STUDIO LEGALE IMPRODA
AVVOCATI ASSOCIATI

CENTRO STUDI ROUTE IMPRESA

SLI INSURANCE WEBZINE

Notizie ed Approfondimenti sul Mondo Assicurativo

1-2025

Attualità

Riassicurazione targata SACE per i rischi catastrofali

SACE, al fine di tutelare le imprese italiane contro i danni provocati dalle catastrofi naturali, ha avviato le operazioni per il rilascio della garanzia pubblica operante contro i rischi catastrofali. La copertura – garantita dallo Stato e regolata con convenzione del Decreto del Ministero dell'Economia e delle Finanze - copre il 50% degli indennizzi assicurativi che le Compagnie assicurano alle imprese italiane per un importo complessivo - non superiore al plafond stabilito dalla legge di bilancio 2024 per il 2025 – fissato a 5 miliardi di euro. Attraverso tale strumento, le imprese potranno accedere ad una protezione specifica che ridurrà le perdite economiche derivanti da imprevisti devastanti. SACE, dunque, promuove la sostenibilità e l'efficienza dei processi con il supporto delle Compagnie di assicurazione.

Cybersecurity: tempo scaduto per i "Soggetti NIS2" obbligati a registrarsi sulla apposita piattaforma

Il 28 Febbraio 2025 è scaduto il termine di registrazione sulla **piattaforma online dell'Agenzia per la Cybersicurezza Nazionale** ("ACN"), previsto dalla Direttiva UE 2022/2555 ("Direttiva NIS2") nei confronti di quelle categorie di imprese rientranti nel relativo ambito di applicazione.

La norma europea è stata recepita in Italia con D. Lgs. n. 138/2024 in vigore dal 18 ottobre 2024 ("Decreto

Approfondimento

Arbitro Assicurativo: la nuova procedura di risoluzione stragiudiziale delle controversie assicurative

Con Decreto del Ministero delle Imprese e del Made in Italy pubblicato in Gazzetta Ufficiale il 9 gennaio 2025 è stato istituito nel nostro ordinamento, in particolare presso l'IVASS, l'Arbitro Assicurativo. Si tratta di un sistema di ADR, "*Alternative Dispute Resolution*", che ha l'obiettivo di ridurre i contenziosi dinanzi ai Tribunali e, dunque, di assicurare tempi celeri di giustizia. Anzitutto, l'arbitro assicurativo sarà competente in materia di controversie che derivano da un contratto assicurativo - ad esclusione dei grandi rischi (quelli definiti all'art. 1, c. 1, lett. R del Codice delle Assicurazioni) e tutti i sinistri che fanno capo alla CONSAP (Concessionaria Servizi Assicurativi Pubblici) – dunque di natura documentale con l'eliminazione di qualsiasi istruttoria. Il procedimento sarà instaurato attraverso un ricorso che dovrà essere preceduto a pena di inammissibilità da un reclamo inviato all'impresa assicurativa rimasta silente nel termine di 45 giorni. Il ricorso, sempre a pena di inammissibilità, dovrà essere presentato entro 12 mesi dalla presentazione del reclamo ed avere il medesimo oggetto. I ricorsi potranno riguardare anche somme di denaro a condizione che non superino i limiti fissati in 150.000 euro per i rami vita e 300.000 euro per le polizze del ramo I; mentre 2.500 euro per i casi di responsabilità civile mediante azione diretta e 25.000 euro in tutti gli altri casi.
Il collegio - composto da cinque membri, di cui tre nominati dall'IVASS, uno dall'associazione di categoria, uno dall'associazione degli intermediari e uno dal Consiglio Nazionale dei Consumatori - entro 90 giorni deciderà sul ricorso formulando una proposta conciliativa che, se accettata, determinerà la cessazione della procedura. In caso contrario, il procedimento (se il ricorso non viene accolto) potrà essere dichiarato estinto e inammissibile se siano necessari ulteriori accertamenti. In conclusione, l'arbitro assicurativo rappresenta un indubbio strumento di celerità per la risoluzione delle controversie ma per la sua diffusione sarà necessario anche informare il cliente della possibilità di adottare una procedura alternativa al contezioso giurisdizionale.

