LA SAPIENZA UNIVERSITÀ DI ROMA
Dipartimento di Scienze Giuridiche

DOTTORATO IN AUTONOMIA PRIVATA, IMPRESA, LAVORO E TUTELA DEI DIRITTI NELLA PROSPETTIVA EUROPEA ED INTERNAZIONALE

Curriculum di Realtà e Radici del diritto privato europeo

Tesi di Dottorato

CYBERSECURITY.
PROFILI DI RESPONSABILITÀ E GESTIONE DEL RISCHIO

Tutor
Prof. Avv. Luca Di Donna

Dottoranda
Giulia Angelini

XXXVIII Ciclo
A.A 2025/2026

Sommario

Introduzione

La trasformazione digitale ha inciso in modo strutturale sulle modalità di svolgimento delle attività economiche, sull'organizzazione delle imprese e sull'esercizio dei diritti, determinando una crescente dipendenza da infrastrutture, servizi e prodotti digitali.

In questo contesto, la cybersecurity ha progressivamente assunto una rilevanza giuridica autonoma, non più riconducibile alla sola dimensione tecnica della sicurezza informatica né esauribile nella disciplina settoriale dei servizi digitali. L'emersione del rischio cyber come componente ordinaria dell'attività economica impone, infatti, un ripensamento delle categorie giuridiche tradizionali chiamate a governarne gli effetti. La possibilità di eventi dannosi connessi all'uso di sistemi informativi, prodotti digitali e servizi connessi non rappresenta più un'eccezione, bensì un dato strutturale del funzionamento della società digitale che il diritto è chiamato a regolare secondo logiche di prevedibilità, allocazione e gestione del rischio.

In tale prospettiva, la cybersecurity si configura come un ambito privilegiato per osservare l'evoluzione del diritto civile contemporaneo, nella misura in cui sollecita una riflessione sui criteri di imputazione della responsabilità, sui modelli di diligenza esigibili e sugli strumenti attraverso i quali l'ordinamento consente di assorbire e redistribuire le conseguenze economiche degli eventi dannosi.

La sicurezza cibernetica non si esaurisce, dunque, nella prevenzione tecnica dell'evento ma si inserisce in una più ampia architettura giuridica volta a governare il rischio, combinando obblighi di comportamento, assetti organizzativi e meccanismi di compensazione.

L'intervento del legislatore europeo e nazionale, caratterizzato da un crescente ricorso a modelli regolatori di tipo *risk-based*, conferma tale impostazione. La disciplina della cybersicurezza si sviluppa, infatti, lungo una direttrice che integra prevenzione, responsabilizzazione degli operatori e gestione delle conseguenze del danno, delineando un sistema nel quale la tutela degli interessi coinvolti non è affidata a un unico strumento, ma a una pluralità di tecniche giuridiche tra loro complementari.

La presente ricerca si colloca in questo orizzonte e si propone di analizzare la cybersecurity come fenomeno giuridico complesso, nel quale la responsabilità civile e la gestione del rischio costituiscono due dimensioni inscindibili. L'obiettivo è indagare in che misura il diritto civile sia chiamato a rimodellare le proprie categorie tradizionali per rispondere alle esigenze poste dal rischio cyber e come, all'interno di tale processo, si articolino i rapporti tra prevenzione del danno, imputazione della responsabilità e strumenti di trasferimento del rischio.

L'analisi adotta un approccio sistematico e multilivello, valorizzando il contributo della regolazione europea e il dialogo tra norme di diritto positivo, prassi di mercato e strumenti di governance del rischio.

In questa cornice, la cybersecurity emerge non solo come ambito di regolazione settoriale ma come terreno di osservazione privilegiato delle trasformazioni in atto nel diritto civile, chiamato a confrontarsi con una “nuova normalità” del rischio digitale.

Capitolo I

Cybersecurity: fondamenti giuridici e dimensioni istituzionali

Sommario: 1. Definizione giuridica e dimensioni della cybersecurity; 1.1. La dimensione pubblica della cybersecurity; 1.2. Sicurezza informatica e protezione dei dati personali; 2. L'evoluzione normativa europea: le coordinate di riferimento; 2.1. Dalla Direttiva NIS al Cybersecurity Act; 2.2. Il quadro normativo italiano; 2.3. Il ruolo del GDPR nella sicurezza informatica; 2.4. Il Cyber Resilience Act; 3. Attori della cybersecurity.

1. Definizione giuridica e dimensioni della cybersecurity

La nozione di cybersecurity occupa oggi una posizione centrale nel dibattito giuridico europeo e internazionale.

Dopo una fase iniziale caratterizzata da incertezze definitorie, essa ha progressivamente trovato ingresso negli ordinamenti assumendo una rilevanza trasversale.

La sua definizione risulta infatti dall'intersezione tra dimensioni tecnologiche, organizzative e normative, che impongono un'analisi sistematica e multilivello.

È pertanto necessario esaminare preliminarmente le principali definizioni giuridiche offerte dalle fonti nazionali e sovranazionali, per poi ricostruire le diverse componenti concettuali della cybersicurezza, evidenziandone la natura complessa e multidisciplinare.

Il termine viene talvolta assimilato alla *computer security* e alla *information security*, che tuttavia ne rappresentano soltanto parti costitutive di un concetto più ampio.[1]

L'espressione *computer security* riflette una concezione originaria della sicurezza informatica incentrata sulla protezione del computer e, più in generale, dell'infrastruttura hardware e software.

L'evoluzione tecnologica e socio-economica, unita all'affermazione della cosiddetta società dei dati, ha condotto a un ampliamento di prospettiva determinando l'emergere della cd *information security*, orientata principalmente alla tutela delle informazioni.[2]

In questa prima prospettiva, la sicurezza informatica si configura come l'insieme delle misure volte a garantire l'integrità, la disponibilità e la confidenzialità delle risorse che costituiscono un sistema informativo.

L'evoluzione concettuale emerge in modo evidente anche analizzando gli interventi dell'Unione Europea nel settore.

Dalla direttiva 90/387/CE, volta a promuovere la creazione del mercato interno dei servizi di telecomunicazione attraverso l'introduzione dell'Open Network Provision (ONP), si giunge, ad esempio, alla direttiva Digital Single Market

---

[1] ENISA, *ENISA Overview of cybersecurity and related terminology,* 2017, p. 6.

[2] Per le definizioni, si veda in M. NIELES, K. DEMPSEY, V. YAN PILLITTERI, in *An introduction to Information Security,* in *NITS Special Publication 800-12, revision 1, 2017.*

(2019/790/UE) in materia di diritto d'autore e diritti connessi nel mercato unico digitale, nonché al Regolamento generale sulla protezione dei dati personali (UE/2016/679).

Solo negli ultimi anni si è affermata, sia nella letteratura scientifica e tecnica sia nella normativa nazionale e internazionale, la categoria della cybersecurity di cui tuttavia manca ancora un quadro definitorio pienamente uniforme, data la complessità dei concetti coinvolti.

Tale mutamento è stato determinato dalla crescente consapevolezza della necessità di estendere il tradizionale perimetro semantico della sicurezza informatica.[3]

La nozione di cybersicurezza deriva dal concetto di cyberspazio, inteso come l'insieme delle connessioni e delle interazioni tra dispositivi e sistemi accessibili tramite reti di telecomunicazione, dotati di interfacce che ne permettono il controllo da remoto e l'accesso ai dati. Il termine ha avuto origine negli Stati Uniti, in riferimento alla capacità di proteggere questo spazio digitale dalle minacce cibernetiche.[4]

---

[3] P.L. MONTESSORO, in *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in *Istituzioni del Federalismo*, 2019, pp. 783 e ss.

[4] ENISA, *L'anno in rassegna da gennaio 2019 ad aprile 2020*, 2020; CLUSIT, *Rapporto Clusit 2021 sulla sicurezza ICT in Italia,* 2021.

La sicurezza informatica, dunque, elaborata in principio da professionisti IT, consulenti e decisori politici, si sviluppa come risposta alle vulnerabilità proprie di tale ambiente.[5]

In termini generali, può essere intesa quale estensione della sicurezza informatica e cioè come l'insieme delle tecnologie, dei programmi e dei processi destinati a proteggere dispositivi, dati e reti di uno Stato o di altri enti da intrusioni perpetrate per via informatica.

Il Regolamento UE 2019/881 definisce la cybersecurity come "*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*", definizione ripresa anche dalla Direttiva NIS2, all'art. 6 n. 3.

Le attività di cybersicurezza mirano dunque a contrastare le minacce informatiche e "*qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone*." [6]

---

[5] G. COSTABILE, in *Cybersecurity e digital divide, investiamo anche sul territorio con una regia nazionale, Formiche.net, 2 agosto 2022, https://formiche.net/2022/08/cybersecurity-digital-divide-investiamo-territorio-regia-nazionale/.*

[6] Il riferimento è all'art. all'articolo 2, punto 8) del Regolamento (UE) 2019/881, relativo all'ENISA.

La norma ISO/IEC 27000:2018[7], invece, fa riferimento "*alla preservazione della riservatezza, integrità e disponibilità delle informazioni*" in qualunque forma rappresentate e comunque tramesse.

Le tre dimensioni indicate rinviano ai concetti di *confidentiality* (divieto di divulgazione delle informazioni a soggetti non autorizzati); *integrity*, che attiene all'accuratezza e alla non alterazione del dato; e *availability of information*, relativa alla possibilità per i soggetti autorizzati di accedere ai dati quando necessario. Tali principi, noti come CIA factors secondo il NIST[8], costituiscono il nucleo per la pianificazione e la gestione della sicurezza informatica.[9]

---

[7] La serie ISO/IEC 27000 ricomprende gli standard di sicurezza delle informazioni che si supportano reciprocamente e che insieme forniscono un quadro riconosciuto a livello globale delle best practice per la gestione della sicurezza delle informazioni ed è pubblicata da dall'International Organization for Standardization (ISO) e dall'International Electrotechnical Commission (IEC).

[8] Il National Institute of Standards and Technology (NIST, in origine National Bureau of Standards [NBS]) è un'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie. Fa parte del Dipartimento del Commercio e il suo compito è la promozione dell'economia americana attraverso la collaborazione con l'industria al fine di sviluppare standard, tecnologie e metodologie che favoriscano la produzione e il commercio. Il NIST si sta occupando attivamente delle tessere di identificazione per i dipendenti federali, al fine di controllare e prevenire il terrorismo, i criminali, e tutti gli accessi non autorizzati all'interno di strutture governative e dei loro sistemi informatici. Negli ultimi anni il NIST è tra i principali riferimenti autorevoli relativamente alla cybersecurity.

[9] *Sicurezza delle informazioni: i tre principi per gestire il cyber risk, Agenda Digitale*, 21 giugno 2023, https://www.agendadigitale.eu/sicurezza/sicurezza-delle-informazioni-i-tre-principi-per-gestire-il-cyber-risk/.

In sintesi, le informazioni devono rimanere riservate, accessibili ai soli soggetti autorizzati, integre, modificabili esclusivamente da utenti abilitati e disponibili ogniqualvolta occorra accedervi.

La crescente complessità dell'ecosistema digitale espone tali valori a una molteplicità di minacce che generano rischi di perdita o compromissione del dato e dei sistemi deputati alla sua gestione; tali rischi devono essere valutati considerando i potenziali impatti sul sistema nel suo complesso.[10]

È evidente, anche da questa breve ricostruzione, che ciascuna definizione intercetti aspetti differenti del fenomeno e che quest'ultimo non possa essere ricondotto ad un'unica e univoca prospettiva.

Ridurre la cybersecurity alla mera protezione dei sistemi informativi e dei dati appare oggi insufficiente poiché i valori e i diritti coinvolti si estendono ben oltre tali dimensioni.

Sebbene la disciplina trovi la sua origine nell'informatica, essa si configura ormai come un ambito intrinsecamente trasversale, che richiede competenze integrate in settori quali la gestione del rischio, l'economia, il diritto e persino le scienze comportamentali.

Ne deriva la necessità di adottare un approccio olistico, capace di cogliere la complessità delle minacce attuali e di assicurare un livello adeguato di tutela

[10] ENISA, *Overview of Cybersecurity and Related Terminology*, 2017.

nei confronti dei settori critici in cui le conseguenze di un attacco possono assumere particolare gravità.

Nell'attuale scenario digitale predisporre sistemi di sicurezza adeguati e, conseguentemente, individuare comportamenti, procedure e meccanismi di controllo idonei, significa riconoscere che i fattori di rischio non si esauriscono nelle sole vulnerabilità tecnologiche. Essi comprendono anche la potenziale lesione dei diritti e delle libertà fondamentali delle persone, nonché l'esposizione delle infrastrutture critiche e degli equilibri politici a forme di attacco capaci di generare conseguenze talvolta imprevedibili e, in alcuni casi, irreversibili per comunità, istituzioni e imprese.[11]

Sebbene gli attacchi informatici nascano spesso da nuove vulnerabilità presenti nelle architetture digitali, il loro impatto massimo si manifesta attraverso il fattore umano, oggi considerato l'anello più debole della catena di sicurezza.

La resilienza cibernetica di un Paese non può, pertanto, essere più circoscritta alla sola affidabilità dei presìdi tecnici approntati dagli apparati pubblici e dagli operatori privati, dovendo necessariamente estendersi al livello di sicurezza effettivamente garantito ai singoli utenti.

La vulnerabilità della persona risulta intimamente connessa tanto alla percezione soggettiva del rischio quanto al patrimonio di competenze tecniche

---

[11] R. BRIGHI, P.G. CHIARA, in *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea.,* in *federalismi.it,* 21/2021, p. 21.

possedute, elementi che influiscono in modo decisivo sulla capacità individuale di resistere alle insidie della dimensione digitale.

