

XRI INSURANCE WEBZINE

Notizie ed Approfondimenti sul Mondo Assicurativo

settembre – 2026



Giurisprudenza

Responsabilità medica: la CTU può fondare da sola la prova del nesso causale

Con la sentenza n. 449/2026 il Tribunale di Isernia è tornato a pronunciarsi sul valore probatorio della consulenza tecnica nel contenzioso sanitario, condannando in solido chirurgo e struttura al risarcimento di circa 900.000 euro per la tardiva diagnosi di una complicanza post-operatoria. Richiamando la Cass. SS.UU. n. 3086/2022, il giudice ha affermato che la CTU può da sola fondare il convincimento del giudice, purché il consulente non supplisca all'onere probatorio sui fatti principali. La relazione dell'ATP, anche se viziata, è stata ritenuta utilizzabile come prova atipica. Accolta, infine, la manleva del medico verso l'assicuratore, che non aveva provato la conoscenza del sinistro prima della stipula.

Data Breach nei Sistemi Informatici delle strutture sanitarie: il caso francese de l'Hopital Prive De La Loire

Il 3 settembre scorso la *Commission National de l'Informatique et des Libertés* (CNIL) – l'alter ego francese della nostra Autorità Garante per la Protezione dei Dati Personali – in forza di delibera assunta il 21 luglio 2026, ha inflitto una sanzione pecuniaria di 500.000 euro, oltre ad aver imposto una serie di misure correttive a l'*Hôpital Privé de la Loire* a seguito di un grave

Giurisprudenza

Trasporto aereo: foro competente per la perdita del bagaglio anche sui voli nazionali

La Corte di giustizia ha precisato che, ai sensi degli artt. 1 e 3, par. 1, del Regolamento (CE) n. 2027/97, l'art. 33, par. 1, della Convenzione di Montreal disciplina la competenza giurisdizionale anche nelle azioni risarcitorie per perdita del bagaglio relative a voli effettuati interamente all'interno di un medesimo Stato membro, promosse da un residente nei confronti di un vettore aereo dell'Unione avente sede nello stesso Stato. La Corte ha inoltre escluso che, nei contratti conclusi online, la residenza del passeggero possa essere equiparata al "luogo in cui il vettore possiede un'impresa che ha provveduto alla stipulazione del contratto". I criteri di collegamento previsti dall'art. 33, par. 1, richiedono infatti una presenza fisica del vettore o un nesso diretto con l'attività di trasporto, mentre il foro della residenza del passeggero è stato espressamente riservato dal par. 2 alle sole azioni per morte o lesioni personali. Secondo i giudici di Lussemburgo, un'interpretazione diversa determinerebbe un'eccessiva frammentazione del contenzioso a livello globale, alterando l'equilibrio tra gli interessi delle parti perseguito dalla Convenzione. La pronuncia chiarisce inoltre che, ai fini dell'individuazione del foro competente, rileva il contratto di trasporto del passeggero, anche quando il danno riguardi il bagaglio e il servizio ad esso relativo sia stato acquistato presso una diversa sede del vettore, trattandosi di una prestazione meramente accessoria. La decisione si pone in contrasto con l'orientamento della Corte di cassazione italiana richiamato dal giudice del rinvio, che aveva invece riconosciuto la competenza del foro di residenza del passeggero nei casi di acquisto del titolo di viaggio mediante piattaforme online.

data breach al database della struttura sanitaria avvenuto a fine giugno 2025, nell'ambito del quale erano stati coinvolti i dati personali (dati anagrafici, dati di contatto, dati amministrativi identificativi dei pazienti e, ovviamente, informazioni relative allo stato di salute) di più di 500 mila pazienti e di altri 200 mila e più circa di soggetti terzi identificati come "soggetti terzi fidati" (in gran parte familiari dei pazienti).

L' *Hôpital Privé de la Loire* è un ospedale del comune di Saint-Étienne appartenente al gruppo ospedaliero Ramsay Santé, leader europeo nell'ospedalizzazione privata e nelle cure primarie, attivo in Francia, Svezia, Norvegia, Danimarca e nord Italia.