Attuativo"), il cui articolo 7, infatti, ha ribadito tale obbligo di auto-identificazione da parte dei soggetti considerati essenziali e/o importanti secondo la Direttiva stessa.

Il **censimento dei cc.dd. Soggetti NIS2** rappresenta la fase iniziale del processo di implementazione della recente normativa europea in materia di cybersicurezza. In forza della Direttiva NIS2 ed alla luce degli obblighi che saranno via via definiti più in dettaglio dalla ACN, molti più operatori economici, rispetto a quelli inizialmente individuati dalla Direttiva Nis 1 (Direttiva UE 2016/1148), saranno tenuti a dotarsi di un modello organizzativo *ad hoc* che possa - ragionevolmente - garantire un livello "elevato" di sicurezza dei sistemi informatici; ciò conformemente all'obiettivo che la Direttiva intende perseguire, ovvero assicurare una elevata sicurezza cibernetica all'interno del mercato unico comunitario.

Fra i criteri di individuazione della platea di Soggetti NIS2, vi è *in primis* quello dimensionale: sono tenuti ad implementare, all'interno della propria organizzazione, le disposizioni di cui alla Direttiva le categorie di operatori pubblici e privati rientranti nei **settori elencati negli Allegati I, II, III, IV** della

Giurisprudenza

Responsabilità medica: due ricoveri rappresentano due contratti diversi con la conseguenza che sono diverse le domande e le prestazioni

Con Ordinanza del 13 settembre 2024 n. 24656, la Corte di Cassazione si è pronunciata in tema di responsabilità medica su un caso che ha visto protagonista una paziente ricoverata tre volte in ospedale a distanza di un mese.
La donna veniva ricoverata per la prima volta per un intervento chirurgico di protesi all'anca. In seguito, la donna veniva ricoverata nuovamente lamentando la presenza di un'infezione contratta dal precedente intervento chirurgico. Sottoposta a cura antibiotica, la paziente veniva ricoverata una terza volta a causa del peggioramento delle condizioni cliniche. La donna citava in giudizio la struttura ospedaliera per accertarne la responsabilità del primo del primo dei tre ricoveri nel quale aveva avuto origine l'infezione. In primo grado, veniva esclusa la responsabilità dei sanitari per il primo ricovero ma non per il secondo. Pertanto, l'ospedale veniva condannato al risarcimento. In appello, la sentenza di primo grado veniva riformata stante la responsabilità della struttura per fatti diversi rispetto a quelli avanzati nella domanda. La donna ricorreva, dunque, in Cassazione lamentando che la sentenza della Corte di Appello avesse erroneamente considerato la sentenza di primo grado. Secondo la ricorrente, la domanda doveva considerarsi estesa a tutta l'attività svolta dall'ospedale. In conclusione, la Corte ha stabilito che se il paziente lamenta la cattiva esecuzione dell'intervento, la domanda è estesa a ogni prestazione relativa all'intervento. Dunque, non possono aversi identità di domande, né può affermarsi che l'una contiene l'altra se queste eccepiscono due inadempimenti diversi in quanto relativi a due prestazioni di due diversi contratti.

Direttiva stessa, che superino i massimali delle piccole imprese, secondo la definizione fornita dall'art. 2 comma 2 dell'Allegato alla Raccomandazione 2003/361/CE[1]. Le **medie e grandi imprese**, ovvero quelle realtà il cui numero di addetti effettivi superi le 250 persone e la soglia finanziaria (fatturato o bilancio annuo) superi i 50 milioni di Euro, se operanti nei settori di cui sopra, rientrano di *default* nell'ambito di applicazione della Direttiva.