A plasmare in modo decisivo la più recente concettualizzazione della cybersicurezza ha contribuito, in misura significativa, l'intervento dell'Unione europea la cui azione ha iniziato a delinearsi con particolare chiarezza dal 2012, anno in cui fu presentata la "*Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace*".

Attraverso un approccio marcatamente *top-down*, l'Unione ha posto le basi per un quadro organico di politiche, principi e indirizzi strategici finalizzati a elevare il livello di protezione dello spazio digitale europeo.

In tale contesto, le istituzioni europee hanno sottolineato come il conseguimento di un elevato standard di sicurezza informatica non rappresenti soltanto una condizione necessaria per garantire la continuità dei servizi essenziali e il regolare funzionamento della società contemporanea, fortemente dipendente dalle infrastrutture digitali; esso costituisce altresì un presupposto imprescindibile per la tutela dell'integrità psicofisica degli individui, sempre più esposti alle conseguenze, dirette e indirette, delle minacce informatiche.

La prospettiva europea ha dunque ampliato l'orizzonte della cybersecurity, trasformandola da mero presidio tecnico a strumento di governo del rischio, funzionale alla salvaguardia non solo di asset materiali e immateriali, ma anche dei diritti fondamentali della persona.

Tale evoluzione, lungi dall'esaurirsi nel dato normativo, ha favorito la maturazione di un approccio culturale e regolatorio più consapevole che riconosce nella sicurezza cibernetica un interesse pubblico primario e un elemento cardine della stabilità democratica e sociale.

1.1.La dimensione pubblica della cybersecurity

La progressiva digitalizzazione delle relazioni economiche e sociali ha profondamente trasformato il significato della sicurezza nello spazio cibernetico, facendo emergere una dimensione che va oltre la mera protezione tecnica dei sistemi informativi.

La cybersecurity si configura oggi come un fattore essenziale per il funzionamento ordinato della società digitale e per la tutela dei diritti fondamentali. In tale contesto, una parte della dottrina ha proposto di qualificare la cybersecurity come bene pubblico[12], sottolineandone la funzione sistemica e collettiva.

Secondo questa impostazione, la sicurezza cibernetica non può essere ricondotta alla semplice somma delle misure adottate dai singoli attori pubblici o privati, ma costituisce un interesse collettivo primario la cui realizzazione richiede un'azione coordinata, multilivello e strutturale.

---

[12] R. MARCHIONATTI e F. MORNATI, in *Principi di Economia Politica,* Giappichelli Editore, Torino, 2011, p. 171 ove un bene è definito pubblico quando il suo consumo presenti le caratteristiche della non-rivalità e non escludibilità.

L'interdipendenza delle reti, la natura transfrontaliera delle minacce e la centralità del dato rafforzano l'esigenza di un intervento pubblico stabile e organizzato.[13]

L'assimilazione della cybersecurity ai beni pubblici tradizionali, quali la sicurezza nazionale o la salute, comporta, sul piano teorico, un bilanciamento degli interessi tendenzialmente orientato a favore dell'interesse generale e una valorizzazione del ruolo pubblico nella protezione delle infrastrutture.

Tale ricostruzione, tuttavia, presenta rilevanti criticità.

La cybersecurity, infatti, non appare riconducibile a un'unica dimensione omogenea, né può essere trattata come un bene unitario idoneo a fronteggiare in modo uniforme la molteplicità delle minacce cibernetiche.

Per questa ragione, parte della dottrina limita la qualificazione pubblicistica alla sola componente informativa del sistema, in particolare allo scambio di dati su vulnerabilità, minacce e indicatori di compromissione.[14]

Anche a voler accogliere la qualificazione pubblicistica della cybersecurity, la comparazione mostra come, nei principali sistemi giuridici, la garanzia di un livello adeguato di sicurezza richieda comunque una strutturale cooperazione tra settore pubblico e settore privato.

---

[13] D.K. MULLIGAN e F.B. SCHNEIDER, in *Doctrine for Cybersecurity,* in *Daedalus,* n. 104 vol.4, 2011, pp. 70-90.

[14]P. ROSENZWEIG, in *Cybersecurity and Public Goods: The Public/Private "Partnership",* in *Cyberwarfare: How Conflicts in Cyberspace are Challenging the World,* 2012, pp.7 e ss.

Anche adottando una concezione ampia della cybersecurity come interesse pubblico, l'analisi comparata mostra come la garanzia di un adeguato livello di sicurezza richieda comunque una cooperazione strutturale tra settore pubblico e settore privato. Al primo spettano la definizione di standard minimi, regole tecniche e meccanismi di gestione del rischio; al secondo, che detiene una parte significativa delle infrastrutture critiche, l'implementazione di misure di protezione efficaci.[15]

Tale logica di complementarità tra pubblico e privato caratterizza tanto i modelli statunitensi, improntati a partenariati flessibili, quanto l'ordinamento europeo che predilige approcci più prescrittivi e coordinati.[16]

Alla luce di tali considerazioni, la comprensione effettiva della cybersecurity non può prescindere da un approccio che valorizzi la dimensione collaborativa pubblico–privato.

In conclusione, la qualificazione della cybersecurity come bene pubblico costituisce uno strumento concettuale utile ma non esaustivo.

Una comprensione adeguata del fenomeno richiede un approccio critico e pluralista, capace di tenere insieme intervento pubblico, autonomia privata, innovazione tecnologica e tutela dei diritti e delle libertà fondamentali.

---

[15] M. TADDEO, in *Is Cybersecurity a Public Good?,* in *Mind & Machine,* n. 29, Springer, 2019, p. 351.

[16] Sul punto, F. CAPPELLETTI e L. MARTINO, in *Acheving robust European cybersecurity through public-private partnerships: Approches and developments*, in *Elf discussion papers*, 4, 2021.

1.2.Sicurezza informatica e protezione dei dati personali

Sebbene concettualmente distinti, sicurezza informatica e protezione dei dati personali costituiscono ambiti profondamente interrelati.

Tale correlazione emerge con evidenza nell'attuale contesto tecnologico caratterizzato da un crescente ricorso a sistemi informatizzati e da una continua circolazione delle informazioni.

La cybersecurity è finalizzata a garantire l'integrità, la disponibilità e la riservatezza di reti, sistemi informativi e dati, prevenendo accessi non autorizzati, alterazioni e compromissioni.

La protezione dei dati personali, invece, concerne la tutela delle informazioni riferibili a persone fisiche identificate o identificabili, assicurando che il loro trattamento avvenga nel rispetto di criteri di liceità, correttezza e sicurezza.

Pur muovendo da presupposti differenti, entrambi gli ambiti perseguono finalità convergenti volte a proteggere individui e organizzazioni dai rischi connessi all'evoluzione tecnologica e alla diffusione dei servizi digitali.

Sul piano strettamente giuridico, l'intreccio tra sicurezza informatica e protezione dei dati personali risulta evidente già alla luce delle normative che ne disciplinano i rispettivi ambiti.

In particolare, il Regolamento (UE) 2016/679 (GDPR) impone ai titolari e ai responsabili del trattamento l'adozione di misure tecniche e organizzative

adeguate ai rischi, configurando obblighi che si collocano in stretta continuità con quelli propri della cybersecurity.[17]

Analogamente, la normativa in materia di sicurezza informatica richiede agli operatori di adottare misure idonee a proteggere l'integrità, la disponibilità e la riservatezza dei dati che trattano, compresi quelli di natura personale.

La sicurezza informatica si pone, pertanto, presupposto imprescindibile per un'effettiva protezione dei dati personali: in assenza di adeguate misure tecniche e organizzative, il diritto alla riservatezza e all'autodeterminazione

---

[17] Il riferimento è all'art. 32 del Regolamento 2016/679/UE "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

informativa rischierebbe di rimanere meramente teorico. Al contempo, il regime di protezione dei dati incide in modo significativo sulla conformazione degli obblighi di sicurezza, imponendo standard sempre più elevati di prevenzione, gestione e risposta agli incidenti informatici con rilevanti ricadute sull'operatività degli attori pubblici e privati.

Sul piano tecnico-operativo, tale relazione si manifesta attraverso l'impiego di strumenti e processi comuni, dalla crittografia ai sistemi di controllo degli accessi, fino alla gestione delle vulnerabilità e degli incidenti di sicurezza.[18]

Il rapido sviluppo delle tecnologie digitali e delle reti ha condotto alla creazione di un ecosistema caratterizzato da un flusso continuo e massivo di dati, la cui velocità e ampiezza di circolazione risultano sempre più difficilmente controllabili.[19]

I dati stessi sono oggi considerati uno dei beni più strategici e, proprio per tale ragione, rappresentano un obiettivo privilegiato delle violazioni in materia di sicurezza informatica.

Si assiste, pertanto, a un incremento esponenziale della superficie di attacco con effetti profondi sulla politica, sull'economia e sulla società.

---

[18] S. CALÌ, F. CAPPARELLI, M. HAZAN, F. MARTINI, in *Cybersecurity: tra rischio e responsabilità. Profili operativi in continua evoluzione,* Giuffrè Editore, 2025, pp. 139-142.

[19] D.U. GALLETTA, in *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini?* in "*Ciberspazio e diritto*", 2018, 3, p. 327.

L’uso improprio dei dati personali comporta inevitabilmente una compressione dei diritti e delle libertà fondamentali dell’individuo, esponendolo ai rischi tipici della società digitale.[20]

Da ciò discende l’esigenza di definire regole, strumenti e modelli organizzativi idonei a garantire una protezione effettiva dei dati contro accessi non autorizzati e condotte malevole.[21]

Il rapporto tra cybersecurity e protezione dei dati non è dunque di natura concorrenziale bensì complementare. Entrambi costituiscono pilastri di un medesimo sistema di garanzia, fondato su resilienza tecnologica, organizzativa e giuridica, all’interno di un ecosistema digitale complesso, secondo un rapporto di sinergia e di reciproco bilanciamento in costante evoluzione.[22]

Tale interazione assume, infine, una dimensione multilivello nella quale norme europee, nazionali e strumenti di *soft law* concorrono alla definizione di obblighi, responsabilità e assetti organizzativi che riflettono, da un lato, la

---

[20] E. SORRENTINO, A.F. SPAGNUOLO, in *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in *Rivista italiana di informatica e diritto,* p. 690.

[21] R. FLOR, in *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA- Triad Protection ai più recenti sviluppi,* in *Diritto di Internet*, 2019, 3, p. 5

[22] Sul punto, si veda B. PONTI, in *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi,* in *Rivista italiana di informatica e diritto,* 2024.

centralità del diritto fondamentale alla protezione dei dati personali e, dall'altro, la necessità di garantire la resilienza [23] complessiva del cyberspazio.

2. L'evoluzione normativa europea: le coordinate di riferimento

L'Unione europea ha significativamente inciso sulla ridefinizione concettuale della cybersecurity, trasformandola da mera dimensione tecnica di protezione delle infrastrutture digitali a elemento strutturale della governance del digitale e della tutela dei diritti fondamentali. [24]

L'evoluzione normativa europea in materia di protezione dei dati personali e di sicurezza informatica rappresenta uno dei processi più significativi nel progressivo consolidamento di un ecosistema digitale fondato sulla tutela dei diritti fondamentali e sulla resilienza delle infrastrutture informatiche.

L'Unione europea, nel corso degli ultimi vent'anni, ha elaborato un *corpus* regolatorio articolato e in costante aggiornamento, volto a far fronte alle sfide generate dall'innovazione tecnologica, dalla crescente interconnessione dei sistemi e dall'emersione di nuovi rischi digitali di portata transnazionale.

Ricostruire le coordinate di tale evoluzione significa non soltanto individuare i principali interventi legislativi che hanno scandito la formazione dell'attuale quadro regolatorio, ma anche comprendere le logiche sottese all'azione

---

[23] Per il concetto di resilienza si veda P.G. CHIARA, R. BRIGHI, in *La dimensione della "resilienza" nel diritto UE della cybersicurezza*, in *Rivista Web- Il Mulino*, 2, 2024, pp. 405 e ss.

[24] R. BRIGHI, P.G. CHIARA, *op.cit.*, p. 23.

normativa dell'Unione, orientata alla definizione di standard minimi comuni, al rafforzamento delle responsabilità degli operatori e alla protezione effettiva dei diritti degli interessati.

Il presente paragrafo si propone, pertanto, di analizzare le tappe essenziali del percorso evolutivo europeo, evidenziandone gli snodi concettuali, gli obiettivi strategici e le implicazioni sistemiche, in un contesto caratterizzato da un crescente intreccio tra regolazione, tecnologia e sicurezza.

Proprio in ragione della complessità intrinseca del fenomeno, la definizione di cybersecurity a livello europeo rappresenta l'esito di un processo evolutivo lungo e stratificato, maturato attraverso decenni di progressiva attenzione dell'Unione alle sfide poste dalla trasformazione digitale.

La prima misura a livello europeo in materia risale al 2001, con la Comunicazione sulla criminalità informatica in cui la sicurezza delle reti e dell'informazione ove la cybersecurity veniva intesa "*come la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema*".

Emergeva già vent'anni fa che la sicurezza stava divenendo un settore prioritario in considerazione del fatto "*che le comunicazioni e le informazioni sono ormai fattori determinanti dello sviluppo economico e sociale. Le reti e i sistemi di informazione veicolano un volume e una pluralità di servizi e dati*

ancora inconcepibili fino a pochi anni fa. La loro disponibilità è essenziale per altre infrastrutture quali la rete idrica e la rete elettrica. Poiché tutti, dall'impresa al cittadino privato, alla pubblica amministrazione, desiderano avvalersi delle possibilità offerte dalle reti di comunicazione, la sicurezza di tali sistemi diventa un presupposto essenziale per ulteriori progressi.".[25]

A partire da quel momento, l'Unione europea ha progressivamente fatto ricorso a politiche dedicate e interventi normativi mirati sempre più consistenti per rafforzare il proprio livello di "ciberresilienza".

