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

2003-2025
anni di consulenza per le imprese

ISO 9001
BUREAU VERITAS
Certification
IT334467

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 Qualità, Ambiente, Sicurezza, Etica; servizi di consulenza in ambito Privacy, Modelli Organizzativi, Sicurezza sul lavoro, Consulenza di Direzione e sostenibilità ESG

2025 Febbraio **Il nostro punto di vista su…** *Anno 18 – 1° sem*

Periodico di informazione per i CLIENTI dello STUDIO VIOLI

Indice delle NOTIZIE (N)

SENTENZE DI CASSAZIONE SUL LAVORO

- Sul sito http://www.dottrinalavoro.it/argomento/giurisprudenza-c/corte-di-cassazione-c sono presenti le ultime sentenze di Cassazione relative al lavoro

AFORISMA DEL MESE

"Guardate nel profondo della natura, e allora capirete meglio ogni cosa"

Albert Einstein (fisico)

“Punto di raccolta presso la centrale termica. Sarà davvero sicuro?”

Foto: ing. Sant’Unione, Modena

Notizie

- N1) Sicurezza: Infortuni sul lavoro, decessi in aumento: 96 morti in Emilia Romagna nel 2024

Il settore che nel 2024 ha registrato il numero maggiore di morti sul lavoro è quello del trasporto e magazzinaggio

In base agli ultimi dati Inail, l'Osservatorio permanente sugli infortuni e sulle malattie professionali in Emilia Romagna costituito dalla Cgil Emilia Romagna, ha fornito un quadro completo dell'andamento infortunistico nel 2024 nella nostra regione. Nel 2024 in Emilia-Romagna si sono registrati: 75.868 infortuni denunciati (-1,1% rispetto ai 76.687 del 2023); 96 denunce di infortunio con esito mortale (+5,5% rispetto alle 91 del 2023), di cui 12 morti a Modena; 7.543 malattie professionali denunciate (+15,8% rispetto alle 6.516 del 2023). I settori che nel 2024 hanno registrato il numero maggiore di morti sul lavoro in Emilia-Romagna sono: trasporto e magazzinaggio (23 infortuni mortali denunciati); agricoltura (15); costruzioni (11); noleggio, agenzie di viaggio, servizi di supporto alle imprese (5); fabbricazione di macchinari e apparecchiature (4); commercio e riparazione (3); metallurgia (3); industrie alimentari (3); servizi di alloggio e ristorazione (3); sanità e assistenza sociale (3).
A livello nazionale, parliamo di 589.571 infortuni di cui 1.090 infortuni mortali nel 2024. Questo vuol dire che ogni giorno in Italia si verificano 3 morti sul lavoro e 1.610 infortuni. In cinque anni, dal 2020 al 2024, in Emilia-Romagna hanno perso la vita sul lavoro 576 lavoratrici e lavoratori: 69 nell'agricoltura, 90 nell'edilizia e 117 nel trasporto e magazzinaggio.
Nel 2024 crescono in Emilia-Romagna gli infortuni mortali delle lavoratrici donne (11, +57,1% rispetto al 2023), dei lavoratori nati all'estero (23, +21,1% rispetto al 2023) e dei lavoratori over 65 anni (15, +50% rispetto al 2023). Come dimostrato dai dati nazionali relativi al periodo 2002-2022, il 55,8% degli infortuni mortali riguarda lavoratrici e lavoratori con contratti non standard, il 54,7% si verifica in aziende con meno di 10 addetti. Esattamente come 60 anni fa, il 33% degli infortuni mortali è causato da cadute dall'alto, il 15,7% dallo schiacciamento dovuto alla caduta di oggetti.

'Negli ultimi anni – commenta il segretario generale della Cgil Emilia Romagna Massimo Bussandri - si sono moltiplicate vere e proprie stragi del lavoro: Brandizzo, Esselunga di Firenze, Suviana, Casteldaccia di Palermo, Toyota di Bologna, Eni di Calenzano, Ercolano. Fa impressione constatare come protagoniste siano spesso e volentieri grandi imprese e aziende partecipate dallo Stato. È inaccettabile che 3 lavoratrici e lavoratori al giorno in Italia siano vittime dell'esasperazione del profitto, del disinteresse per i diritti e la sicurezza di chi lavora. In un paese civile questa sarebbe la priorità di qualsiasi Governo: mettere in sicurezza i luoghi di lavoro, aumentare i controlli e sanzionare con durezza chi non rispetta le regole, sostenere il ruolo e il lavoro fondamentale dei rappresentanti dei lavoratori per la sicurezza, investire in formazione. Queste dovrebbero essere le priorità del Governo, che invece – seguendo la retorica del "non disturbare chi produce" – appare assente e disinteressato'.