Nelle ipotesi di gruppi di imprese, laddove il suddetto criterio dimensionale non risulti proporzionato, occorrerà distinguere fra imprese autonome, imprese associate ed imprese collegate[2]; per poi indagare, per ciascuna, il livello di indipendenza dal gruppo cui essa appartiene, al fine di invocare - ove ne ricorrano i presupposti di autonomia, meglio individuati dal DPCM n. 221/2024 del 10 febbraio 2025 - l'applicabilità, o meno, della **clausola di salvaguardia** di cui all'art. 3 comma 4 del Decreto Attuativo.

Tale clausola, in altri termini, consente di operare un "declassamento" della società:

[1] *"2. Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR".*
[2] Per le relative definizioni cfr. Art. 3 Allegato Raccomandazione 2003/361/CE.

Attualità

Polizza catastrofale: scatta l'obbligo per le imprese di dotarsi dell'assicurazione CAT-NAT

È entrato in vigore, con Decreto del Ministero dell'Economia e delle Finanze del 30 gennaio 2025, il regolamento sulle modalità operative degli schemi di assicurazione dei rischi catastrofali secondo quanto disposto dall'art. 1, c. 150 della legge 213/2023. Quest'ultimo obbliga le imprese di dotarsi entro il 31 marzo 2025 della polizza catastrofale a copertura dei danni ai beni di cui all'art. 2424, c.1 derivanti dalle calamità naturali. Al riguardo il Decreto del MEF ha stabilito le modalità operative di individuazione degli eventi di rischio, di determinazione e adeguamento dei premi e di coordinamento. In particolare, sono definiti eventi calamitosi: le alluvioni, le inondazioni, esondazioni, i sismi e le frane. Con riguardo all'assunzione del rischio, questo dovrà essere aggiornato con cadenza annuale e con riferimento all'intero portafoglio. Il Decreto stabilisce inoltre i principi che regolano i massimali e i limiti di indennizzo: sino a un milione di euro di somma assicurata, un limite di indennizzo pari alla somma assicurata; da un milione a 30 milioni di euro della somma assicurata, un limite di indennizzo non inferiore al 70%; superiore a 30 milioni di euro della somma assicurata, il massimale è rimesso alla negoziazione tra le parti. Inoltre, il Decreto stabilisce le misure di trasparenza dell'offerta assicurativa: sia in tema di trasparenza e concorrenzialità nonché di informazione che le imprese dovranno assolvere pubblicando sul proprio sito internet i documenti ai sensi dell'art. 185 del Codice delle Assicurazioni Private.

i) da grande a media impresa, con effetti rispetto alla qualifica del soggetto come <<essenziale>> o <<importante>>, rispetto agli obblighi ed alla misura delle sanzioni in caso di violazione;

ii) da media a piccola impresa, con conseguente esclusione della società dal campo di applicazione della Direttiva NIS2.

A prescindere dal criterio dimensionale, ai fini dell'assoggettamento dell'impresa (o del soggetto pubblico) all'ambito di applicazione della normativa *de qua*, bisogna valutare caso per caso la sussistenza delle fattispecie illustrate nei commi 5, 9 e 10 dell'art. 3 del Decreto Attuativo, ovvero verificare la peculiarità del servizio svolto dall'impresa ed il relativo impatto a livello nazionale, oppure se questa rientri fra determinate tipologie di soggetti non elencate nei suddetti Allegati, o ancora il ruolo della società nella *supply chain* del soggetto essenziale o importante.

All'esito della fase di auto-identificazione da parte delle imprese, secondo un principio di *accountability*, che rimanda al medesimo approccio adottato dal GDPR (reg. UE 2016/679) in materia di protezione dei dati personali, entro il **31 marzo 2025** l'ACN comunicherà

presso il domicilio digitale fornito al momento della registrazione, l'inserimento, la permanenza o l'espunzione dall'elenco del soggetto registrato, il quale tra il **15 aprile ed il 31 maggio 2025** dovrà, a sua volta, fornire i chiarimenti o le integrazioni eventualmente richiesti dall'Autorità.