Il significativo aumento del numero e della gravità degli attacchi e degli incidenti informatici ha determinato, a partire dal 2013, un'intensificazione dell'azione europea nel settore. Parallelamente, gli Stati membri hanno adottato o aggiornato le proprie strategie nazionali di cibersicurezza, avviando percorsi di allineamento con gli standard delineati a livello unionale.[26]

In questa direzione, il punto di svolta è rappresentato dal documento "*Cybersecurity Strategy*" ("Strategia dell'Unione europea per la cybersecurity") con cui l'UE ha definito gli obiettivi e le azioni concrete per

---

[25] COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE E AL COMITATO DELLE REGIONI. Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo, in *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:IT:PDF*

[26] *Le sfide insite in un'efficace politica dell'UE in materia di cybersicurezza*, ECA, 2019, in *https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_it.pdf*

raggiungere la resilienza, per ridurre il cybercrime, per sviluppare politiche, capacità di difesa informatica, risorse industriali e tecnologiche e stabilire una politica internazionale coerente per il cyberspazio, evidenziando il ruolo centrale dei diritti e delle libertà fondamenti nella regolamentazione della materia.

Tuttavia, nonostante i progressi compiuti e l'avvio di un percorso sempre più strutturato, nella fase iniziale l'azione dell'Unione europea in materia di cibersicurezza e protezione dei dati non aveva ancora dato luogo ad un quadro regolatorio compiuto e armonico.

Le prime iniziative, se pur significative, erano caratterizzate da un approccio prevalentemente settoriale e frammentato.

Proprio l'assenza di una disciplina organica e coordinata ha reso necessaria l'adozione di nuovi strumenti normativi che hanno progressivamente consolidato un vero e proprio sistema europeo di regolazione della cybersicurezza.

In tale prospettiva, particolare rilievo assumono le Direttive, quale primo tentativo di armonizzazione minima, e il successivo Regolamento che segna un salto qualitativo nella costruzione di un quadro uniforme e vincolante.

È a questi atti, e alle loro ricadute sull'assetto complessivo della governance europea del digitale, che si dedica la parte che segue.

2.1.Dalla Direttiva NIS al Cybersecurity Act

La marcata accelerazione dei processi di digitalizzazione, intensificata dall'emergenza pandemica da Covid-19, e l'emersione di nuove e sempre più sofisticate minacce informatiche, ha imposto all'Unione europea la necessità di intraprendere una profonda trasformazione del proprio approccio alla sicurezza del cyberspazio.

La prima normativa organica in materia di sicurezza delle reti e dei sistemi informativi è stata la Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, nota con l'acronimo NIS (Network Information System) la quale ha introdotto un insieme di regole rivolte alle organizzazioni che possiedono caratteristiche di criticità sotto il profilo della cybersecurity.

Più nel dettaglio, la NIS rappresenta il primo tentativo dell'Unione di rafforzare il livello complessivo di cybersicurezza tra gli Stati membri e di definire una base comune di garanzie destinate a sviluppare un ecosistema di fiducia.

Essa attribuisce un ruolo primario agli Operatori dei Servizi Essenziali (OSE), ossia quelle aziende che forniscono un servizio fondamentale, la cui eventuale interruzione avrebbe un impatto significativo sull'andamento dell'economia o della società in termini di rischi. [27]

Per cogliere la *ratio* innovatrice dell'intervento comunitario, si riportano qui di seguito i Considerando nn. 1) 2) e 3) ove è previsto che "*Le reti e i sistemi e*

[27] La definizione degli OSE è quella fornita dall'Anssi (National Cybersecurity Agency of France).

servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno. La portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. Tali sistemi possono inoltre diventare un bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi. Tali incidenti possono impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione. Le reti e i sistemi informativi, e in prima linea internet, svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone. Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi, intenzionali o meno e indipendentemente dal luogo in cui si verificano, possono ripercuotersi su singoli Stati membri e avere conseguenze in tutta l'Unione. La sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno".[28]

Nasce l'esigenza di un approccio globale a livello europeo che statuisca regole ed obblighi comuni, funzionali all'incremento della cooperazione in tale settore e alla definizione di una "*capacità minima comune e disposizioni minime in*

[28] Per il testo della Direttiva UE 2016/1148 si veda *https://eur-lex.europa.eu/eli/dir/2016/1148/oj/ita/pdf.*

materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza." [29]

I settori ricompresi nell'ambito di applicazione della Direttiva NIS riguardano l'energia, i trasporti, le banche, i mercati finanziari, la sanità, la fornitura e la distribuzione di acqua potabile, le infrastrutture digitali, i motori di ricerca, i servizi cloud e le piattaforme di commercio elettronico, ferma restando la possibilità per gli Stati membri di estendere l'ambito di applicazione delle proprie disposizioni anche ad ulteriori settori.

Una delle principali novità introdotte è costituita dall'ampliamento del concetto di "infrastruttura critica" mediante la teorizzazione di due categorie di operatori potenzialmente idonei a compromettere la continuità dei servizi essenziali dei Paesi in caso di incedente cibernetico: gli OSE (Operatori di Servizi Essenziali) e i FSD (Fornitori di Servizi Digitali). Tali soggetti sono tenuti a adottare un approccio *risk-based*, in armonia con gli standards internazionali e con le normative in materia di cybersecurity e data protection.[30]

La Direttiva individua, inoltre, le autorità competenti incaricate di garantire l'effettività delle misure di sicurezza, tra cui un'autorità nazionale competente,

[29] Considerando 6 della Direttiva UE 2016/1148 in *https://eur-lex.europa.eu/eli/dir/2016/1148/oj/ita/pdf.*

[30] In particolare, agli standards internazionali elaborati dalle Organizzazioni più rilevanti, quali ISO e NIST.

un punto di contatto unico e i Computer Security Incident Response Team (CSIRT).[31]

A tal fine viene istituita una rete europea di CSIRT allo scopo di promuovere una cooperazione rapida ed efficace, con il supporto dell'ENISA e la partecipazione della Commissione europea in qualità di osservatore.[32]

La Direttiva consente poi agli Stati membri di adottare o mantenere in vigore disposizioni atte a conseguire un livello più elevato di sicurezza della rete e dei sistemi informativi.[33]

Particolare rilievo assume l'istituzione del cd gruppo di cooperazione, previsto dall'art. 11 della Direttiva, funzionale a "*sostenere e agevolare la cooperazione strategica e lo scambio di informazioni fra Stati membri, di sviluppare la fiducia e nell'ottica di conseguire un livello comune elevato di sicurezza delle reti e dei servizi informativi nell'Unione*".

Il capo IV della Direttiva è dedicato invece a tutti gli "obblighi in materia di sicurezza e notifica degli incidenti". Viene imposta agli OSE e ai FSD

---

[31] Si vedano artt. 8 e 9 della Direttiva UE 2016/1148 in *https://eur-lex.europa.eu/eli/dir/2016/1148/oj/ita/pdf.*

[32]Art. 12 della Direttiva UE 2016/1148.

[33] Dal 2012, infatti, l'ENISA sostiene gli Stati nello sviluppo, nell'attuazione e nella valutazione delle loro strategie nazionali in materia di cybersicurezza. Si veda, in tal senso, *«National Cybersecurity Strategies (NCSSs) Map», Topic, ENISA, https://www.enisa.europa.eu/topics/national-cyber- security-strategies/ncss-map.*

l'adozione di misure tecniche ed organizzative adeguate e proporzionate alla gestione dei rischi posti dalla sicurezza delle reti e dei sistemi informativi, nonché l'obbligo di notificare tempestivamente gli incidenti di maggiore impatto alle autorità competenti o ai CSIRT.

Pur rappresentando un significativo punto di svolta nella disciplina della sicurezza informatica delle infrastrutture critiche, la Direttiva NIS ha mostrato significativi limiti strutturali in ragione dell'elevato grado di discrezionalità riconosciuto agli Stati membri.

Cò ha determinato una frammentazione dei regimi nazionali con disomogeneità nell'attuazione degli obblighi e dei livelli di protezione.

Alla luce di tali criticità, nel dicembre 2020 la Commissione europea ha presentato una nuova proposta normativa, culminata nell'adozione della Direttiva (UE) 2022/2555, nota come Direttiva NIS2 [34], volta a rafforzare l'omogeneità, il rigore e la resilienza del quadro europeo in materia di cybersicurezza.

La NIS2 persegue l'obiettivo di rafforzare la resilienza operativa e la sicurezza delle reti e dei sistemi informativi all'interno dell'Unione europea, in armonia con i principi sanciti dall'art. 114 TFUE circa l'adozione di misure volte al miglioramento del mercato interno, includendo la sicurezza dei servizi digitali che vi operano.

---

[34] Si veda Direttiva UE 2555/2022 in *https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=it*

Tra le innovazioni di maggior rilievo, senza pretesa di esaustività, la Direttiva NIS2 introduce un significativo ampliamento dell'ambito soggettivo di applicazione (artt. 2–3), estendendo gli obblighi di cybersicurezza a un numero più ampio di settori considerati "critici" o "ad alta criticità", quali energia, trasporti, sanità, infrastrutture digitali, pubblica amministrazione, servizi ICT gestiti, produzione di dispositivi critici e altri comparti essenziali per il funzionamento dell'economia e della società.

Sul piano istituzionale, la NIS2 nel capo VI rafforza i poteri delle autorità nazionali competenti attribuendo loro strumenti incisivi in termini di vigilanza, poteri ispettivi, richieste di informazioni e capacità sanzionatorie. Essa potenzia anche la cooperazione transfrontaliera mediante la creazione del Cyber Crisis Liaison Organisation Network (EU-CyCLONe) (art. 16), concepito per agevolare la gestione coordinata delle crisi cibernetiche su larga scala.

Un'altra innovazione strutturale consiste nella eliminazione della distinzione precedentemente introdotta tra "operatori di servizi essenziali" e "fornitori di servizi digitali": la NIS2 unifica tali categorie e opera una differenziazione basata esclusivamente sulla classificazione in soggetti essenziali e soggetti importanti (artt. 3–4).[35]

[35] Considerando 6 della Direttiva UE 2555/2022 si legge "In particolare, la presente direttiva mira a superare le carenze della differenziazione tra gli operatori di servizi essenziali e i fornitori di servizi digitali, che si è rivelata obsoleta, in quanto non riflette l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno."

La Direttiva NIS2 prevede poi specifiche misure di gestione dei rischi di cybersicurezza per i soggetti essenziali (art. 21).

Tra queste si concentra sulla sicurezza della cd *supply chain* e cioè sulla sicurezza della catena di approvvigionamento in cui ricomprende anche aspetti relativi ai rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi. Si tratta di un punto di svolta significativo, poiché riconosce il ruolo sistemico dei rischi derivanti da terze parti nella costruzione della resilienza complessiva.

L'art. 20 ("Governance") definisce inoltre ruoli, obblighi e responsabilità con particolare riferimento agli organi di direzione, chiamati a garantire un adeguato livello di supervisione strategica e a rispondere, anche personalmente, in caso di inadempimento delle misure previste dalla Direttiva.

La Direttiva NIS2 rafforza, inoltre, il ruolo del c.d. gruppo di cooperazione (art. 14) e dell'ENISA, ampliandone le funzioni di coordinamento e di supporto tecnico e attribuendo all'Agenzia una posizione centrale nello sviluppo di metodologie comuni, nell'analisi delle minacce, nei programmi di formazione e nella definizione di standard tecnici condivisi.

Infine, in materia sanzionatoria, si realizza un'innovazione profonda. Mentre la Direttiva 2016/1148 demandava pressoché integralmente agli Stati membri la definizione delle sanzioni, questa stabilisce parametri minimi armonizzati e livelli massimi delle sanzioni amministrative pecuniarie (art. 34), introducendo

un sistema più severo e maggiormente coerente con il modello sanzionatorio già sperimentato in altri atti dell'Unione, come il GDPR.

L'evoluzione normativa culminata nella NIS2, qui brevemente esposta, ha evidenziato tuttavia come le sole direttive, pur fondamentali, non garantiscano un livello di uniformità soddisfacente.

Infatti, a differenza dei regolamenti, le direttive non sono immediatamente applicabili e non obbligatorie in tutti i loro elementi negli Stati membri.

Per tale ragione si è giunti all'adozione del Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.[36]

Il Cybersecurity Act, ossia il Regolamento (UE) 2019/881, si struttura in due sezioni fondamentali, entrambe finalizzate al rafforzamento dell'architettura europea di cybersicurezza.

La prima parte del Regolamento interviene sul ruolo dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA), conferendole un mandato permanente (art. 4) e potenziandone in modo significativo le competenze. ENISA non svolge più soltanto una funzione consultiva o di supporto tecnico-specialistico ma assume anche un ruolo operativo nella prevenzione, individuazione e gestione delle minacce cibernetiche, nella raccolta e condivisione di

[36] Si veda, in proposito, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881*

informazioni rilevanti e nel coordinamento delle risposte, in collaborazione con gli Stati membri e con le istituzioni dell'Unione.

La seconda parte del Regolamento introduce un quadro europeo comune di certificazione della cybersicurezza per prodotti ICT, servizi digitali e processi connessi. L'obiettivo perseguito è garantire un livello elevato e uniforme di sicurezza, volto a tutelare la disponibilità, l'integrità, la riservatezza e l'autenticità dei dati e, più in generale, delle funzioni e dei servizi erogati tramite tecnologie dell'informazione e della comunicazione.