Ebbene, la vicenda è un classico caso di scuola per i professionisti in materia di privacy e cybersecurity, se si osservano le criticità riscontrate dall'autorità francese sull'infrastruttura informatica dell'Ospedale, le cui lacune sul piano della sicurezza si sono rivelate un moltiplicatore di violazioni ai sensi del GDPR.

Giurisprudenza

Responsabilità solidale della società di sharing per il sinistro causato dal monopattino: perdita del bagaglio anche sui voli nazionali

Il Giudice di pace di Rimini ha accolto la domanda risarcitoria proposta dalla conducente di una bicicletta a pedalata assistita, urtata da un monopattino elettrico a noleggio durante una manovra di sorpasso su una pista ciclabile, condannando in solido il conducente e la società di sharing proprietaria del mezzo ex art. 2054 c.c. Premessa l'equiparazione dei monopattini elettrici ai velocipedi (art. 1, comma 75-quinquies, L. n. 160/2019) e la loro conseguente qualificazione come veicoli ai sensi degli artt. 46 e 47 C.d.S., il giudice ha attribuito l'esclusiva responsabilità del sinistro al conducente del monopattino, che, sulla base della CTU, aveva circolato sulla pista ciclabile in violazione dell'art. 190 C.d.S. e non aveva mantenuto un'adeguata distanza laterale ai sensi dell'art. 148, comma 3, C.d.S. Quanto alla società di noleggio, è stata ritenuta irrilevante l'eccezione di circolazione contro la sua volontà, in quanto sfornita di prova e incompatibile con l'oggetto stesso dell'attività, consistente nel mettere i mezzi a disposizione di terzi per la circolazione su strada. Sul piano del quantum, il danno morale è stato liquidato come frazione del danno biologico tabellare, oggetto di successiva personalizzazione, e le spese di assistenza stragiudiziale sono state riconosciute a titolo di danno emergente. La pronuncia si inserisce nel quadro dell'obbligo assicurativo RCA per i monopattini introdotto dalla L. n. 177/2024, e lascia aperta la questione della posizione del gestore del servizio non proprietario dei mezzi, come nei modelli in franchising.

Secondo quanto riportato i dati personali violati non sarebbero mai stati né venduti, né pubblicati, ma non è questo il punto.

La dinamica dell'incidente: un ecosistema informatico vulnerabile

L'intrusione informatica che ha consentito agli hacker di penetrare all'interno del *dossier patient informatisé* (DPI) della struttura – che centralizza i dati di tutti i pazienti - ed accedere a dati sanitari e altri dati personali di oltre 727.000 persone (di cui, nello specifico, 524.867 pazienti e 202.246 contatti fidati o familiari), è avvenuta sfruttando le credenziali dell'account di un medico. Il DPI era accessibile sia dal personale interno dell'Ospedale mediante collegamento alla VPN aziendale, sia da personale esterno ma - si legge nella delibera del CNIL - quest'ultimo senza preventiva connessione alla VPN, nonché dai dipendenti della software house sviluppatrice del DPI stesso, i quali godevano di una prerogativa di accesso permanente ed incontrollata per i servizi di manutenzione.

Le criticità riscontrate. Profili giuridici

La prima grave violazione contestata dal CNIL attiene alla non conformità delle misure di

Giurisprudenza

Responsabilità professionale dell'avvocato: la sconfitta in giudizio non prova l'inadempimento

Con l'ordinanza n. 21279/2026 la Cassazione torna sui criteri di accertamento della responsabilità professionale del difensore, escludendo che essa possa desumersi automaticamente dall'esito sfavorevole della lite o dalla prospettazione, a posteriori, di una strategia difensiva ritenuta più efficace. La vicenda nasce da un giudizio di opposizione a decreto ingiuntivo, promosso dagli acquirenti di un'azienda per il saldo del prezzo: il difensore rinunciava al mandato dopo la prima udienza e, rigettata l'opposizione, agiva per i compensi; i clienti eccepivano che la sconfitta fosse dipesa da una difesa impostata erroneamente, ma il giudice di merito escludeva ogni responsabilità. La Corte ha ribadito nell'ordinanza che chi lamenta l'errore del difensore deve dimostrare che la condotta alternativa avrebbe avuto una concreta e apprezzabile probabilità di condurre a un esito diverso, e che il semplice richiamo a iniziative difensive non intraprese non basta a fondare la domanda risarcitoria. La valutazione della strategia difensiva e delle possibilità di successo della lite resta riservata al giudice di merito e, se adeguatamente motivata, non è sindacabile in sede di legittimità.