Denunce di infortunio e di infortunio mortale a livello provinciale

Provincia	Infortuni denunciati 2024	Infortuni denunciati 2023	Variazione % infortuni denunciati (2024-2023)	Denunce di infortunio mortale 2024	Denunce di infortunio mortale 2023	Variazione infortuni mortali (2024-2023)
Bologna	16.546	16.472	+0,4%	24	15	+9
Ferrara	4.170	4.291	-2,8%	9	7	+2
Forlì-Cesena	6.822	6.845	-0,3%	8	13	-5
Modena	14.623	14.736	-0,8%	12	15	-3
Parma	7.732	8.416	-8,1%	10	12	-2
Piacenza	4.465	4.467	+0%	8	8	0
Ravenna	7.017	6.871	+2,1%	8	11	-3
Reggio Emilia	9.292	9.536	-2,6%	8	7	+1
Rimini	5.201	5.053	+2,9%	9	3	+6
Totale ER	75.868	76.687	-1,1%	96	91	+5
Totale Italia	589.571	585.356	+0,7%	1.090	1.041	+49

- N2) Sicurezza: Nota 656 del 23 gennaio 2025 - l'Ispettorato Nazionale del Lavoro chiarisce le novità sul tesserino di riconoscimento

Cosa cambia? La nuova normativa abroga l'art. 36-bis del D.L. 223/2006, ma conferma l'obbligo del tesserino di riconoscimento ai sensi del D.Lgs. 81/2008, semplificando la disciplina ed evitando duplicazioni legislative.

La reiterazione della violazione determina la possibilità di sospensione dell'attività fino alla regolarizzazione.

L'INL ribadisce l'importanza di garantire la tracciabilità dei lavoratori nei contesti di appalto e subappalto, rafforzando la sicurezza e la trasparenza nei luoghi di lavoro.

1 Ambito di applicazione

Con la Nota prot. 656 del 23 gennaio 2025 l'Ispettorato Nazionale del Lavoro chiarisce le novità sul tesserino di riconoscimento per i lavoratori introdotte con la pubblicazione della Legge 17 dicembre 2024, n. 203.
La normativa sul tesserino di riconoscimento riguarda le attività svolte in regime di appalto o subappalto, inclusi i cantieri temporanei e mobili. Le disposizioni si applicano a:

1. lavoratori subordinati impiegati da imprese appaltatrici e subappaltatrici;
2. lavoratori autonomi che operano in tali contesti;
3. componenti di imprese familiari, artigiani, piccoli commercianti e coltivatori diretti quando prestano attività in luoghi soggetti ad appalto o subappalto.

I riferimenti normativi principali sono:

- Art. 26, comma 8, del D.Lgs. 81/2008: obbligo per i datori di lavoro di dotare il personale della tessera di riconoscimento.
- Art. 20, comma 3, del D.Lgs. 81/2008: obbligo per i lavoratori di esporre la tessera.
- Art. 21, comma 1, lett. c, del D.Lgs. 81/2008: obbligo per lavoratori autonomi e altre categorie di munirsi della tessera.

2. Modifiche e abrogazioni introdotte

La Legge 17 dicembre 2024, n. 203 ha modificato l'art. 304, comma 1, lett. b) del D.Lgs. 81/2008, abrogando i commi 3, 4 e 5 dell'art. 36-bis del D.L. 223/2006 (convertito con modifiche dalla L. 248/2006).
Le disposizioni abrogate prevedevano:

- L'obbligo, per il datore di lavoro, di fornire ai lavoratori un tesserino di riconoscimento.
- L'obbligo, per i lavoratori, di esporlo nei cantieri edili.

L'abrogazione è stata giustificata dal fatto che tali obblighi sono già previsti e regolamentati dal D.Lgs. 81/2008.