Il sistema europeo di certificazione è concepito per ridurre la frammentazione normativa, favorire la fiducia degli utenti e agevolare la circolazione dei prodotti ICT nel mercato interno.[37]

In particolare, sono previsti schemi di certificazione predisposti dall'ENISA, adottati mediante atti di esecuzione da parte della Commissione europea e pubblicati sul sito web dell'ENISA (artt. 47-50 Reg.to UE 2019/881).

Un elemento di rilievo, ai sensi dell'art. 56, è rappresentato dal carattere volontario della certificazione europea della cybersicurezza, fatta salva l'eventuale previsione di obblighi derivanti dal diritto dell'Unione o da disposizioni nazionali adottate in conformità allo stesso.

---

[37] S. CALÌ, F. CAPPARELLI, M. HASSAN, F. MARTINI, *op.cit.,* p. 58.

Gli schemi europei di certificazione sono destinati a sostituire gli schemi nazionali a decorrere dalla data indicata nell'atto di esecuzione relativo a ciascuno schema, secondo quanto previsto dall'art. 57.

L'*excursus* normativo delineato riflette chiaramente le coordinate entro cui si sviluppa la disciplina europea della cybersicurezza, evidenziando un percorso di progressiva integrazione, armonizzazione e rafforzamento istituzionale.

La Strategia dell'UE per la cybersicurezza del 2013 rappresenta il primo documento organico in cui viene riconosciuta la necessità per l'Unione di promuovere e rafforzare la ciberresilienza come elemento strategico per il corretto funzionamento del mercato interno e per la tutela degli interessi economici e sociali degli Stati membri. In questa fase iniziale, l'attenzione dell'Unione è rivolta principalmente alla sicurezza delle reti e dei sistemi informativi, con un approccio prevalentemente tecnico-infrastrutturale e con l'obiettivo di predisporre un quadro minimo di protezione e cooperazione tra gli Stati membri.[38]

Un'evoluzione significativa si registra con la Strategia del 2017[39]che adotta un approccio multilivello, riconoscendo come la cybersicurezza non costituisca soltanto una questione tecnica, ma una sfida sociale condivisa, che coinvolge

---

[38] Commissione europea e Alto Rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza 2013 in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013JC0001*

[39] Commissione europea e Alto Rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza 2017 in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017JC0450*

istituzioni, imprese, cittadini e operatori privati. In tale quadro, l'attenzione si sposta progressivamente dal mero rafforzamento delle reti alla centralità del coordinamento istituzionale europeo, accompagnato da un potenziamento strutturale del ruolo dell'ENISA e da una più intensa cooperazione a livello sovranazionale.

La Strategia dell'UE per la cybersicurezza del 2020, infine, amplia ulteriormente l'orizzonte dell'azione europea, integrando alla dimensione tecnica il rafforzamento delle capacità industriali e tecnologiche, la sicurezza della catena di approvvigionamento e, più in generale, la protezione dell'intero ecosistema socioeconomico e digitale europeo. L'attenzione si estende ai prodotti ICT, alle tecnologie emergenti, ai servizi digitali e ai rischi connessi alle dipendenze strategiche esterne, riconoscendo la cybersicurezza come componente essenziale dell'autonomia strategica dell'Unione e della sua capacità competitiva nello scenario globale.[40]

La ricostruzione delle principali strategie e degli interventi normativi dell'Unione europea consente di individuare chiaramente le coordinate entro cui si sviluppa la disciplina europea della cybersicurezza: un percorso di progressiva integrazione, armonizzazione e rafforzamento istituzionale, con una crescente consapevolezza dell'Unione circa la necessità di strumenti normativi sempre più uniformi e direttamente applicabili.

---

[40] P.G. CHIARA, R. BRIGHI, op.cit., pp. 413 e ss.

Ciò testimonia l'evoluzione da un modello basato sulla cooperazione tra Stati membri a un sistema che tende verso un *corpus* normativo europeo, capace di rispondere in modo efficiente a minacce transnazionali che, per loro natura, non conoscono confini.

Le coordinate così delineate costituiscono dunque la base imprescindibile per comprendere la *ratio* e la direzione del legislatore europeo e per analizzare, nei capitoli successivi, gli strumenti normativi emergenti che compongono il mosaico della sicurezza cibernetica nell'ordinamento dell'Unione.

2.2.Il quadro normativo italiano

Negli ultimi anni anche il legislatore italiano ha progressivamente intensificato gli interventi in materia di cybersecurity, in risposta ad un contesto caratterizzato da una digitalizzazione pervasiva e da un incremento delle minacce informatiche, che impongono strumenti giuridici sempre più sofisticati.

L'attenzione al tema nasce certamente da esigenze interne, ma è stata significativamente rafforzata e guidata dalle iniziative dell'Unione europea volte a creare uno spazio digitale più sicuro e resiliente.

Tale dinamica multilivello ha prodotto un insieme di norme che si integrano con gli standard europei, delineando un modello di sicurezza cibernetica complesso e in continua evoluzione.

Le prime misure, adottate a partire dal 2013, hanno posto le basi di un coordinamento istituzionale volto alla tutela delle infrastrutture critiche,

anticipando un sistema che sarebbe divenuto progressivamente più strutturato. Un passaggio decisivo si è realizzato con il recepimento della Direttiva NIS mediante il d.lgs. 65/2018 [41] che, per la prima volta, ha introdotto obblighi puntuali di sicurezza e di notifica degli incidenti per gli operatori di servizi essenziali e per i fornitori di servizi digitali, orientando anche gli attori privati a una gestione del rischio cibernetico sistematica.

Un ulteriore intervento di rilievo è rappresentato dalla disciplina del Perimetro di sicurezza nazionale cibernetica, introdotta dal d.l. n. 105/2019, convertito con modificazioni dalla l. n. 133/2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, nonché dal d.P.C.M. n. 131/2020, pubblicato nella Gazzetta Ufficiale del 21 ottobre 2020.[42]

Tale disciplina segna un punto di svolta per il nostro ordinamento poiché la sicurezza cibernetica non è più considerata solo una questione tecnica ma un presidio strategico di rilevanza nazionale, regolato da procedure vincolanti e controlli istituzionali.

Il PSNC mira a rafforzare il livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici dal cui corretto funzionamento dipende l'esercizio di funzioni e servizi essenziali dello Stato. A tal fine, la normativa

---

[41]Per il testo ufficiale si veda in *https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;65*

[42]Per il testo ufficiale si veda in *https://www.gazzettaufficiale.it/eli/gu/2019/11/20/272/sg/pdf*

impone specifici obblighi a carico di amministrazioni pubbliche, enti e operatori pubblici e privati, con sede nel territorio nazionale, che svolgono funzioni o servizi essenziali e il cui malfunzionamento o utilizzo improprio dei sistemi informatici potrebbe arrecare un pregiudizio alla sicurezza nazionale.

Un altro passaggio importante si registra con l'adozione del d.l. 14 giugno 2021 n. 82 recante *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*. Per la prima volta il legislatore fornisce una definizione di cybersicurezza nazionale intesa come "*l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico*." [43] Questo percorso è stato infine consolidato con la creazione dell'Agenzia per la Cybersicurezza Nazionale alla quale è affidato il compito di coordinare la strategia nazionale, sovrintendere alla prevenzione e alla risposta agli incidenti

[43] Art. 1, co. 1, lett. a) del d.l. 82/2021 *in https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14;82*

e a rappresentare il punto di raccordo con gli strumenti europei di regolazione (art. 5 d.l. 82/2021).

L'allineamento con gli standards sovranazionali è divenuto ancora più evidente con l'emanazione del d.lgs. 138/2024[44] attuativo della Direttiva NIS2.

Il decreto ha ampliato il novero dei soggetti obbligati, rafforzando i requisiti organizzativi e tecnici e introducendo un modello più rigoroso di gestione del rischio in armonia con l'obiettivo europeo di innalzare il livello complessivo di sicurezza del mercato interno.

In particolare, esso attribuisce un ruolo centrale alla Agenzia per la cybersicurezza nazionale dotandola di poteri di intervento, definisce obblighi specifici in capo ai soggetti essenziali ed importanti, introduce rigorosi meccanismi di notifica, istituisce un sistema di controllo articolato e costruisce un sistema sanzionatorio più incisivo.

L'insieme di tali interventi normativi è volto alla prevenzione e alla gestione dei rischi informatici e alla costruzione di un quadro regolatorio improntato alla responsabilizzazione e alla consapevolezza dei soggetti coinvolti. [45]

---

[44] Per il testo si veda in *https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-04;138*

[45] S. CALÌ, F. CAPPARELLI, M. HAZAN, F. MARTINI, *op. cit.*, pp. 139-142

I successivi provvedimenti attuativi e le Linee Guida emanate dall'ACN hanno ulteriormente precisato obblighi, schemi di certificazione e misure di conformità, completando un impianto che oggi si presenta complesso.

Questo processo testimonia come l'Italia abbia progressivamente maturato un approccio integrato alla sicurezza cibernetica nel quale le spinte europee e le esigenze interne si combinano per definire un sistema normativo robusto e orientato alla prevenzione dei rischi digitali.

Come già osservato con riferimento alla dimensione europea, anche nel contesto nazionale, la cybersicurezza emerge come il risultato della compenetrazione di due anime: da un lato, quella tecnico-operativo della sicurezza informatica; dall'altro, quella di carattere giuridico-politico, che la colloca tra le attività dirette a tutelare la sicurezza e in generale l'interesse della Nazione.[46]

In questa prospettiva, parte della dottrina ha evidenziato come la cybersicurezza nazionale non coincida pienamente con la più ampia nozione di sicurezza nazionale, pur costituendone una componente essenziale almeno con riferimento ai beni e ai servizi informatici.[47]

---

[46] M.A. RIZZI, F. SERINI, in *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista Italiana di Informatica e Diritto*, 2/2024, pp. 123-125-

[47] A. PANSA, in *La sicurezza nazionale. Innovazione e nuovi limiti,* in *Gnosis,* 2019, n. 1.

Il richiamo espresso alla tutela della sicurezza nazionale nel dominio cibernetico conferma, in ogni caso, una crescente attenzione del legislatore e del Governo verso questa area strategica.

2.3.Il ruolo del GDPR nella sicurezza informatica

Si è già analizzata l'interconnessione tra la cybersecurity e la protezione dei dati personali. Tuttavia, per approfondire ulteriormente tale rapporto, è opportuno soffermarsi sul già citato Regolamento (UE) 2016/679 (GDPR – General Data Protection Regulation), definito "*come la prima e più importante risposta che il diritto abbia espresso nei confronti della rivoluzione digitale.*"[48]

Il GDPR persegue, tra i suoi obiettivi essenziali, l'armonizzazione a livello europeo della disciplina concernente la tutela dei dati personali e la definizione di strumenti normativi capaci di rispondere in modo efficace alle nuove sfide imposte dai processi di digitalizzazione e dall'evoluzione tecnologica.

In tale prospettiva, il Regolamento rappresenta uno dei pilastri fondamentali anche nell'evoluzione del quadro europeo della cybersicurezza poiché integra in modo sistematico la protezione dei dati personali con la sicurezza dei sistemi informativi.

La logica del GDPR si fonda su due principi cardine: il principio di accountability e il principio di privacy by design e by default.

---

[48] Così il Garante per la protezione dei dati personali nella sua intervista *Barriera Ue contro il Far West dei dati* pubblicata in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9108780*

In virtù del principio di accountability, il titolare del trattamento è tenuto ad adottare politiche e misure adeguate non solo a garantire, ma anche a dimostrare che il trattamento dei dati personali è conforme alle disposizioni del Regolamento.[49]

Il principio di privacy by design e by default, a sua volta, impone al titolare del trattamento l'implementazione di misure tecniche e organizzative idonee ad assicurare un'effettiva protezione dei dati personali fin dalla progettazione del trattamento e per impostazione predefinita. Nella definizione di tali misure, il titolare è chiamato a tener conto di una pluralità di fattori, tra cui lo stato dell'arte, i progressi tecnologici, i costi di attuazione, nonché la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, valutando i rischi che esso comporta, in termini di probabilità e gravità, per i diritti e le libertà delle persone fisiche.[50]

---

[49] L'art. 24 Reg. UE 2016/679 in particolare statuisce che "1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento."

[50] Art. 25 Reg. UE 2016/679

Ne deriva un approccio *risk-based* con una valutazione del rischio che deve essere fatta sin dalle fasi iniziali di progettazione dei processi e dei sistemi informativi.

L'interconnessione crescente tra cybersecurity e *data protection* emerge altresì nel dialogo normativo tra GDPR e la Direttiva NIS2 che, pur disciplinando ambiti distinti, presentano evidenti punti di contatto.

A tal proposito, si sottolinea che un attacco informatico diretto a sistemi considerati "critici" può facilmente tradursi in un illecito trattamento di dati personali con conseguente compromissione dei diritti e delle libertà fondamentali degli utenti-cittadini.