arco temporale esiguo.

sicurezza implementate dall'Ospedale rispetto al disposto dell'**art. 32 del GDPR** sotto vari profili tecnico-organizzativi:

- la scarsa robustezza della procedura di autenticazione al DPI, sia perché accessibile come detto anche da medici esterni all'Ospedale (senza rete VPN), sia perché non vi era un sistema di autenticazione a più fattori;
- l'inadeguatezza delle policy di accesso al sistema e l'assenza di compartimentazione delle cartelle dei pazienti, tale per cui ciascun professionista sanitario o équipe poteva accedere indistintamente - anche a scapito del segreto professionale - a dossier relativi a pazienti diversi da quelli in cura;
- la mancanza di sistemi per il monitoraggio e tracciamento in tempo reale e di rilevamento di attività informatiche sospette con alert automatici che rilevassero anomalie del sistema, quali appunto l'accesso di un solo account, astrattamente attribuibile ad un solo medico, che massivamente interrogava centinaia di migliaia di cartelle cliniche in un

L'articolo 32, paragrafo 1, del GDPR prevede che, tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi, il titolare del trattamento e il responsabile del trattamento

Giurisprudenza

Notaio: nessuna responsabilità per il vincolo omissso nel rogito se l'acquirente ne era già a conoscenza

Se l'acquirente conosceva con certezza i vincoli gravanti sull'immobile, il notaio che non li abbia indicati nell'atto non risponde di alcuna responsabilità. Lo ha stabilito il Tribunale di Caltagirone in relazione a una compravendita in cui i beni erano stati descritti come liberi da pesi e vincoli, benché gravati da limitazioni che lo stesso contraente aveva in precedenza costituito. Il Tribunale ribadisce che la prestazione notarile non si esaurisce nell'accertamento della volontà delle parti e nella redazione dell'atto, ma comprende le attività necessarie a garantire la certezza degli effetti del negozio e il risultato pratico perseguito dalle parti. Salvo dispensa concorde, la verifica dei pubblici registri è un obbligo discendente dall'incarico, la cui violazione genera responsabilità contrattuale ex art. 1176, comma 2, c.c., letto alla luce della buona fede. Il notaio deve inoltre informare le parti di ogni circostanza idonea a incidere sugli effetti dell'atto e, ove conosca o sospetti iscrizioni pregiudizievoli, anche quando sia stato esonerato dalle visure. Tale obbligo non si estende però ai vincoli già noti con certezza al contraente: in questo caso l'omissione non lede la sua libertà di autodeterminazione negoziale, perché l'informazione era già in suo possesso, e difettano sia la violazione della diligenza qualificata sia il nesso causale con la stipula. Per il mancato accertamento di ipoteche o pignoramenti, il giudice richiama infine la possibilità di condanna al risarcimento per equivalente, commisurato ai costi di cancellazione, oppure in forma specifica, mediante cancellazione della formalità non rilevata.

mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e, in particolare, mezzi che garantiscano la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento, nonché una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

L'articolo 32, paragrafo 2, precisa che nella valutazione dell'adeguato livello di sicurezza si tiene conto in particolare dei rischi presentati dal trattamento, derivanti in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata dei dati personali trasmessi, conservati o comunque trattati, o dall'accesso non autorizzato a tali dati, accidentalmente o illecitamente.

