. 81/2008

Si è concluso l'iter del Decreto-Legge 4 maggio 2023, n. 48 (il cosiddetto DL Lavoro) ed è stata pubblicata la Legge 3 luglio 2023, n. 85 "Conversione in legge, con modificazioni, del decreto-legge 4 maggio 2023, n. 48, recante misure urgenti per l'inclusione sociale e l'accesso al mondo del lavoro".

La Legge 85/2023 è stata pubblicata sulla Gazzetta ufficiale Serie Generale n. 153 del 3 luglio 2023, **ed è in vigore dal 4 luglio 2023.**

Riportiamo qui di seguito tutti gli articoli modificati:

1.1. **Nomina del medico competente e valutazione dei rischi**

1.2. Gli obblighi a carico delle amministrazioni tenute alla fornitura e alla manutenzione degli edifici scolastici statali

1.3 Nuovo obbligo per i componenti dell'impresa familiare di cui all'articolo 230-bis del Codice civile e i lavoratori autonomi

1.4. **Nuovi obblighi e facoltà del Medico Competente**

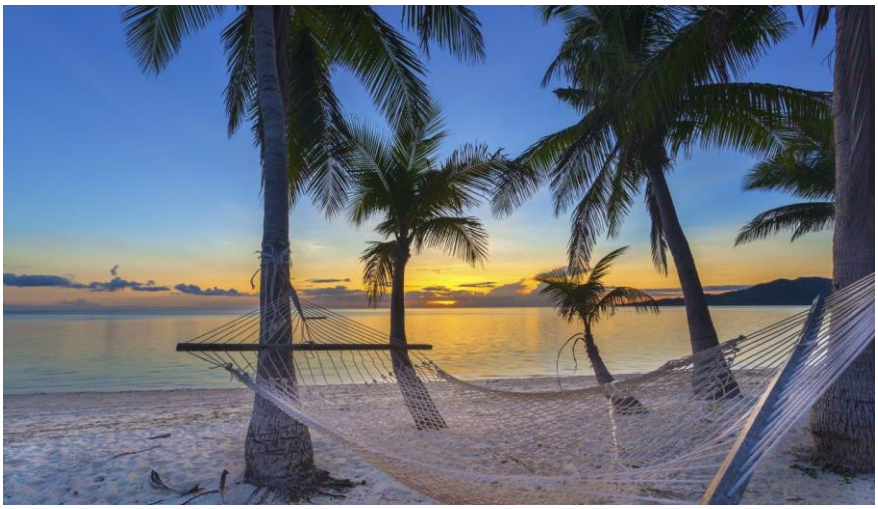
1.5. **Monitoraggio sulla formazione: contrasto ai falsi attestati**

1.6. Soggetti privati abilitati alle verifiche periodiche quali incaricati di pubblico servizio

1.7. **Obblighi dei noleggiatori e dei concedenti in uso**

1.8. **Uso di attrezzature da parte del datore di lavoro: obbligo di formazione ed addestramento**

1.9 Riconoscimento ulteriori titoli per svolgere la funzione di CSP e CSE



La chiusura dello Studio Violi è prevista da lunedì 31 luglio a venerdì 25 agosto compresi.

Per urgenze contattare l'ing. Violi al 338/6132605 o givioli@gmail.com
da lunedì 31 luglio a venerdì 4 agosto e da lunedì 21 a venerdì 25 agosto

Buone ferie di agosto a tutti

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