Tale circostanza rende indispensabile che i soggetti gestori di tali infrastrutture procedano a una revisione approfondita delle misure di sicurezza adottate, valutando l'esigenza di modulare i livelli di tutela in funzione della natura, della sensibilità e del valore informativo dei dati trattati. [51]

Ne emerge, pertanto, il ruolo del GDPR quale componente strutturale di un ecosistema regolatorio nel quale la protezione dei dati non rappresenta soltanto un fine da perseguire, ma si configura come un vero e proprio strumento di

[51] V. AMENTA, R. DELUCA, in *L'approccio alla cybersecurity nello scenario normativo europeo*, in *La Comunicazione – Note, Recensioni e Notizie n. 68*, 2024, p. 9.

sicurezza, funzionale a garantire la resilienza, la continuità operativa e l'affidabilità delle infrastrutture digitali. [52]

2.4.Il Cyber Resilience Act

Nel delineare una panoramica degli interventi più significativi in materia di cybersicurezza assume rilievo centrale il Cyber Resilience Act (c.d. CRA), ossia il Regolamento (UE) 2024/2847, adottato dal Parlamento europeo e dal Consiglio il 23 ottobre 2024, che introduce requisiti di cybersicurezza di carattere orizzontale per i prodotti dotati di elementi digitali. [53]

L'iniziativa normativa, finalizzata a definire un quadro armonizzato di tutela per l'intero ecosistema dei servizi e dei prodotti digitali nell'Unione, muove dalla consapevolezza che la carenza di adeguati standard di sicurezza informatica nei dispositivi connessi costituisce un fattore di rischio anche per la protezione degli operatori economici e degli utenti.[54]

---

[52] Sul rapporto tra GDPR e sicurezza informatica, si veda P. VOIGT, in *The EU General Data Protection Regulation (GDPR)*, Springer, 2017, pp. 123-145.

[53] Il Regolamento UE 2024/2847 si applicherà in tutti gli Stati Membri a partire dall'11 dicembre 2027. Per il testo si veda in *https://www.acs.it/it/blog/sicurezza-informatica/cyber-resilience-act/*

[54] Considerando 1 Reg. UE 2024/2847: "La cibersicurezza è una delle sfide principali per l'Unione. Il numero e la varietà dei dispositivi connessi aumenteranno esponenzialmente nei prossimi anni. Gli attacchi informatici costituiscono una questione di interesse pubblico dal momento che hanno un impatto determinante non solo sull'economia dell'Unione, ma anche sulla democrazia, nonché sulla sicurezza dei consumatori e sulla salute. Occorre pertanto rafforzare l'approccio dell'Unione alla cibersicurezza, occuparsi della ciberresilienza a livello dell'Unione nonché migliorare il funzionamento del mercato interno, definendo un quadro giuridico uniforme per i requisiti essenziali di cibersicurezza per l'immissione sul mercato dell'Unione di prodotti con elementi

La sicurezza di tali prodotti, infatti, risulta indissolubilmente legata alla dimensione della *safety*, intesa come salvaguardia dell'integrità fisica e della vita umana rispetto a potenziali pericoli derivanti da vulnerabilità digitali. [55]

Prima dell'elaborazione del CRA, il quadro normativo europeo in materia di sicurezza dei prodotti si presentava fortemente frammentato e dominato da un'impostazione di tipo verticale e basata su discipline settoriali eterogenee.

Tale configurazione generava sovrapposizioni normative e contribuiva a una crescente disomogeneità ed incertezza giuridica nel mercato interno. [56]

Il Cyber Resilience Act, invece, si distingue per l'adozione di un approccio trasversale, intervenendo in modo unitario su tutti i prodotti che incorporano elementi digitali e introducendo obblighi omogenei in materia di cybersicurezza.

---

digitali. È opportuno affrontare i due problemi principali che comportano ulteriori costi per gli utilizzatori e la società: un basso livello di cibersicurezza dei prodotti con elementi digitali, testimoniato da vulnerabilità diffuse e dalla fornitura insufficiente e incoerente di aggiornamenti di sicurezza per porvi rimedio così come un'insufficiente comprensione delle informazioni e un accesso limitato alle stesse da parte degli utilizzatori, che impediscono loro di scegliere prodotti con proprietà di cibersicurezza adeguate o di utilizzarli in modo sicuro."

[55] M. DURANTE, in *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks,* in M.V. D'ALFONSO, *"On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence"*, Springer, 2019, p. 372.

[56] P. G. CHIARA, in *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali,* in *Rivista italiana di informatica e diritto,* fasc. 1-2023, p. 144.

In tal modo, il legislatore europeo mira ad assicurare un livello minimo e uniforme di protezione all'interno del mercato unico, riducendo le incoerenze normative e favorendo una cornice regolatoria maggiormente coerente e integrata.

In particolare, il Regolamento si applica ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati, logica o fisica, diretta o indiretta, a un dispositivo o a una rete.[57]

Attraverso una definizione ampia, il Regolamento qualifica come "prodotto con elementi digitali" qualsiasi prodotto software o hardware, nonché le relative soluzioni di elaborazione dati da remoto, includendo anche i componenti software o hardware immessi sul mercato separatamente.[58]

Il CRA adotta un approccio *risk based.* [59]

I prodotti con elementi digitali possono essere immessi sul mercato soltanto se soddisfano i requisiti essenziali di cybersicurezza di cui all'allegato I, parte I, e a condizione che siano correttamente installati, adeguatamente mantenuti e utilizzati conformemente alla loro finalità prevista o in condizioni ragionevolmente prevedibili, nonché che siano stati installati i necessari

---

[57] Art. 2 (Ambito di applicazione), par.1, Reg. UE 2024/2847.

[58] Art. 3 (Definizioni), n.1), Reg. UE 2024/2847.

[59] G. DE GREGORIO. P. DUNN, in *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, vol. 59, 2022, n.2, pp. 473 e ss.

aggiornamenti di sicurezza. Parallelamente, i processi adottati dal fabbricante devono essere conformi ai requisiti essenziali di cybersicurezza di cui all'allegato I, parte II (art. 6 Reg. UE 2024/2847).

Inoltre, in considerazione del livello di rischio, i prodotti vengono classificati in "prodotti con elementi digitali importanti" o "prodotti con elementi digitali critici". La distinzione tra le due tipologie è da rinvenirsi principalmente nella diversa procedura di valutazione della conformità a cui il prodotto deve essere sottoposto.

Un ulteriore profilo che evidenzia la natura orizzontale del Cyber Resilience Act concerne la pluralità dei soggetti coinvolti negli obblighi previsti dal Regolamento. Il CRA estende in modo sistematico la disciplina dell'Unione all'intera catena di fornitura dei prodotti con elementi digitali, includendo espressamente fabbricanti gestori, importatori e distributori, secondo un modello di governance che mira a responsabilizzare tutti gli operatori economici che concorrono all'immissione del prodotto sul mercato.[60]

Questa impostazione segna una significativa discontinuità rispetto al quadro previgente, nel quale gli operatori economici erano spesso destinatari soltanto di raccomandazioni, linee guida o *best practices* in materia di cybersicurezza, strumenti per loro natura non vincolanti e incapaci di assicurare un livello di protezione uniforme.

---

[60] Artt. 13 e ss, Reg. UE 2024/2847.

Tale assetto aveva prodotto un evidente *deficit* di sicurezza e una marcata eterogeneità degli standard adottati nel mercato interno.

Il CRA, al contrario, introduce obblighi giuridicamente vincolanti, ripartiti in modo puntuale tra i diversi attori della *supply chain*, delineando così un regime di corresponsabilità che intende prevenire vulnerabilità derivanti da comportamenti omissivi o da insufficienti misure di protezione lungo l'intero ciclo di vita del prodotto.

In tal modo, il Regolamento non solo rafforza la tutela degli utenti finali, ma promuove anche una cultura della sicurezza condivisa, fondata su obblighi comuni e su un approccio sistemico all'affidabilità dei prodotti digitali.

Ancora, il Cyber Resilience Act introduce un meccanismo di vigilanza del mercato strutturato, affidato alle Autorità nazionali competenti degli Stati membri, responsabili di verificare la conformità dei prodotti con elementi digitali ai requisiti di cybersicurezza stabiliti dal regolamento. Tali Autorità dispongono di poteri di controllo, ispezione e imposizione di misure correttive, inclusi richiami, restrizioni alla commercializzazione e sanzioni amministrative.

Il CRA si coordina, infine, con il quadro del Regolamento (UE) 2019/1020, rafforzando la cooperazione tra le autorità nazionali e prevedendo il coinvolgimento del CSIRT e di ENISA, per il supporto tecnico e la condivisione di informazioni (art. 52 Reg. UE 2024/2847).

In tal modo, viene assicurata una vigilanza più omogenea ed efficace, riducendo le lacune di controllo che caratterizzavano il sistema precedente.

In conclusione, il Regolamento oggetto di analisi rappresenta un passaggio decisivo per il rafforzamento della sicurezza e della resilienza dell'ecosistema digitale europeo.

Colmando le lacune normative in materia di sicurezza dei prodotti digitali e creando sinergie efficaci con altri strumenti regolatori, si pone come punto di riferimento imprescindibile per la protezione dei prodotti digitali e la stabilità del mercato unico, in un quadro normativo europeo in continua evoluzione.

3. Attori della cybersecurity

La cybersicurezza è un ecosistema complesso che coinvolge diversi attori, ciascuno con ruoli e responsabilità specifiche.

Non si tratta solo di implementare strumenti tecnici di protezione o monitoraggio: la sicurezza informatica dipende dall'integrazione tra governance organizzativa, competenze professionali specializzate e comportamenti diligenti degli utenti finali.

Gli attori della cybersicurezza operano nell'intersezione tra tecnologie, processi organizzativi e standard normativi con l'obiettivo di garantire continuità operativa, protezione dei dati e resilienza dei servizi digitali.

La loro efficacia deriva tanto dalle competenze tecniche quanto dalla capacità di collaborare tra loro per assicurare, assieme a fornitori e produttori di sistemi, un approccio coerente lungo la catena tecnologica.

La Cybersecurity Governance costituisce il modello organizzativo attraverso il quale le organizzazioni strutturano la gestione del rischio cyber, integrandola stabilmente nei processi decisionali e di controllo.

Le definizioni elaborate in ambito internazionale e recepite nell'ordinamento nazionale convergono nel descrivere la governance della cybersicurezza come un sistema articolato di obiettivi, ruoli, responsabilità, politiche, processi e procedure, volto a garantire la sicurezza delle informazioni e la continuità operativa dell'ente.

L'Agenzia per la cybersicurezza nazionale definisce la Cybersecurity Governance "*come il sistema di obiettivi, ruoli, responsabilità, politiche, processi e procedure volti a garantire la cybersicurezza e la continuità operativa di un'organizzazione (o un insieme di organizzazioni)* il cui scopo principale è "*quello di coordinare le decisioni e le azioni organizzative al fine di individuare e prioritizzare gli interventi da attuare per la gestione e la mitigazione e dei rischi cyber a cui un'organizzazione può essere soggetta.*" [61]

Essa assume quindi una funzione eminentemente organizzativa e direzionale, travalicando la dimensione puramente tecnica della sicurezza informatica per collocarsi sul piano delle scelte preventive dell'organizzazione e rappresenta lo strumento attraverso il quale l'ente definisce i propri assetti organizzativi in

---

[61] Definizione presente in *https://www.acn.gov.it/portale/w/cybersecurity-governance-fundamentals-definizione*.

relazione a un rischio strutturalmente connesso all'esercizio dell'attività economica che si svolge.

L'esigenza di una governance efficace nasce dalla crescente consapevolezza dell'aumento degli incidenti di cybersicurezza e della complessità delle minacce cui imprese e individui sono esposti. [62]

In questo contesto, la governance opera come meccanismo di coordinamento delle decisioni strategiche e operative, consentendo di individuare le misure di mitigazione del rischio cyber in funzione degli obiettivi perseguiti e del contesto operativo dell'ente.

La sua rilevanza civilistica emerge nella definizione degli assetti organizzativi esigibili e dei modelli di comportamento che l'organizzazione è tenuta a adottare nella gestione di un rischio ormai prevedibile.

Le Linee Guida fornite dall'Agenzia per la Cybersicurezza Nazionale valorizzano, in particolare, un modello di governance articolato su più livelli ("Governance multilivello"), volto a garantire un collegamento strutturato tra indirizzo strategico e attuazione operativa.

---

[62] Nella Relazione al Parlamento 2023 dell'ACN, si legge "Nel corso del 2023, in un contesto caratterizzato dal considerevole incremento della minaccia cyber, l'Agenzia ha rafforzato il proprio impegno per garantire la diffusione di informazioni sui rischi cyber oltre che per fornire assistenza alle vittime. Grazie anche a un'opera di rilevamento, analisi e allertamento su possibili attacchi e vulnerabilità, è stata portata avanti una costante e puntuale attività di prevenzione, non disgiunta dal supporto, sia da remoto che in loco, in caso di incidenti." in *https://www.acn.gov.it/portale/relazione-annuale/2023*.

A livello strategico, i vertici dell'organizzazione e la direzione collaborano alla definizione di un quadro guida per la gestione della cybersicurezza, delineando gli obiettivi prioritari, pianificando le iniziative fondamentali e individuando i modelli di riferimento cui attenersi. A livello tattico, i responsabili di funzione hanno il compito di tradurre tali indicazioni in azioni concrete nei propri ambiti di competenza, monitorando costantemente il progresso verso il conseguimento degli obiettivi stabiliti. Sul piano operativo, è altresì cruciale che i team interni e i collaboratori esterni acquisiscano piena consapevolezza delle direttive strategiche e adottino comportamenti coerenti, contribuendo attivamente all'efficace gestione del rischio cyber e alla corretta implementazione della governance organizzativa.

Un significativo riconoscimento della centralità della governance si rinviene anche nell'evoluzione del NIST Cybersecurity Framework, che nella versione 2.0, ha introdotto una specifica funzione di "Govern", accanto alle tradizionali funzioni operative di sicurezza.