Da tali disposizioni, lette alla luce dei Considerando 75-76-83 del GDPR e dell'articolo 2 L. 1470-2 del Codice della sanità pubblica francese (che regola l'identificazione elettronica obbligatoria per gli utenti dei servizi digitali sanitari), consegue che quando il trattamento riguarda categorie particolari di dati personali, come i dati relativi alla salute, il trattamento deve beneficiare di misure di sicurezza

Giurisprudenza

Errore diagnostico: il Tribunale di Trani esclude la responsabilità del medico

Con la sentenza n. 768 del 30 giugno 2026, il Tribunale di Trani ha respinto la domanda di risarcimento proposta dal figlio di un paziente morto per carcinoma polmonare contro il medico refertante e la struttura sanitaria. Il Tribunale ha infatti riconosciuto l'errore diagnostico, ma ha escluso che abbia inciso sulla sorte del paziente. Nell'ottobre 2007 l'uomo si era sottoposto a una radiografia del torace, ma nel referto non c'era traccia della massa. La neoplasia era emersa solo sei mesi dopo, con una nuova lastra e una TAC, quando ormai non era più operabile, e il paziente era morto nel settembre 2008. Secondo il figlio, una diagnosi tempestiva avrebbe consentito l'intervento chirurgico, portando le probabilità di sopravvivenza dal 5% al 57%. La consulenza tecnica ha confermato che la lesione era visibile già nel 2007 e che il medico avrebbe dovuto segnalarla. I periti hanno però escluso che l'omissione abbia pesato sull'esito. Il tumore era così aggressivo che anche una diagnosi anticipata avrebbe portato alle stesse cure e alle stesse probabilità di sopravvivenza. Pertanto, per il Tribunale spetta al paziente dimostrare, secondo la regola del "più probabile che non", che l'errore ha causato o aggravato il danno. Il giudice ha distinto poi due piani da non confondere: la perdita di chance riguarda l'incertezza sull'entità del danno, non sulla sua causa. Se resta il dubbio che il danno derivi dall'errore, non c'è una chance perduta da risarcire, ma un nesso causale che manca.

rafforzate. L'adequatezza di tali misure deve essere valutata concretamente, esaminando se siano state attuate dal titolare tenendo conto dei diversi criteri indicati nella norma e delle esigenze di protezione dei dati specificamente inerenti al trattamento interessato, nonché dei potenziali rischi da esso derivanti¹.

In secondo luogo, l'*Hôpital Privé de la Loire* è stato sanzionato per violazione dell'**art. 34 del GDPR** - che impone la comunicazione tempestiva del data breach agli interessati in presenza di rischi elevati - per aver notificato la violazione solamente ai pazienti e non anche ai più di 200 mila "soggetti terzi" i cui dati personali erano stati ugualmente interessati dal data breach. L'esposizione di informazioni personali e di natura clinica configura di per sé un rischio elevatissimo per i diritti e le libertà delle persone (si pensi al furto d'identità, al ricatto o alla discriminazione sanitaria) e la reticenza o il ritardo nella notifica individuale hanno potenzialmente privato gli interessati della possibilità di adottare contromisure rapide².

¹ La CGUE nella sentenza del 14 dicembre 2023 (CGUE, 14 dicembre 2023, C-340/21) ha chiarito che il GDPR istituisce un regime di gestione dei rischi e non mira affatto a eliminare i rischi di violazione dei dati personali; si limita ad imporre al titolare del trattamento di adottare misure tecniche e organizzative volte a evitare, per quanto possibile, qualsiasi violazione dei dati personali

² Cfr. Linee Guida 9/2022 Comitato Europeo per la Protezione dei Dati

Attualità

Marsh, People Risk Report 2026: la scarsa cultura cyber è il primo rischio "umano" per le imprese italiane