Veniamo ora al cuore della Direttiva NIS2 ed ai principali obblighi ivi previsti.

Fermo restando il potere dispositivo dell'ACN, la quale può stabilire proporzionalmente specifici obblighi in capo ai Soggetti NIS2, tenendo conto del relativo grado di esposizione ai rischi, delle dimensioni del soggetto e del grado di probabilità che si verifichi un incidente informatico, l'art. 24 del Decreto Attuativo prevede che i soggetti essenziali e importanti adottino misure tecniche, operative ed organizzative adeguate e proporzionate alla gestione dei rischi per la sicurezza dei propri sistemi informativi e di rete, nonché idonee a prevenire e ridurre al minimo l'impatto di eventuali incidenti.

Agli operatori si richiede un **approccio multirischio**, volto a proteggere a 360° i sistemi informatici, per lo più, attraverso:

Approfondimento

Osservatorio Cybersecurity & Data Protection del Politecnico di Milano: il mercato cyber è in forte crescita

Secondo quanto analizzato dall'Osservatorio sulla Cybersecurity del Politecnico di Milano sono in aumento, in Italia, gli attacchi informatici. Lo dimostrano i numeri con il 73% delle imprese che hanno subito almeno un attacco nell'ultimo anno. Il mercato della cybersecurity cresce infatti del 15% per un controvalore totale di 2,48 miliardi di euro. Ma se i dati mostrano una tendenza in aumento delle minacce, l'Italia è all'ultimo posto tra i membri del G7 che investono in cybersicurezza. Come sottolineato da **Alessandro Piva**, Direttore dell'Osservatorio Cybersecurity & Data Protection: "*Nonostante questo segnale incoraggiante il 'cyber divide' tra organizzazioni mature e non mature è sempre più evidente e rappresenta una criticità silenziosa: la protezione rischia di rimanere un 'privilegio' per poche organizzazioni. È essenziale che le istituzioni locali ed internazionali continuino a lavorare per abbattere le barriere che impediscono l'introduzione di tecnologie e competenze. Nonostante l'aumento degli investimenti, infatti, ancora oggi la cybersecurity viene vista in molte realtà come un'attività onerosa e c'è il rischio che sia compromessa la capacità di resilienza e risposta alle minacce. Inoltre, il progresso dell'AI generativa rischia di creare nuove vulnerabilità e un'ulteriore intensificazione degli attacchi.*" Dello stesso tenore anche **Gabriele Faggioli**, Responsabile dell'Osservatorio Cybersecurity & Data Protection che ha affermato:" *Il panorama delle minacce informatiche si conferma allarmante: nel 2024 sono stati registrati 3.541 incidenti cyber gravi di dominio pubblico a livello globale, di cui circa il 10% in Italia, ma la capacità di gestire efficacemente i rischi cyber moderni non si sta diffondendo alla stessa velocità. Di certo, si evidenzia una crescente centralità della cybersecurity nelle priorità aziendali e istituzionali per la maggiore rilevanza delle minacce informatiche, per i progressi tecnologici e anche per l'evoluzione delle normative. Persone con scarsa alfabetizzazione digitale possono essere sempre più vittima di disinformazione, frodi online e violazioni della privacy. La cybersecurity si appresta a diventare un pilastro della competitività economica e dell'equilibrio sociale e politico*". Panorama che muterà, grazie alla NIS 2, con l'obbligo per le imprese di adeguarsi nella capacità di resilienza.