Tale scelta riflette la crescente consapevolezza che la cybersicurezza non possa essere affidata esclusivamente a interventi tecnici settoriali ma richiede un assetto organizzativo capace di integrare le decisioni in materia di sicurezza nei processi decisionali dell'organizzazione. [63]

[63] The CSF Core Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — organize cybersecurity outcomes at their highest level. • GOVERN (GV) — The organization's cybersecurity

risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy. • IDENTIFY (ID) — The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions. • PROTECT (PR) — Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure. • DETECT (DE) — Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities. • RESPOND (RS) — Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication. • RECOVER (RC) — Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts." in *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*

All'interno di questo quadro, la comprensione del contesto è essenziale: la valutazione dell'esposizione dell'organizzazione alle minacce cyber deve considerare fattori tecnologici, settoriali e geopolitici.[64]

Questo processo, continuo e basato sulla Cyber Threat Intelligence[65] e su meccanismi di *information sharing*[66], permette di monitorare l'evoluzione delle minacce, anticiparne le dinamiche e orientare le strategie di prevenzione e mitigazione.

La distribuzione chiara delle competenze decisionali e operative costituisce inoltre un parametro per valutare l'adeguatezza degli assetti predisposti e per

---

[64] ACN, in *Cybersecurity Governance Fundamentals - La valutazione del contesto cyber di un'organizzazione*, in *https://www.acn.gov.it/portale/w/cybersecurity-governance-fundamentals-la-valutazione-del-contesto-cyber-di-un-organizzazione#list-item-titoloParagrafo-2*

[65] Definita come "l'insieme di attività riguardanti l'analisi di dati rilevanti relativi alle minacce cyber. Essa viene condotta attraverso l'utilizzo di vari strumenti e tecniche di raccolta delle informazioni che possono aiutare un'organizzazione a identificare, valutare, monitorare e rispondere alle minacce informatiche" in *Domini della cybersicurezza - Event, Threat and Incident Management*, in *https://www.acn.gov.it/portale/w/domini-della-cybersicurezza-event-threat-and-incident-management*

[66] "Information sharing is the key to preventing a wide-spread cyber-attack. Information sharing is essential to furthering cybersecurity for the nation. Isolating cyber-attacks and preventing them in the future requires the coordination of many groups and organizations. By rapidly sharing critical information about attacks and vulnerabilities, the scope and magnitude of cyber events can be greatly decreased. With the right plans, processes, and connections in place, information sharing can be seamless step of incident response procedures and a first defense against wide-spread cyber-attacks*."* Così, Cybersecurity and Infrastructure Security Agency (CISA) in *https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing*

garantire che chi progetta e gestisce le misure di sicurezza sia consapevole delle sue responsabilità.

La protezione dei sistemi informativi e dei dati non può prescindere dall'intervento dei professionisti della sicurezza informatica, figure la cui competenza è determinante per garantire continuità operativa e resilienza dell'organizzazione di fronte a minacce digitali complesse.

L'evoluzione tecnologica e la crescente sofisticazione degli attacchi hanno reso necessaria l'istituzione di strutture dedicate alla prevenzione, al monitoraggio e alla gestione degli incidenti, come i CSIRT (Computer Security Incident

Response Team) [67] e i SOC [68] (Security Operations Center), punti nevralgici di un ecosistema nel quale tempestività della risposta e condivisione delle informazioni rappresentano fattori essenziali.

---

[67] Articolo 10 Team di risposta agli incidenti di sicurezza informatica (CSIRT) "1. Ogni Stato membro designa o istituisce uno o più CSIRT. È possibile designare o istituire i CSIRT all'interno di un'autorità competente. I CSIRT sono conformi ai requisiti di cui all'articolo 11, paragrafo 1, si occupano almeno dei settori, dei sottosettori e dei tipi di soggetto di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita. 2. Gli Stati membri provvedono affinché ogni CSIRT disponga di risorse adeguate per svolgere efficacemente i suoi compiti di cui all'articolo 11, paragrafo 3. 3. Gli Stati membri provvedono affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente attraverso la quale scambiare informazioni con i soggetti essenziali e importanti e con gli altri portatori di interesse pertinenti. A tal fine gli Stati membri provvedono affinché ogni CSIRT contribuisca allo sviluppo di strumenti sicuri per la condivisione delle informazioni. 4. I CSIRT cooperano e, se opportuno, scambiano informazioni pertinenti conformemente all'articolo 29 con comunità settoriali o intersettoriali di soggetti essenziali e importanti. 5. I CSIRT partecipano alle revisioni tra pari organizzate conformemente all'articolo 19. 6. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT. 7. I CSIRT possono stabilire relazioni di cooperazione con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi. Nell'ambito di tali relazioni di cooperazione, gli Stati membri facilitano uno scambio di informazioni efficace, efficiente e sicuro con tali team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, compreso il protocollo TLP (Traffic Light Protocol). I CSIRT possono scambiare informazioni pertinenti con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, compresi dati personali a norma del diritto dell'Unione in materia di protezione dei dati. 8. I CSIRT possono cooperare con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi o con organismi equivalenti di paesi terzi, in particolare al fine di fornire loro assistenza in materia di cibersicurezza. 9. Ogni Stato membro notifica alla Commissione senza indebiti ritardi l'identità del CSIRT di cui al paragrafo 1 del presente articolo e del CSIRT designato come coordinatore conformemente all'articolo 12, paragrafo 1, i

I CSIRT, inizialmente concepiti come gruppi di supporto per la gestione di eventi specifici, hanno progressivamente ampliato le proprie funzioni, includendo il coordinamento con altri team, la comunicazione con stakeholders

---

rispettivi compiti in relazione ai soggetti essenziali e importanti e qualsiasi ulteriore modifica dei medesimi. 10. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo dei CSIRT.

In particolare, l'art. 11 della Direttiva 2022/2555 i CSIRT svolgono i seguenti compiti "a) monitorano e analizzano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale, e, su richiesta, forniscono assistenza ai soggetti essenziali e importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informatici e di rete; b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e importanti interessati, nonché alle autorità competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale; c) forniscono una risposta agli incidenti e forniscono assistenza ai soggetti essenziali e importanti interessati, se del caso; d) raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza; e) effettuano, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo; f) partecipano alla rete di CSIRT e forniscono assistenza reciproca secondo le loro capacità e competenze agli altri membri della rete di CSIRT su loro richiesta. g) se del caso, agiscono in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1; h) contribuiscono allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui all'articolo 10, paragrafo 3.I CSIRT possono effettuare una scansione proattiva e non intrusiva dei sistemi informatici e di rete accessibili al pubblico di soggetti essenziali e importanti. Tale scansione è effettuata per individuare sistemi informatici e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati. Tale scansione non ha alcun impatto negativo sul funzionamento dei servizi dei soggetti. Nello svolgimento dei compiti di cui al primo comma, i CSIRT possono dare priorità a determinati compiti sulla base di un approccio basato sul rischio." Dal testo della Direttiva NIS2 disponibile in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555*

[68] IBM, "*Cos'è un Security Operations Center (SOC)*" in *https://www.ibm.com/it-it/think/topics/security-operations-center*

nazionali e internazionali, la definizione di linee guida operative e la promozione di standard condivisi a livello europeo.

I SOC svolgono un ruolo centrale nel monitoraggio costante dei sistemi, analizzando log e flussi di rete, individuando comportamenti anomali, gestendo allarmi e coordinando le azioni di contenimento, spesso in stretta collaborazione con i CSIRT.

All'interno di questo contesto strutturato, i professionisti della sicurezza informatica svolgono ruoli specifici e complementari.[69]

Il Security Specialist, ad esempio, è responsabile dell'implementazione delle politiche di sicurezza, della configurazione e dell'aggiornamento dei sistemi e delle applicazioni, dell'analisi delle vulnerabilità e della promozione di programmi di formazione e sensibilizzazione continua, assicurando che le procedure adottate siano coerenti con le normative e gli standard di settore.

Il Malware Analyst si dedica all'individuazione e all'analisi dei codici malevoli, sviluppando strumenti di difesa avanzati e utilizzando metodologie basate sia sulle firme locali sia sul monitoraggio del traffico di rete, richiedendo un aggiornamento tecnico costante e una conoscenza approfondita dei sistemi operativi, delle reti e della programmazione. Il Security Consultant, spesso esterno all'organizzazione, ha il compito di valutare la sicurezza complessiva

---

[69] Agenzia per la cybersicurezza nazionale, Ruoli e responsabilità della cybersicurezza, in *https://www.acn.gov.it/portale/w/ruoli-e-responsabilita-della-cybersicurezza-le-figure-principali*

dei sistemi, condurre audit, identificare vulnerabilità e proporre interventi correttivi, coordinando progetti complessi e assicurando la conformità alle normative europee e agli standard internazionali. Il Security Engineer, con un ruolo tecnico intermedio, implementa e verifica le soluzioni di sicurezza, indaga sulle intrusioni e supporta la gestione operativa degli incidenti, mentre il Security Architect assume una posizione senior nella progettazione e nella manutenzione dell'infrastruttura di sicurezza, integrando conoscenze di framework, protocolli, crittografia e gestione del rischio, garantendo così la coerenza delle strategie di sicurezza a livello organizzativo. Infine, il Chief Information Security Officer (CISO) coordina le attività strategiche e operative, sovrintendendo ai team, gestendo il rischio, predisponendo piani di emergenza e assicurando la continuità dei processi, fungendo da punto di connessione tra la governance aziendale e le funzioni tecniche, definendo metriche di monitoraggio e gestendo il budget dedicato alla sicurezza.

L'integrazione e la collaborazione tra queste figure professionali permette un approccio globale e strutturato alla cybersicurezza, combinando prevenzione, gestione degli incidenti, formazione continua e creando un sistema resiliente in grado di adattarsi rapidamente all'evoluzione delle minacce digitali, come

evidenziato nei report ENISA sullo stato dei CSIRT e sulle capacità di risposta agli incidenti in Europa.[70]

La cybersicurezza deve essere concepita non solo come un insieme di strumenti e procedure tecniche, ma come un processo integrato che coinvolge tanto le strutture organizzative e i professionisti specializzati quanto tutti coloro che interagiscono quotidianamente con i sistemi informativi, contribuendo in tal modo alla protezione complessiva delle informazioni e alla resilienza digitale dell'organizzazione.

Completato il quadro dei soggetti professionalmente incaricati della gestione e della protezione dei sistemi informativi, emerge come la sicurezza complessiva dipenda non solo dall'efficacia degli assetti organizzativi e delle misure tecniche, ma anche dal comportamento degli utenti finali.

La loro consapevolezza, formazione e osservanza delle regole costituiscono elementi essenziali per prevenire e mitigare il rischio cyber, rendendo necessario un approfondimento specifico sui loro ruoli e responsabilità connesse all'interno del modello di cybersecurity governance.

L'utente finale non è né completamente passivo né titolare del potere di governo del rischio tecnologico. Pur non partecipando alla progettazione,

---

[70] "*Study on CSIRT landscape and IR capabilities in Europe 2025*" disponibile in *https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O.3.1.3%20CSIRT%20landscape%202020.pdf*

sviluppo o gestione dell'infrastruttura, il suo comportamento interagisce con il rischio cyber e può incidere, in misura variabile, sull'evento dannoso.

Tradizionalmente considerato il soggetto debole del rapporto digitale[71], a causa dell'asimmetria informativa e tecnica che caratterizza il suo rapporto con fornitori di servizi, gestori delle infrastrutture e produttori di sistemi informatici, l'utente contribuisce comunque alla sicurezza complessiva attraverso comportamenti quotidiani, che possono amplificare o contenere il rischio.

È bene specificare che l'utente finale non deve possedere competenze informatiche avanzate ma è tenuto a mantenere comportamenti diligenti, conformemente ai principi del diritto civile, ed in particolare all'art. 1176 c.c.

La sua condotta assume rilievo come elemento concorrente nella produzione del danno, senza costituire causa esclusiva e senza interrompere il nesso causale rispetto ai soggetti responsabili della gestione del sistema.[72]

---

[71] Per una più ampia visione della rilevanza dell'asimmetria informativa nei rapporti contrattuali, si veda G. ALPA, in *Il diritto dei consumatori*, Bari, 1995.

[72] Art. 1227 c.c. (Concorso del fatto colposo del creditore) il quale prevede che "*Se il fatto colposo del creditore ha concorso a cagionare il danno, il risarcimento è diminuito secondo la gravità della colpa e l'entità delle conseguenze che ne sono derivate. Il risarcimento non è dovuto per i danni che il creditore avrebbe potuto evitare usando l'ordinaria diligenza.*"

In altre parole, il ruolo dell'utente va valutato all'interno di una dinamica complessa, caratterizzata dall'interazione tra vulnerabilità tecnologiche, scelte organizzative e condotte individuali.

In sintesi, l'utente finale contribuisce indirettamente alla sicurezza complessiva e deve operare in modo consapevole e cooperativo, senza perciò divenire cogestore del rischio cyber. La responsabilità primaria resta infatti in capo ai professionisti qualificati.

Tale approccio risulta coerente con la normativa europea in materia di cybersicurezza, che rafforza gli obblighi organizzativi e informativi dei gestori dei sistemi, senza attribuire agli utenti finali compiti diretti di gestione del rischio.

Capitolo II

Responsabilità civile e gestione del rischio nel cyberspazio

Sommario: 1. Responsabilità civile nel cyberspazio: profili generali; 1.1. Responsabilità extracontrattuale: modello aquiliano e logica del rischio; 1.2. Responsabilità per prodotti difettosi; 1.3. Responsabilità del prestatore di servizi digitali; 1.4. Il danno informatico; 2. Intelligenza artificiale: potenzialità e rischi nella protezione dei sistemi informatici; 3. Verso una riconfigurazione della responsabilità nel cyberspazio.

1. Responsabilità civile nel cyberspazio: profili generali

La crescente digitalizzazione delle attività economiche e sociali ha creato un nuovo spazio operativo, il cyberspazio, caratterizzato da interconnessione sistemica, complessità tecnica e vulnerabilità diffuse.