Il principale rischio per le imprese italiane nel prossimo biennio è l'insufficiente consapevolezza delle minacce informatiche. È quanto emerge dal *People Risk Report 2026* di Marsh, basato sulle valutazioni di oltre 4.500 professionisti HR e risk management in 26 mercati. Nella graduatoria nazionale seguono l'insicurezza finanziaria dei dipendenti, la scarsa competitività delle strategie di attrazione e retention, la carenza di competenze tecnologiche specialistiche e la mancanza di personale. Il dato tecnologico ricorre più volte nella top ten italiana. Oltre alla cyber awareness compaiono il deficit di competenze tecnologiche, al quarto posto, e la gestione impropria di dati e proprietà intellettuale, all'ottavo. Secondo Marco Araldi, CEO di Marsh Italia, il rischio cyber va ormai letto come rischio organizzativo e culturale, non soltanto tecnico. Per questo la formazione dell'intera popolazione aziendale diventa decisiva. L'adozione dell'intelligenza artificiale amplia il perimetro di esposizione. Tra le priorità indicate dalle imprese italiane figurano la formazione del personale per riconoscere contenuti malevoli o disinformazione generati dall'AI (38%), la prevenzione di violazioni di privacy e riservatezza (36%), la gestione dei rischi di sicurezza legati ai sistemi AI o a un'adozione troppo rapida (36%) e le vulnerabilità cyber connesse all'AI (33%). Il report segnala infine un'integrazione ancora incompleta tra HR e risk management. Solo il 37% dei rispondenti italiani dichiara una piena collaborazione tra le due funzioni, contro il 47% che la definisce parziale e il 16% minima. Sul versante assicurativo, il 41% considera prioritario agevolare l'accesso dei dipendenti a coperture contro eventi climatici come incendi e alluvioni.

La negligenza dell'Ospedale si è manifestata anche successivamente, in occasione della procedura di reimpostazione delle password degli utenti del DPI esterni all'Ospedale, in quanto la struttura ha assegnato una password temporanea identica a tutti i professionisti, trasmessa peraltro non a loro direttamente, ma comunicata al presidente della commissione medica dell'istituto, incaricato poi di ritrasmetterla al personale sanitario. Anche tale condotta è stata ritenuta dal CNIL non conforme ai requisiti di sicurezza di cui all'art. 32 GDPR.

Le ispezioni dell'Autorità hanno, infine, evidenziato un'altra falla sistemica diffusa in ambito aziendale e sanitario, ovvero la gestione dei fornitori esterni che riflette una carenza strutturale nella governance dei responsabili del trattamento. Nel caso in commento è emerso che la software house produttrice del DPI era in grado di accedere regolarmente e di propria iniziativa ai dati ivi presenti per attività di manutenzione, senza alcuna autorizzazione o tracciamento

Attualità

Il Senato approva la delega per la riforma degli ordinamenti professionali: prescrizione quinquennale dell'azione di responsabilità

Il 3 agosto 2026 il Senato ha approvato il disegno di legge delega per la riforma della disciplina degli ordinamenti professionali, che passa ora all'esame della Camera. Il testo delega il Governo ad adottare, entro 24 mesi dall'entrata in vigore della legge, i decreti legislativi che riscriveranno accesso, esercizio, compenso e organizzazione di 15 professioni regolamentate, tra cui ingegneri, architetti, geometri, geologi, agronomi, consulenti del lavoro, giornalisti, attuari e consulenti in proprietà industriale. Sul piano della responsabilità professionale, due i profili di maggiore interesse. Da un lato, la delega conferma l'obbligo di polizza per la responsabilità civile professionale, con massimali da aggiornare almeno ogni cinque anni. Dall'altro, fissa in cinque anni il termine di prescrizione dell'azione di responsabilità professionale per le controversie non già disciplinate dalla legge sull'equo compenso. Si tratta di un criterio destinato, se confermato, a incidere sulla durata dell'esposizione dei professionisti e dei loro assicuratori, anche in relazione alle garanzie postume delle polizze claims made. Tra gli ulteriori contenuti: il compenso dovrà essere proporzionato alla prestazione, con parametri aggiornati da proporre da ciascun Consiglio nazionale anche ai fini della L. n. 49/2023; per le società tra professionisti, i soci professionisti dovranno detenere almeno i due terzi del capitale e dei diritti di voto. Le nuove regole diverranno operative solo con i decreti legislativi, che saranno trasmessi alle Camere per un parere non vincolante.

preventivo da parte dell'Ospedale committente e titolare del trattamento.

Tale prerogativa di accesso incondizionata non era proporzionale e necessaria rispetto alla funzione di assistenza tecnica e di manutenzione da parte della società produttrice del software: in caso di un intervento di manutenzione, infatti, sarebbe stato opportuno che i dipendenti del produttore del software chiedessero sistematicamente la preventiva autorizzazione dell'Ospedale.