Giurisprudenza

La Cassazione sui criteri di interpretazione del contratto di assicurazione

La Corte di Cassazione con Ordinanza n. 3013 del 6 febbraio 2025, ha analizzato i criteri di interpretazione di un contratto assicurativo contro il rischio di infortuni e malattie.
La vicenda trae origine dal ricorso ex art. 702 bis c.p.c. di un dirigente a tempo determinato che, nelle more del perfezionamento del contratto di lavoro a tempo indeterminato, veniva colpito da infarto e a causa dei postumi non si perfezionava l'assunzione. Ebbene, prima dell'evento disdicevole, la società datrice di lavoro aveva stipulato un contratto di assicurazione contro il rischio di infortuni e malattie a beneficio dei propri dirigenti. Pertanto, il dirigente chiedeva la condanna della società al pagamento dell'indennizzo dovuto. Il Tribunale di Roma accoglieva la domanda con Ordinanza che veniva appellata dalla società. La Corte di Appello con sentenza riformava l'Ordinanza statuendo che non vi era prova che la risoluzione del rapporto di lavoro era avvenuto in conseguenza di una malattia. Con ricorso in Cassazione, il dirigente denunciava con il quinto motivo la violazione, da parte della Corte di Appello, degli articoli 1363, 1366, 1367 e 1370 c.c. in tema di interpretazione del contratto. La Cassazione, sul punto, ha accolto il quinto motivo così motivando:" La *Corte d'appello, pertanto, è effettivamente incorsa nel duplice vizio, da un lato, di interpretare il contratto senza valutare le clausole in modo complessivo; e dall'altro di non rilevare che le clausole, unitariamente valutate, presentavano un evidente margine di ambiguità. Dinanzi a tale ambiguità la Corte d'appello ha effettivamente violato l'art. 1370 c.c., interpretando il contratto in senso favorevole al predisponente, ma senza dare alcun conto, in motivazione, né tale ambiguità, né della possibilità e soprattutto, degli specifici argomenti per superarla, in un senso o nell'altro*". Dunque, la Cassazione ha sconfessato l'interpretazione del contratto di assicurazione secondo il quale il pagamento dell'indennizzo doveva ritenersi subordinato alla circostanza che l'infortunio avesse determinato l'interruzione del rapporto di lavoro.

- delle politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;

- una gestione degli incidenti e relative notifiche;

- una continuità operativa dei sistemi (ad es. backup, ripristino in caso di disastro, gestione delle crisi);

- la sicurezza della catena di approvvigionamento e, quindi, nei rapporti con clienti/fornitori;

- delle politiche di sviluppo e manutenzione dei sistemi;

- delle politiche e procedure per valutare l'efficacia delle misure via via implementate;

- una formazione in materia di sicurezza informatica;

- dei meccanismi di autenticazione a più fattori e protette, delle procedure di crittografia e cifratura dei dati.

Rispetto a quanto sopra, un ruolo fondamentale è svolto dalla Governance: gli **organi di amministrazione di direzione**, infatti, ai sensi dell'art. 23 del Decreto Attuativo, approvano le misure di gestione dei rischi, sovrintendono all'implementazione dei suddetti obblighi, promuovono l'attività di formazione e, soprattutto,

rispondono di eventuali violazioni. In particolare, l'art. 38 comma 5 del Decreto Attuativo prevede che *"Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza".*

In tali casi, fra le sanzioni irrogabili ai sensi dell'art. 38 del Decreto Attuativo, il relativo comma 6 prevede la sanzione amministrativa accessoria dell'**incapacità a svolgere funzioni dirigenziali** all'interno dell'organizzazione, mentre i successivi commi 9 lett. a) e b), comma 11 lett. a) e b), comma 12 e 13 prevedono l'irrogazione della **sanzione amministrativa pecuniaria** sul fatturato aziendale, che varia a seconda della tipologia della violazione commessa (commi 8 e 10), del fatto che il soggetto sia ritenuto essenziale o importante e dell'eventuale reiterazione della violazione. La **mancata registrazione alla piattaforma** online dell'ACN, di cui all'art. 7 del Decreto attuativo, comporta l'applicazione della sanzione più grave aumentata fino al triplo attribuita alle violazioni indicate nei commi 8 e 10 dell'art. 38 del Decreto Attuativo.