Non si tratta più di un semplice luogo virtuale di comunicazione ma di un ambiente operativo in cui si manifestano rischi concreti capaci di produrre effetti patrimoniali e non patrimoniali nella sfera giuridica dei soggetti coinvolti.

L'adozione massiccia di piattaforme digitali e sistemi di intelligenza artificiale ha reso dati e infrastrutture informatiche estremamente sensibili, esponendoli a potenziali attacchi in grado di compromettere l'operatività di settori socialmente strategici.[73]

---

[73] Considerando 3, Direttiva UE 2225/2022: "I sistemi informatici e di rete occupano ormai una posizione centrale nella vita di tutti i giorni, con la rapida trasformazione digitale e l'interconnessione della società, anche

Questo fenomeno rientra nel concetto di *cyber risk,* inteso come il rischio connesso alla compromissione della sicurezza di dati, sistemi e infrastrutture digitali, derivante da attacchi esterni, minacce interne, errori umani o vulnerabilità tecnologiche.

In tal senso, la Direttiva NIS 2 evidenzia *Poichè le minacce alla sicurezza dei sistemi informatici e di rete possono avere origini diverse, le misure di gestione dei rischi di cibersicurezza dovrebbero essere basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni detenute dai soggetti essenziali o importanti e agli impianti di trattamento delle informazioni di questi ultimi e dalle interferenze con tali informazioni o impianti che possano compromettere*

---

negli scambi transfrontalieri. Ciò ha portato a un'espansione del panorama delle minacce informatiche, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. Il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti stanno aumentando e rappresentano una grave minaccia per il funzionamento dei sistemi informatici e di rete. Tali incidenti possono quindi impedire l'esercizio delle attività economiche nel mercato interno, provocare perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e alla società dell'Unione. Pertanto, la preparazione e l'efficacia della cibersicurezza sono oggi più che mai essenziali per il corretto funzionamento del mercato interno. Inoltre, la cibersicurezza è un fattore abilitante fondamentale per molti settori critici, affinché questi possano attuare con successo la trasformazione digitale e cogliere appieno i vantaggi economici, sociali e sostenibili della digitalizzazione."

la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi. Le misure di gestione dei rischi di cibersicurezza dovrebbero pertanto affrontare anche la sicurezza fisica e dell'ambiente dei sistemi informatici e di rete includendo misure volte a proteggere detti sistemi da guasti del sistema, errori umani, azioni malevole o fenomeni naturali, in linea con le norme europee e internazionali, come quelle di cui alla serie ISO/IEC 27000. A tale riguardo, i soggetti essenziali e importanti dovrebbero altresì, nell'ambito delle loro misure di gestione dei rischi di cibersicurezza, affrontare la questione della sicurezza delle risorse umane e disporre di strategie adeguate di controllo dell'accesso. Tali misure dovrebbero essere coerenti con la direttiva (UE) 2022/2557.[74]

La rilevanza del tema è confermata dal fatto che il *cyber risk* è oggi considerato tra le minacce più gravi a livello globale. [75]

Dal punto di vista tecnico, i rischi cibernetici possono avere origine intrinseca o estrinseca rispetto al sistema.[76]

---

[74] Considerando 79 Direttiva (UE) 2225/2022.

[75] Si veda il *World Economic Forum Global Risks Report 2025*, in https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf.

[76] S. CALÌ, F. CAPPARELLI, M. HAZAN, F. MARTINI, op. cit., p. 179.

Nel primo caso, derivano da malfunzionamenti o difetti degli stessi dispositivi; nel secondo, da fattori esterni come attacchi *ransomware* (cd. estorsione informatica), *malware* o tecniche di ingegneria sociale, tra cui *phishing.* [77]

Qualunque sia la causa, tali rischi generano danni significativi e crisi operative che impattano settori cruciali, dalla continuità aziendale alla protezione dei dati personali sino alla sicurezza della persona.

Dinanzi a simili scenari, un approccio esclusivamente reattivo limitato all'analisi delle conseguenze dannose risulta insufficiente.

È pertanto necessario integrare una gestione preventiva dei rischi con un apparato di responsabilità efficace.

Dal punto di vista giuridico, l'applicazione tradizionale della responsabilità civile nel contesto digitale presenta limiti rilevanti: la difficoltà di attribuire materialmente l'illecito, le complessità probatorie, la molteplicità degli attori coinvolti e le vulnerabilità intrinseche ai sistemi informatici complicano la ricostruzione del nesso causale e l'individuazione del soggetto responsabile.

Proprio per queste ragioni, la gestione del rischio cyber richiede di integrare prevenzione e responsabilità, quest'ultima necessaria non solo a compensare i danni ma anche a incentivare comportamenti diligenti.

[77] Sul fenomeno del *pishing* e della responsabilità contrattuale delle banche, si veda Cass. n. 3780/2024.

In questo contesto assumono rilievo i soggetti che, a diverso titolo, immettono sul mercato o gestiscono tecnologie digitali, contribuendo alla creazione e al governo del rischio cibernetico.

In particolare, ai fini dell'analisi della responsabilità civile, è possibile distinguere, in senso funzionale e non meramente formale, tra produttori di prodotti digitali e prestatori di servizi digitali, consapevoli tuttavia della crescente ibridazione tra le due categorie.

Rientrano nella prima categoria i soggetti che sviluppano e immettono sul mercato *software*, dispositivi connessi, sistemi informatici o componenti digitali destinati a operare in modo autonomo o integrato, rispetto ai quali il rischio può derivare da difetti di progettazione, sviluppo o sicurezza. In tali ipotesi, la responsabilità tende ad avvicinarsi a modelli di tipo oggettivo.

Diversamente, i prestatori di servizi digitali, quali fornitori di servizi cloud, hosting, gestione, manutenzione o monitoraggio di sistemi informatici, esercitano un controllo continuativo sull'infrastruttura e sull'operatività del sistema, assumendo obblighi di diligenza qualificata nella gestione della sicurezza. Qui, la responsabilità civile si fonda prevalentemente sull'accertamento della colpa, valutata alla luce degli standard tecnici e organizzativi esigibili, nonché delle misure di prevenzione adottate.

L'analisi che segue, dunque, non si limita a una ricostruzione normativa bensì mira a interpretare criticamente l'applicazione dei modelli di imputazione tradizionali ai nuovi rischi digitali.

Il capitolo si propone di offrire un quadro sistematico della responsabilità civile nel cyberspazio con particolare attenzione agli scenari in cui la tecnologia digitale si intreccia con la tutela dei diritti fondamentali e la continuità dei servizi essenziali.

1.1. Responsabilità extracontrattuale: modello aquiliano e logica del rischio

La responsabilità civile nel diritto privato è stata storicamente concepita come un istituto volto primariamente alla riparazione del pregiudizio ingiustamente arrecato e, in via indiretta, alla dissuasione dal compimento di comportamenti dannosi.

Tale costruzione, radicata nella tradizione liberale e nella centralità dell'agire individuale, si fondava sull'idea che la responsabilità rappresentasse la reazione dell'ordinamento alla violazione del precetto del *neminem laedere*, secondo la nota formulazione groziana *ut nemo laedatur*[78], e che tale reazione si articolasse essenzialmente nella sanzione civilistica comminata a chi avesse cagionato un danno per dolo o colpa.[79]

---

[78] Come ricorda, F. GALGANO, in *Le antiche e le nuove frontiere della responsabilità civile*, in *Contr. impr.*, 2008, p. 80.

[79] M. FRANZONI, in *Dei fatti illeciti (2043-2059)*, in A. SCIALOJA, G. BRANCA (a cura di), Comm. Cod. civ., Bologna-Roma, 1993, p. 39 ss. L'Autore evidenzia che solo la colpa poteva costituire il criterio di selezione degli interessi meritevoli di tutela.

La responsabilità era pertanto ancorata al principio di auto-responsabilità, in forza del quale ciascun consociato era chiamato a rispondere delle conseguenze dannose del proprio agire.[80]

Tuttavia, l'evoluzione delle attività economiche caratterizzate da crescente complessità tecnica e processi produttivi opachi ha mostrato i limiti di tale approccio.

L'accertamento della colpa diveniva infatti incerto, faticoso e spesso privo di effettività, con il risultato paradossale di lasciare il danno a carico della vittima nonostante la chiara riconducibilità dell'evento al rischio intrinseco dell'attività svolta.[81]

Questa trasformazione ha reso dunque inevitabile l'emersione di modelli di responsabilità oggettiva, fondati non già sulla rimproverabilità della condotta,

---

[80] S. LANDINI, in *Assicurazione e responsabilità*, Milano, 2004, p. 66.

[81] U. RUFFOLO, in *Intelligenza artificiale e responsabilità. Responsabilità "da algoritmo"? A.I. e automobili self-driving, automazione produttiva, robotizzazione medico-farmaceutica A.I e attività commerciali Le tendenze e discipline unionali (a cura di Ugo Ruffolo)*, Giuffrè Editore, 2017, p. 14 ove l'Autore sottolinea come "solo da qualche decennio è davvero superato il pregiudizio connesso al tabù del "*nessuna responsabilità senza colpa",* che ha a lungo distorto la responsabilizzazione personale degli esseri umani, proprio in considerazione della tipologia della loro intelligenza-coscienza. Pregiudizio che ha impedito o seriamente ritardato il ricorso – normativo e interpretativo – a forme di responsabilità personale oggettiva più consone a contesti socio-produttivi emergenti della prima rivoluzione industriale, ed alle correlative esigenze di minimizzazione di nuovi rischi e di attribuzione della loro gestione". G. CAZZETTA, *Responsabilità aquiliana e frammentazione del diritto comune civilistico (1865- 1914)*, Milano, 1991, p. 118

ma sulla pericolosità dell'attività e sulla necessità di allocare il rischio presso il soggetto che trae vantaggio dalla stessa.[82]

La dottrina giuridica e la teoria sociale hanno colto tale mutamento qualificandolo come passaggio verso una vera e propria "società del rischio" o "cultura del rischio" [83] in collegamento con l'emergere di innovazioni tecnologiche e scientifiche della cui rischiosità si è sempre più incerti.

In particolare, si è assistito a una evoluzione dell'idea di rischio: l'accelerazione tecnologica contemporanea ha prodotto una situazione nella quale la tecnologia opera talvolta al di là della conoscenza scientifica consolidata, generando forme di incertezza qualitative e non puramente probabilistiche.[84]

L'assunzione del rischio diviene una componente fisiologica della vita economica e sociale e l'attribuzione della responsabilità tende a orientarsi verso criteri che selezionano i soggetti più idonei alla gestione del rischio stesso.

Il principio di precauzione rafforza tale logica, imponendo di adottare misure preventive anche quando il rischio non sia pienamente determinabile o

---

[82] Sul punto, C. CASTRONOVO, in *La nuova responsabilità civile*, Milano, 2006, p. 277 ss.; S. SICA, in *La responsabilità civile tra struttura funzioni e «valori» (a proposito di un recente libro),* in *Resp. civ. prev.,* 1994, p. 543 e ss.;

[83] Di cui parla U. BECK, in *La societé du risque. Sur la voie d'une autre modernité,* Aubier, Parigi, 2001 (1ed. 1986). Nella sua traduzione in lingua italiana, *La società del rischio. Verso una seconda modernità.,* Carrocci, 2013.

[84] G. COMANDÉ, in *Gli strumenti della precauzione: nuovi rischi, assicurazione e responsabilità*, Giuffrè Editore, p. 33.

quantificabile. [85] Pur essendo nato e consacrato dall'Unione europea per la protezione del bene ambiente,[86] esso ha progressivamente ampliato il proprio raggio d'applicazione e oggi rappresenta un criterio interpretativo di riferimento nei settori caratterizzati da incertezza tecnologica e scientifica.

Lo stesso è generalmente invocato dai legislatori nazionali ed europei ogni qualvolta occorra disciplinare ambiti che, sulla base di una valutazione tecnico-scientifica, risultino potenzialmente rischiosi.

Alla luce di queste trasformazioni, la responsabilità civile assume una funzione prevalentemente allocativa e compensativa: diviene lo strumento attraverso il quale il rischio connesso allo svolgimento di determinate attività viene ripartito tra gli operatori economici secondo criteri di efficienza, prossimità al rischio e capacità di prevenzione.

Il criterio di imputazione, lungi dal limitarsi a identificare il soggetto colpevole, agisce dunque quale meccanismo di traslazione del danno, spostandolo dalla

---

[85] M. RENNA, in *Il principio di precauzione e la sua attuabilità*, in *Forum di Quaderni Costituzionali*, 2, 2023, p. 341.

[86] La cultura della precauzione nasce in Germania negli anni Settanta come risposta ad una rinnovata percezione dei rischi per l'ambiente derivanti dallo sviluppo tecnologico ed industriale. Le prime riflessioni sono da ricondurre a H. JONAS, in *Il principio di responsabilità. Un'etica per la civiltà tecnologica*, Torino, 1990; e U. BECK, *op. cit.*

vittima al soggetto che, per posizione, competenza o controllo, risulta maggiormente idoneo ad assumerne il costo. [87]

La sfida centrale diviene, pertanto, l'individuazione dei criteri di allocazione della responsabilità: un compito che richiede l'abbandono di approcci rigidamente soggettivi per abbracciare un modello di imputazione orientato alla gestione del rischio e alle esigenze di effettività della tutela.[88]

La materia della cybersicurezza impone di sviluppare una riflessione autonoma sul piano della responsabilità extracontrattuale.