3. Cosa cambia in pratica

L'obbligo di dotare i lavoratori di un tesserino di riconoscimento rimane, ma viene ricondotto esclusivamente alle norme del D.Lgs. 81/2008, eliminando i riferimenti alla normativa previgente.
Viene semplificata la disciplina, evitando duplicazioni normative tra il D.L. 223/2006 e il Testo Unico sulla Sicurezza.
L'obbligo si estende non solo ai cantieri, ma a tutte le attività in appalto o subappalto, garantendo un'applicazione più uniforme.

4 Regime sanzionatorio previsto in caso di inadempienza

Le sanzioni per la mancata osservanza degli obblighi relativi al tesserino di riconoscimento sono disciplinate dal D.Lgs. 81/2008:

- Datore di lavoro che non fornisce il tesserino ai propri lavoratori:
  Sanzione amministrativa pecuniaria da €2.500 a €10.000, ai sensi dell'art. 55, comma 5, lett. i), del D.Lgs. 81/2008.
- Lavoratore che non espone la tessera:
  Sanzione amministrativa pecuniaria da €50 a €300, ai sensi dell'art. 59, comma 1, lett. b), del D.Lgs. 81/2008.
- Lavoratore autonomo che non si munisce del tesserino:
  Sanzione amministrativa pecuniaria da €300 a €1.200, ai sensi dell'art. 60, comma 1, lett. b), del D.Lgs. 81/2008.
- Lavoratore autonomo che non espone il tesserino:
  Sanzione amministrativa pecuniaria da €100 a €600, ai sensi dell'art. 60, comma 2, del D.Lgs. 81/2008.

Inoltre, nel caso di reiterata inadempienza, l'INL può disporre la sospensione dell'attività lavorativa fino alla regolarizzazione dell'obbligo.
L'abrogazione dell'art. 36-bis del D.L. 223/2006 semplifica la normativa, mantenendo inalterati gli obblighi per datori di lavoro e lavoratori ma riconducendoli esclusivamente al D.Lgs. 81/2008. La mancata conformità è sanzionata in maniera chiara e dettagliata, confermando la necessità di un rigoroso rispetto delle disposizioni in materia di sicurezza sul lavoro.

- N3) Sicurezza: Polizza anti calamità, una tassa in più sulle aziende

Il L'obbligo scatta l'1 aprile ma, contrariamente a quello che si potrebbe pensare, non è uno scherzo.

Stiamo parlando ovviamente della necessità **per tutte le imprese di assicurarsi contro i rischi catastrofali**.
Un adempimento che interessa quattro milioni di imprenditori, i quali hanno a disposizione poco più di un mese per informarsi, trovare una compagnia assicuratrice che garantisca il miglior rapporto costi/benefici, scegliere il tipo di polizza più adatta alle proprie esigenze, stipulare il contratto di assicurazione. Un percorso a ostacoli perché i tempi stretti si sommano a una impreparazione delle agenzie assicurative e alla mancanza di disposizioni attuative di dettaglio che non sono ancora state deliberate dagli organismi ministeriali competenti (i quali, evidentemente, hanno un senso del tempo diverso da quello dei comuni mortali).
Regolamenti che sono importanti anche perché dovrebbero gestire i diversi livelli di rischio presenti sul territorio nazionale anche per rendere più omogenee e gestibili le politiche di prezzo praticabili dagli assicuratori.
Inoltre, come ha sottolineato la Cna, manca ancora il portale a cura dell'Ivass per confrontare le varie offerte e consentire così alle imprese di essere nelle condizioni di sottoscrivere polizze efficaci nella piena consapevolezza. Quindi non proprio dei dettagli.
Il costo delle polizze, che andrebbero a coprire i rischi legati a terremoti, frane, esondazioni o alluvioni, parte da poche centinaia di euro, per le imprese di minori dimensioni, e arriva a qualche migliaia di euro per quelle di medie dimensioni, per aumentare ancora, ovviamente, per le grandi imprese. Comunque, per rendere meno gravoso l'adempimento, lo Stato ha stanziato 5 miliardi di euro per permettere alle compagnie di assicurazione di riassicurarsi con Sace coprendo fino al 50% del rischio.