Conclusioni: il vero costo di un data breach sanitario

La sanzione economica inflitta a un ospedale del gruppo Ramsay Santé è senz'altro importante, ma non impattante quanto il danno reputazionale che consegue alla vicenda.

Il messaggio che lancia al settore è inequivocabilmente chiaro: considerato che i dati sanitari rimangono l'obiettivo più sensibile e remunerativo, la cybersecurity e la privacy non possono essere considerate esclusivamente una scelta di investimento tecnologico.

Attualità

Rischi catastrofali: cresce la copertura delle imprese, ma il divario resta ampio

ANIA e Confindustria hanno pubblicato lo scorso 24 settembre una guida operativa sull'obbligo per le imprese di assicurarsi contro i rischi catastrofali (alluvioni, terremoti, frane, inondazioni ed esondazioni), illustrando coperture, scadenze e conseguenze del mancato adeguamento. L'obbligo, introdotto dalla L. n. 213/2023, è operativo dal 1° aprile 2025 per le grandi imprese, dal 1° ottobre 2025 per le medie, dal 1° gennaio 2026 per micro e piccole imprese e dal 1° aprile 2026 per quelle turistico-ricettive e della somministrazione di alimenti e bevande. La guida chiarisce inoltre i casi di beni in affitto o leasing e gli effetti sull'accesso alle agevolazioni pubbliche, principale conseguenza dell'inadempimento in assenza di sanzioni immediate. I dati IVASS mostrano un mercato in crescita ma ancora lontano dalla piena diffusione: le imprese non agricole assicurate sono il 16% dei 4,3 milioni censiti dall'Istat, rispetto al 13% di gennaio. Le polizze attive sono circa 683.000 (+14,5%), mentre tra gennaio e aprile 2026 il valore assicurato è aumentato di circa il 30% e i premi del 27,9%. Nel comparto operano 45 imprese, di cui 33 vigilate dall'IVASS e 12 estere. Permane un forte divario dimensionale: secondo ANIA, la copertura interessa il 14% delle microimprese, il 46% delle piccole, il 51% delle medie e il 97% delle grandi. Un dato che, insieme al provvedimento IVASS del 30 settembre sulla rilevazione dei prezzi di queste polizze, conferma la crescente attenzione

Non si tratta soltanto di introdurre firewall, antivirus o sistemi di backup, meccanismi di autenticazione robusti, minimizzazione dei privilegi di accesso, strumenti di monitoraggio continuo e capacità di risposta agli incidenti informatici. A questi elementi deve aggiungersi la dimensione organizzativa e culturale aziendale: conoscere quali dati vengono trattati, chi può accedervi ed in che limiti, prevedere strategicamente e prevenire i rischi di violazioni.

Una violazione di dati sanitari, infatti, può produrre conseguenze che vanno ben oltre la sanzione amministrativa: furto d'identità, phishing mirato, utilizzo fraudolento dei dati e, nel caso delle informazioni relative alla salute, possibili conseguenze sulla vita privata e professionale delle persone. L'elenco delle attività ispettive per il periodo agosto-dicembre 2026 pubblicato dal Garante Privacy italiano³ conferma l'attenzione delle Autorità al settore sanitario, dove, proteggere il dato significa anche proteggere la persona.

Il caso francese evidenzia, insomma, un principio fondamentale: la sicurezza dei dati

³ "b) verifica dei trattamenti dei dati personali contenuti nei fascicoli sanitari elettronici e di quelli svolti mediante l'utilizzo delle cd. app mediche [...] h) verifiche sui trattamenti di dati personali connessi all'utilizzo dei sistemi di intelligenza artificiale da parte di Comuni ed ASL", cfr. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10296923>

sanitari non è un investimento accessorio, ma parte integrante della qualità e dell'affidabilità di un'organizzazione sanitaria. Un ospedale, infatti, può curare correttamente un paziente sul piano clinico ma, al contempo, esporlo a un rischio significativo se non protegge adeguatamente le informazioni che lo riguardano.

Avv. Flavia Bartolazzi
Associate
at Improda Studio Legale