Approfondimento

Aon, Swiss Re e Floodbase lanciano un nuovo prodotto parametrico per le tempeste

Aon in collaborazione con Floodbase e Swiss Re Corporate Solutions, ha lanciato sul mercato una nuova soluzione ideata per affrontare le mareggiate causate dagli uragani al fine di offrire prodotti economicamente vantaggiosi rispetto a quelli che sul mercato richiedono franchigie elevate o esclusioni di garanzia per le mareggiate. Da quanto emerge dal rapporto di Aon "*Climate and Catastrophe Insight 2025*" l'uragano Helene è stato l'evento più catastrofico del 2024, con 75 miliardi di dollari di perdite economiche a causa delle inondazioni costiere degli Stati Uniti e con richieste di risarcimento pari a 37,5 miliardi di dollari. Il prodotto si distingue per l'utilizzo di dati meteorologici per valutare le inondazioni da mareggiate che, a differenza di un classico prodotto i cui pagamenti sono proporzionati ai danni fisici, la soluzione parametrica si basa su diversi elementi come l'altezza dell'acqua. Come dichiarato da Cole Mayer, responsabile delle soluzioni parametriche Aon: "*I nostri dati mostrano che l'ondata di tempesta può essere un fattore significativo di perdite per aziende, enti pubblici e (ri)assicuratori; quindi, abbiamo sviluppato questa soluzione parametrica collaborativa per aiutare a rafforzare i livelli di copertura esistenti. La soluzione può funzionare sia come prodotto autonomo sia in combinazione con polizze assicurative tradizionali e non tradizionali, per garantire che i clienti possano ottenere una protezione completa per le loro esposizioni all'ondata di tempesta negli Stati Uniti. Fa parte di una serie di offerte di prodotti Aon che insieme stanno aiutando a modellare decisioni migliori e fonti di liquidità più complete per i clienti".* Come prospettato Oltreoceano, una soluzione simile potrebbe essere introdotta anche nel panorama nazionale, considerati i fenomeni atmosferici e di dissesto idrogeologico che provocano ogni anno ingenti danni.

Attualità

ANIA: cresce la produzione mensile del 15,6%

Dal rapporto mensile di ANIA, a gennaio la nuova produzione vita sale a €7,4 miliardi circa il 15,6% in più rispetto al 2024. Con riguardo ai premi raccolti dalle imprese U.E., si registra un aumento del 5,8% per un totale di € 648 milioni con i nuovi affari del ramo vita che hanno toccato a gennaio € 8 miliardi. In calo la raccolta del ramo I a € 5 miliardi rispetto alla crescita del 15,7% dello stesso mese del 2024. Positivi dati del ramo V e del ramo III con un importo raggiunto di € 199 milioni per il primo ramo e di € 2,2 miliardi per il secondo. Complessivamente, dai dati riportati dall'ANIA, i volumi d'affari hanno raggiunto ottime cifre più che triplicate rispetto ai mesi del 2024 con una raccolta degli sportelli bancari e postali che ha toccato quota € 5,3 miliardi.

L'importanza sempre crescente che l'Unione Europea riconosce alla sicurezza informatica, cercando di adottare normative che tutelino tale aspetto in maniera uniforme tra gli Stati membri dell'Unione, è una delle risposte alla rilevanza e frequenza che gli attacchi informatici hanno acquisito negli ultimi anni, in un mondo sempre più dipendente dai dati.

In tale contesto, una corretta analisi e **gestione del rischio cyber** non può prescindere dalla opportunità di dotarsi di una idonea **copertura assicurativa**. L'assicurazione sulla cybersecurity deve, quindi, essere considerata come uno strumento per integrare i processi e le tecnologie di sicurezza che implementano le strategie di gestione del rischio informatico adottate dall'azienda.

Avv. Gabriella Napolano
Partner at Studio Legale Improda

Avv. Flavia Bartolazzi
Associate at Studio Legale Improda