Per chi non si assicura c'è il rischio di perdere contributi, sovvenzioni, agevolazioni pubbliche e naturalmente risarcimenti, nel caso in cui l'evento calamitoso dovesse realmente verificarsi.
In pratica l'impresa dovrà pagarsi i danni di tasca propria senza più l'aiuto dello Stato. Possibile anche un peggioramento delle condizioni di credito perché le banche si troverebbero davanti ad aziende con un tasso di rischio maggiorato.
Qualcuno ha parlato di questo nuovo obbligo come di una tassa aggiuntiva a carico delle imprese: se questo può essere vero da un punto di vista finanziario, da un punto di vista più generale è forse più opportuno parlare di uno Stato che sceglie di ritirare una garanzia offerta agli imprenditori in caso di eventi calamitosi e chiede loro di farsene carico in proprio con una normale copertura assicurativa. Anche in considerazione del fatto che il risarcimento offerto dallo Stato è più teorico che reale, nel senso che normalmente arriva con ritardi enormi, quando le imprese coinvolte spesso hanno cessato di esistere. La speranza è che il trasferimento del rischio sulle assicurazioni private renda almeno più veloci e più congrui i risarcimenti offerti ai chi dovesse subire i danni provocati da eventi che sono sì naturali, ma spesso aggravati anche dall'incuria umana.

-N4) Privacy: Pubblicato il piano delle attività ispettive del Garante Privacy per il primo semestre 2025

Il nuovo piano ispettivo per il primo semestre 2025 pubblicato dal Garante https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10100360 presenta vari motivi di interesse.

Oltre a quello generale di richiamare l'attenzione di tutti i titolari del trattamento (e di tutti gli altri attori dell'ecosistema privacy, a partire dai responsabili del trattamento) su quelli che sono i temi su cui il Garante ha ritenuto di porre l'attenzione (un piano di audit fra le sue determinanti ha l'analisi del rischio, fra cui, in ambito privacy, la triade data breach – reclami – segnalazioni) in questa occasione se ne coglie uno in particolare: **la sicurezza e l'utilizzo delle banche dati.**

Infatti, la tematica delle banche dati appare in tre degli ambiti di indagine selezionati e con riguardo a tre diverse dimensioni:

1. verifica dei sistemi di sicurezza e profili di accessibilità delle banche dati stesse, mediante accertamenti relativi ai data breach che hanno coinvolto banche dati pubbliche di particolare rilievo e sensibilità;

2. misure adottate per rilevare tempestivamente e/o prevenire le violazioni di sicurezza e connesso assolvimento dell'obbligo di segnalazione delle violazioni, con riguardo alle banche dati degli istituti di credito;

3. utilizzo illegittimo di indirizzari e banche dati, con riguardo trattamento di dati effettuato da imprese che gestiscono call center e servizi di email marketing

Tale focus rafforza l'attenzione delle Autorità di settore alla questione della sicurezza dei dati, questione impostasi al dibattito per vari motivi fra cui:
a) la progressiva definizione del quadro normativo UE (ad es. NIS2, DORA) che spinge ad un rafforzamento della sicurezza IT;
b) episodi anche preoccupanti di violazione di base dati in ambito pubblico e privato;
c**) la necessità di comprendere come la protezione delle informazioni sensibili** non sia solo un obbligo normativo, ma anche un fattore cruciale per la fiducia degli utenti e la reputazione delle organizzazioni.

In argomento va ricordato anche l'input **dell'Agenzia per la Cybersicurezza Nazionale (ACN)** rappresentato dalle Linee Guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio, che rappresenta un riferimento base delle misure per contrastare accessi abusivi e minacce, sia interne che esterne, soffermandosi su alcuni step centrali:

1) **Controllo degli accessi**
2) **Applicazioni di principi e buone pratiche di sviluppo sicuro dei sistemi e delle applicazioni**
3) **Gestione del ciclo di vita dei sistemi e delle applicazioni**
4) **Gestione rischi e sicurezza della catena di approvvigionamento**
5) **Monitoraggio e auditing**
6) **Formazione del personale.**

Tale documento, corredato da un elenco di misure di sicurezza, pur nella sua semplicità (ed è un merito e non una critica), costituisce, per ogni manager, una lettura minima essenziale per la consapevolezza dei rischi e l'interazione con le funzioni tecniche.

Alla luce di questi elementi, il piano ispettivo del Garante per il primo semestre 2025 si configura come un'iniziativa strategica per garantire un livello più elevato di protezione dei dati personali.

Ma la pubblicazione del Piano ispettivo oltre a incrementare la trasparenza sull'attività del Garante ha in concreto anche valore pedagogico incentivando - in un'ottica subliminale, nudging - la conformità alle normative vigenti e la diffusione di buone pratiche in ambito di sicurezza informatica.

Questo approccio riflette l'importanza crescente della sicurezza delle banche dati nell'ambiente digitale contemporaneo.

Nel rimandare per una più compiuta analisi alla lettura del citato Piano, si evidenzia che gli altri ambiti individuati dal Garante sono:

- progetti del Programma Statistico Nazionale che prevedano l'utilizzo di big data e dati sintetici;
- attivazione di contratti non richiesti nel settore energetico;
- utilizzo di dati biometrici per gli esami della patente di guida presso la Motorizzazione civile;
- **cookie di profilazione**;
- trattamenti dati delle società che gestiscono, i gestori dell'identità digitale (SPID) e sulla filiera dei soggetti di cui essi si avvalgono per il rilascio di servizi fiduciari (SPID e firma digitale);
- **le scuole con riguardo ai registri elettronici**;
- l'osservanza delle disposizioni in materia di protezione dei dati personali, ivi incluse le istruttorie relative a reclami e segnalazioni formali proposti all'Autorità ed in istruttoria presso i relativi Dipartimenti e Servizi.

Infine, come rammentato nel Piano semestrale, per l'attività ispettiva il Garante può avvalersi della Guardia di Finanza.

- N5) Privacy: Aumentati del 197% gli attacchi hacker veicolati tramite email, e il 31% dei messaggi ricevuti è spam; Inoltrare gli screenshot delle chat WhatsApp è una pessima abitudine e può violare la privacy

Aumentati del 197% gli attacchi hacker veicolati tramite email, e il 31% dei messaggi ricevuti è spam. L'ultimo rapporto sulle minacce informatiche pubblicato da Acronis per il secondo semestre del 2024 evidenzia un netto incremento degli attacchi malware e ransomware, con una particolare attenzione ai rischi legati all'intelligenza artificiale.

Il report offre un'analisi dettagliata delle minacce più recenti e alcuni suggerimenti pratici per aiutarti a proteggere le proprie organizzazioni. Tra le conclusioni che tira il report:

- si registra un incremento del 5% degli attacchi ransomware, che hanno colpito soprattutto i settori critici dei trasporti, della sanità e manifatturiero;
- gli attacchi basati su e-mail crescono quasi triplicati, un dato che sottolinea l'esigenza di soluzioni di sicurezza avanzate per le e-mail.
- i cyber criminali utilizzano sistemi di intelligenza artificiale generativa come ChatGPT per creare malware sofisticati e avviare campagne di spear-phishing avanzate.

Tra luglio e dicembre dello scorso anno, il numero di attacchi veicolati tramite email è infatti aumentato del 197% rispetto allo stesso periodo dell'anno precedente, mentre il 50% degli utenti ha subito almeno un tentativo di attacco basato su email malevole.

Il phishing resta la modalità d'attacco più diffusa (74%), seguita dal social engineering (22%) - in crescita del 7% rispetto all'anno precedente - e dai malware (3%). Per numero di attacchi, nel 2024 l'Italia è al quinto posto fra i Paesi più colpiti.

I settori più colpiti dalla violazione dei dati sono quello finanziario e quello sanitario. In questo secondo caso, l'attacco informatico è anche il più costoso, con quasi 10 milioni di euro per attacco. È il 13esimo anno consecutivo che viene classificato come il settore più costoso in caso di violazione dei dati.

Un altro elemento rilevato riguarda i Managed Service Provider (MSP), i fornitori esterni di servizi gestiti, che stanno diventando obiettivi privilegiati per gli hacker. Il phishing è stato il metodo d'attacco più diffuso, colpendo il 33% degli MSP, seguito dagli exploit che sfruttano vulnerabilità nei protocolli di accesso remoto e i dispositivi non aggiornati.

Fra i motivi per cui l'uso di sistemi di accesso remoto accresce il rischio, secondo Acronis ci sono l'aumento della superficie di attacco e richiede misure di sicurezza proattive per ridurre i rischi.

Nell'ultimo anno il ransomware si è evoluto, con gruppi di cybercriminali che adottano tattiche di spionaggio avanzato, come l'uso di credenziali rubate e attacchi alla supply chain, per infiltrarsi nei sistemi degli MSP e poi propagarsi ai clienti.

Il rapporto segnala che nel quarto trimestre del 2024 Acronis ha bloccato oltre 48 milioni di URL dannosi, un aumento del 7% rispetto allo stesso periodo dell'anno precedente.

Inoltre, il 31,4% di tutte le email analizzate risultava spam, con l'1,4% contenente malware o link di phishing.

Sul fronte dei ransomware, nel quarto trimestre del 2024 sono stati registrati 1.712 attacchi con 580 vittime, tra cui quelle causate dai gruppi RansomHub, Akira, Play e KillSec. I tre settori più colpiti dai ransomware sono stati quelli di trasporti, sanità e produzione.

Il rapporto individua l'Italia tra i paesi più colpiti dagli attacchi malware di dicembre 2024, insieme a Emirati Arabi Uniti e Singapore, mettendo in mette in luce il fatto che "l'Italia è un obiettivo importante, ma anche che le difese devono aumentare", ha commentato Denis Cassinerio, general manager dell'area meridionale della zona Emea di Acronis.

"L'errore umano resta l'anello debole della sicurezza" - ha evidenziato invece Irina Artioli, Cyber Protection Evangelist della Threat Research Unit di Acronis, durante la presentazione del rapporto – "Anche un hacker con poche competenze può creare un malware grazie agli strumenti di intelligenza artificiale". Per esempio, essa viene usata per creare ransomware "in poche ore" e per configurare complesse operazioni di phishing in meno tempo.

Inoltrare gli screenshot delle chat WhatsApp è una pessima abitudine e può violare la privacy. Come anche gli utenti meno esperti sanno, scattare un'istantanea di ciò che appare sul display del proprio cellulare è un gioco da ragazzi, e anche inoltrare tali schermate ad altri è talmente facile che la mania di condividere con altri gli screenshot delle chat di WhatsApp o altre app di messaggistica ha contagiato praticamente tutti.

Se a mostrare certi contenuti privi di dati personali altrui non c'è assolutamente niente di male in sé, e ognuno è libero di inoltrare ad altri tutto ciò che lo riguarda personalmente, il problema si pone invece quando nelle conversazioni o nelle immagini che si condividono è coinvolto qualcun altro che non è al corrente di tale divulgazione di informazioni che magari ci ha fornito ritenendo implicitamente che rimanessero riservate e confidenziali tra lui e noi, e la questione si complica ulteriormente se nel contenuto vi sono dati di natura sensibile, riguardanti abitudini sessuali, dati sulla salute, opinioni politiche, e ogni altra faccenda che dovrebbe rimanere privata tra le due persone che si scambiano la corrispondenza telematica.

Se siete tra coloro che hanno l'abitudine di fare screenshot e inoltrarli ad altri, è bene quindi mettere in conto che c'è il rischio di commettere degli errori, infatti uno studio di Federprivacy ha evidenziato che un utente su quattro (24%) che inoltra contenuti tramite

WhatsApp sbaglia destinatario. Ma c'è anche il pericolo di incappare in conseguenze di natura legale per violazioni della privacy e di altre normative applicabili alla incauta gestione dei dati personali.

Occorre infatti premettere che le chat sono considerate a tutti gli effetti uno scambio di corrispondenza, e l'inoltro di un messaggio o di una email privata di cui non si era i destinatari costituisce reato di rivelazione di contenuti privati, punito dall'articolo 616 del Codice Penale. Commette questo reato, ad esempio, chi prende visione dei messaggi, delle chat su Whatsapp o della posta elettronica di amici, colleghi, coniugi, etc. e li trasmette, mediante screenshot o analoghe forme di inoltro, ad altre persone ad insaputa dei diretti interessati.

Infatti, il fatto che si sia legittimati a visionare dei contenuti ricevuti lecitamente da qualcuno, non ci rende legittimati anche a poterli condividere poi ulteriormente con terzi senza che il mittente originario ci abbiamo espressamente autorizzato.

Nel caso in cui i messaggi inoltrati a terzi contenessero dati sensibili del mittente, la loro condivisione violerebbe l'articolo 617 septies del Codice Penale, che punisce con la reclusione fino a quattro anni qualsiasi persona che, "al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di incontri privati o registrazioni, pur esse fraudolente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione".

Se poi il messaggio che viene riprodotto con screenshot e così viene diffuso ad altri proviene da un medico o uno psicologo, oppure da un altro professionista tenuto al segreto professionale, la violazione della privacy e agli eventuali danni che ne sono conseguiti è punibile con la reclusione fino a un anno ai sensi dell'articolo 622 del Codice Penale.

Si pensi a chi, ad esempio, fa uno screenshot di un messaggio con cui venisse comunicato in modo superficiale a persone diverse dall'interessato l'esito delle analisi cliniche, e la relativa diagnosi di patologia con conseguente terapia, magari per il solo fatto che appartengono al nucleo familiare, ma in assenza di una valida delega.

Se lo screenshot di una chat o di un qualsiasi altro tipo di conversazione privata viene invece diffuso con intenti lesivi della reputazione di qualcuno, sussiste il reato di diffamazione, che può essere aggravata dall'uso della stampa o di altro mezzo di pubblicità: la giurisprudenza considera tale anche la diffusione avvenuta sul web e attraverso i sistemi di messaggistica.

Allo stesso modo, se il contenuto della conversazione riprodotta con gli screenshot viene alterato in modo da cambiarne il significato, si pensi a chi, manipolando la foto o la schermata riprodotta, taglia parti essenziali del discorso e omette di riportare alcune frasi determinanti per la comprensione della conversazione, sussiste l'intento diffamatorio e dunque il reato.

Per prevenire gravi e spiacevoli conseguenze legali, prima di inoltrare uno screenshot di una chat o di un'altra conversazione privata è quindi opportuno resistere alla pessima abitudine spesso compulsiva di condividerlo subito con qualcun altro, prendendosi invece il tempo per assicurarsi che il contenuto non sia riservato, verificare che lo screenshot riprodotto non contenga dati personali e sensibili, accertarsi che quanto diffuso non sia protetto da copyright o altre forme di protezione dei diritti d'autore o da privative aziendali, o tutelato dal segreto professionale, e soprattutto ottenere il preventivo consenso del mittente alla divulgazione del messaggio che c'è stato inviato.

- N6) Ambiente: Proroga RENTRI - Convertito il D.L. Milleproroghe

E' in vigore dal 25 febbraio la Legge 21 febbraio 2025 , n. 15 di conversione del decreto-legge 27 dicembre 2024, n. 202 (c.d. Milleproroghe), recante disposizioni urgenti in materia di termini normativi, pubblicata sulla Gazzetta Ufficiale del 24 febbraio 2025.

La legge prevede un'importante **proroga per l'operatività del RENTRI**, nello specifico dispone che:

"2 -bis. Ai fini dell'operatività del Registro elettronico nazionale per la tracciabilità dei rifiuti, di cui all'articolo 188 -bis del decreto legislativo 3 aprile 2006, n. 152, con decreto del Ministro dell'ambiente e della sicurezza energetica, da adottare entro trenta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, il termine di sessanta giorni previsto dall'articolo 13, comma 1, lettera a) , del regolamento di cui al decreto del Ministro dell'ambiente e della sicurezza energetica 4 aprile 2023, n. 59, è aumentato a centoventi giorni".

Ciò cosa comporta? Attenzione!

1. Uno spostamento del **termine di chiusura delle iscrizioni dal 13 febbraio al 14 aprile ma solo se e quando verrà adottato il previsto DM**;

2. E, di conseguenza, **verrebbe spostata anche l'entrata in vigore dei nuovi modelli di Registri di carico e scarico e di FIR** [che, si ricorda, già dal 13 febbraio centinaia di migliaia di operatori stanno usando!] e l'abrogazione dei vecchi.

Tale proroga, quindi, non è immediata, poiché entro il 27 marzo ["entro 30 giorni dalla data di entrata in vigore della legge di conversione"] il MASE dovrebbe adottare un DM per prorogare "ex post" il termine del 13 febbraio fino al 14 aprile 2025 [120 giorni dal termine del 15 dicembre 2024].
Ciò costringerebbe tutti gli operatori a tornare ai modelli cartacei di FIR e Registri C/S del 1998, ma solo fino al 14 aprile (per soli 14 giorni) per poi ripartire il 15 aprile con i nuovi modelli in vigore già dal 13 febbraio scorso.

Con la conversione in Legge del "milleproroghe" nessuna scadenza RENTRI viene dunque posticipata "di default" e **pertanto ad oggi i soggetti obbligati che ancora non si sono iscritti al RENTRI rimangono esposti alle relative sanzioni di cui all'. art. 258, commi 10 e 11, del D.L.vo 152/2006 e bisogna continuare ad utilizzare i nuovi modelli di FIR e registro**.

Si prospetta, dunque, uno scenario veramente problematico e confuso per tutti gli operatori del settore.

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