Quest'ultima appunto viene in rilievo ogniqualvolta il danno colpisca soggetti non legati da alcun vincolo negoziale e risulti riconducibile alla violazione del generale dovere del *neminem laedere*, nonché alla lesione di diritti assoluti o di altre situazioni giuridiche soggettive meritevoli di tutela per l'ordinamento. [89]

La responsabilità aquiliana si configura, dunque, nelle ipotesi in cui il pregiudizio si produca in capo a soggetti che non intrattengono alcun rapporto contrattuale con l'autore del fatto dannoso.

In tali casi, l'analisi si sposta dalla struttura dell'obbligazione e dall'accertamento dell'inadempimento alla valutazione del comportamento

---

[87] R. GIOVAGNOLI, in *Manuale di diritto civile*, Itaedizioni, V edizione, p. 1904.

[88]G. COMANDÉ, in *Intelligenza artificiale e responsabilità tra liability e accountability, in Analisi giuridica dell'economia,* 1, 2019, pp. 169 e ss.

[89] *Ex multis*, F. CARNELUTTI, in *Sulla distinzione tra colpa contrattuale e colpa extracontrattuale, nota di commento ad App. Venezia*, in *Riv. dir. comm.,* 1912, II, 744

tenuto dal soggetto agente, il quale può essere chiamato a rispondere ai sensi dell'art. 2043 c.c., secondo cui "*qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno*".

La fattispecie delineata dall'art. 2043 c.c. costituisce il modello generale della responsabilità civile e si fonda su un criterio di imputazione che valorizza l'elemento soggettivo del dolo o della colpa del danneggiante.

La norma individua, in via generale, gli elementi strutturali dell'illecito aquiliano (fatto illecito, nesso causale tra condotta ed evento dannoso, danno ingiusto ed elemento soggettivo) comuni alle diverse ipotesi di responsabilità extracontrattuale previste dall'ordinamento.

Accanto a tale paradigma classico, fondato sull'accertamento della colpa, si sono progressivamente affermate ipotesi di responsabilità oggettiva o di responsabilità aggravata, giustificate come anzidetto dall'esigenza di una più efficiente allocazione del rischio.

In tali modelli, la nozione di rischio assume rilievo quale criterio autonomo di imputazione della responsabilità, rafforzando la funzione preventiva del sistema e la sua attitudine alla distribuzione dei costi sociali del danno.

Queste forme di responsabilità muovono dall'assunto secondo cui chi trae utilità dall'esercizio di un'attività intrinsecamente rischiosa deve sopportarne anche i costi e le conseguenze dannose, indipendentemente dall'accertamento di una colpa in senso tradizionale.

L'emersione della responsabilità oggettiva è, non a caso, storicamente connessa al fenomeno dell'industrializzazione che ha determinato un significativo incremento dei rischi e dei danni connessi allo svolgimento di attività produttive complesse.

L'evoluzione dei processi industriali, caratterizzati da catene causali articolate e da un'elevata frammentazione delle fasi di produzione, ha reso sempre più difficile, se non addirittura impossibile, individuare con precisione la causa del danno e ricondurla alla condotta colposa di un singolo soggetto. [90]

È in tale contesto che il modello aquiliano tradizionale ha mostrato i propri limiti sul piano della tutela effettiva dei danneggiati, rischiando di tradursi in una sostanziale deresponsabilizzazione dei soggetti che esercitano attività economicamente rilevanti e potenzialmente pericolose.

Pertanto, il sistema della responsabilità oggettiva è stato talvolta prospettato come il modello maggiormente idoneo a offrire una risposta a qualsiasi nocumento si produca nell'esercizio di attività complesse o intrinsecamente rischiose. [91]

---

[90] J.J. LO´ PEZ JACOISTE, in *Transformaciones y paradojas de la responsabilidad extracontractual*, Madrid, Real Academica de Jurisprudencia y Legislacion, 1994, pp. 26-30.

[91] R. SCOGNAMIGLIO, in *Responsabilità civile*, in *Novissimo Digesto Italiano*, vol. XV, Torino, UTET, 1982, pp. 628-657: 636

In questa prospettiva, il concetto di "rischio" assume un ruolo centrale tanto che parte autorevole della dottrina lo considera il principio maggiormente idoneo a fondare una categoria generale e unitaria di responsabilità oggettiva.[92]
Alla luce dei principi generali e della logica del rischio appena esaminata, l'ordinamento individua ipotesi tipizzate di responsabilità oggettiva o di responsabilità aggravata, nelle quali l'imputazione del danno prescinde, in tutto o in parte, dall'accertamento della colpa.
Per quel che qui interessa, particolare rilievo assumono la responsabilità per l'esercizio di attività pericolose (art. 2050 c.c.) e la responsabilità per danno cagionato da cose in custodia (art. 2051 c.c.).
La loro applicazione al cyberspazio consente di esplorare le potenzialità ed i limiti della responsabilità oggettiva nell'era digitale al fine di valutare se e in che misura tali fattispecie possano offrire strumenti idonei a fronteggiare i danni derivanti da incidenti informatici, violazioni di sicurezza e attacchi cibernetici.
L'art. 2050 c.c. dispone che "*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno."*

---

[92] P. TRIMARCHI, in *Responsabilità civile, atti illeciti, rischio, danno.,* Giuffrè, III ed., pp. 301 e ss.

Tale norma fonda la responsabilità per l'esercizio di attività pericolose e si configura come un'ipotesi di responsabilità sostanzialmente oggettiva[93], che prescinde da ogni valutazione in merito alla presenza dell'elemento soggettivo, in virtù del rigore della prova richiesta per superare la presunzione di colpa (il soggetto deve provare di aver fatto tutto il possibile per evitare il danno) e del conseguente favore riservato alla posizione del danneggiato. [94]

Il limite entro cui tale responsabilità viene circoscritta è individuato in un criterio di ragionevolezza oggettiva, il quale opera quale parametro di valutazione dell'idoneità delle misure preventive adottate in rapporto al rischio concretamente generato dall'attività.

In tale prospettiva, l'esercente risponde dei danni riconducibili a rischi che avrebbero potuto essere evitati mediante l'adozione di tutte le cautele esigibili secondo le conoscenze tecniche e scientifiche del tempo, non essendo

---

[93] Si veda sulla nozione di responsabilità "sostanzialmente oggettiva" *ex multis* Cass. n. 7093/2015; Cass. n. 26516/2009 in *italgiure.it*.

[94] Cass. civ. 16170/2022: "La presunzione di responsabilità contemplata dall'art. 2050 c.c. per attività pericolose può essere vinta solo con una prova particolarmente rigorosa, e cioè con la dimostrazione di aver adottato tutte le misure idonee ad evitare il danno: pertanto non basta la prova negativa di non aver commesso alcuna violazione delle norme di legge o di comune prudenza, ma occorre quella positiva di avere impiegato ogni cura o misura volta ad impedire l'evento dannoso, di guisa che anche il fatto del danneggiato o del terzo può produrre effetti liberatori solo se per la sua incidenza e rilevanza sia tale da escludere, in modo certo, il nesso causale tra attività pericolosa e l'evento e non già quando costituisce elemento concorrente nella produzione del danno, inserendosi in una situazione di pericolo che ne abbia reso possibile l'insorgenza a causa dell'inidoneità delle misure preventive adottate*."*

sufficiente, ai fini della prova liberatoria, il mero rispetto di standard normativi o di prassi consolidate. [95]

Il problema centrale nell'analisi della responsabilità prevista dall'art. 2050 c.c. consiste nell'individuare cosa debba intendersi per "attività pericolosa".

Tale nozione è stata oggetto di un'ampia elaborazione, dapprima dottrinale e successivamente giurisprudenziale, che merita di essere sinteticamente riportata.

In linea generale, vi rientrano tutte quelle attività che, pur socialmente utili, sono caratterizzate da un elevato pericolo di arrecare danni. Occorre, tuttavia, limitare l'ambito applicativo a quelle pratiche pericolose che si concretizzano in una successione ripetuta e continua di atti coordinati tra loro, svolti nel corso di un determinato periodo di tempo. [96]

Proprio la continuità e la prevedibilità delle attività cd seriali costituiscono il parametro per determinare il livello di diligenza richiesto.[97]

---

[95] R. GIOVAGNOLI, op. cit., p. 1942.

[96] G. MIRABILE, in *Le tendenze evolutive della giurisprudenza riguardo alla nozione di attività pericolosa*, in *Responsabilità Civile e Previdenza*, 2018, 2, p. 454.

[97] Sul punto, Cass. civ. 1425/1983 fa riferimento a "una successione continua e ripetuta di atti che si svolge nel tempo e che rivela una notevole potenzialità di danno, superiore al normale ed apprezzabile in un momento anteriore all'evento dannoso, così da consentire all'operatore la predisposizione di adeguate misure di prevenzione e da costituire il parametro di commisurazione della diligenza dovuta, la cui mancanza integra la colpa presunta dall'art. 2050, anche qualora tali atti si coordinino non già, come di norma, all'esercizio di una impresa, bensì semplicemente ad un fine tipico oggettivamente pericoloso."

Inizialmente, la lettura che veniva offerta dagli interpreti era molto rigorosa tanto che le fattispecie che vi rientravano erano solo quelle definite "pericolose" ai sensi degli artt. 63-67 del Testo Unico delle leggi di Pubblica sicurezza n. 773 del 1981.

Tale lettura fu ben presto superata, soprattutto mediante l'elaborazione della Suprema Corte di Cassazione che, partendo dall'assunto per cui ogni attività umana porta con sé un grado più o meno di pericolosità intrinseco, ha sottolineato che debbono essere prese in considerazione solo quelle potenzialmente dannose per l'alta percentuale di danni cagionati, in ragione della natura e dei mezzi adoperati. [98]

L'esigenza di ampliare l'ambito applicativo dell'art. 2050 c.c., resa possibile anche dall'indeterminatezza della sua formulazione, ha indotto parte della dottrina a richiamare il principio di precauzione quale criterio interpretativo idoneo a rileggere le norme civilistiche in contesti caratterizzati da elevata incertezza scientifica e tecnologica.

In tale prospettiva, il principio viene valorizzato come strumento volto a rafforzare gli obblighi di prevenzione gravanti sull'esercente attività pericolose, anticipando la soglia di tutela rispetto al verificarsi del danno e

[98] Cass. civ. 16052/2015 "In tema di risarcimento dei danni ai sensi dell'art. 2050 c.c., sono attività pericolose non solo quelle qualificate come tali dalla legge di pubblica sicurezza, ma anche quelle che, per la loro stessa natura o per le caratteristiche dei mezzi adoperati, comportino, in ragione della loro spiccata potenzialità offensiva, una rilevante possibilità del verificarsi di un danno."

spostando l'attenzione sul momento organizzativo e preventivo dell'attività stessa. [99]

Nel contesto che qui interessa, appare dunque naturale interrogarsi se, dinanzi all'impiego di strumenti tecnologici di varia natura e al riconoscimento del rischio intrinseco connesso allo sfruttamento di sistemi informatici complessi, e per il solo fatto di trovarsi dinanzi a un'attività esposta a rischio cibernetico, il modello di responsabilità delineato dall'art. 2050 c.c. possa costituire una risposta adeguata dell'ordinamento.

Alla luce dell'interpretazione ormai ampia che la giurisprudenza riserva al concetto di attività pericolosa, non può escludersi che vi rientrino anche attività caratterizzate da un elevato rischio cyber, qualora tale rischio sia strutturalmente connesso alle modalità di svolgimento dell'attività stessa.

Ai fini della configurabilità della responsabilità ex art. 2050 c.c., resta imprescindibile l'accertamento del nesso di causalità tra attività pericolosa e danno; è infatti indispensabile che il danno sia direttamente riconducibile all'esercizio dell'attività pericolosa in quanto tale, e non già a un comportamento meramente occasionale o colposo dell'agente.

In difetto di tale requisito, non potrà trovare applicazione la responsabilità speciale di cui all'art. 2050 c.c., restando al danneggiato la sola possibilità di

[99] R. GIOVAGNOLI, op. cit., p. 1944.

invocare la disciplina generale dell'art. 2043 c.c., ove ne ricorrano i presupposti.

Il nesso causale deve inoltre essere diretto e adeguato, nel senso che tra l'esercizio dell'attività e il danno deve sussistere una sequenza regolare tale per cui l'evento lesivo possa qualificarsi, secondo un criterio di normalità statistica, come conseguenza tipica e prevedibile di quella determinata attività. È pertanto necessario che non intervengano fattori sopravvenuti autonomi, quali, ad esempio, il fatto del terzo, idonei a interrompere il nesso eziologico. [100]

Una volta accertati tali elementi, l'esercente dell'attività pericolosa risponde del danno, salvo che riesca a fornire la prova liberatoria, consistente nella dimostrazione di aver predisposto un'organizzazione dell'attività idonea e di aver rispettato non solo tutti gli standard tecnici previsti dalla normativa di settore, ma anche ogni ulteriore misura necessaria, secondo lo stato dell'arte, per prevenire il danno.

In particolare, l'esercente deve dimostrare di aver impiegato tutte le risorse concretamente disponibili al fine di evitare l'evento lesivo, a prescindere dal costo delle misure adottate. [101]

---

[100] Sull'onere della prova in materia di nesso causale, *ex multis*, Cass. civ. n. 18812/2014; Cass. civ. n. 16170/2022.

[101] Sul punto, si veda, *ex multis*, Cass. civ. n. 11454/2003.

È evidente, in tale prospettiva, come la prova liberatoria richiesta assuma connotati gravosi soprattutto in settori, come quello della cybersicurezza, caratterizzati da un'elevata complessità tecnica, da un rischio intrinsecamente dinamico e da un continuo mutamento degli standard di riferimento.

L'esigenza di dimostrare non solo il rispetto delle prescrizioni normative vigenti, ma anche l'adozione di ogni misura tecnicamente possibile secondo lo stato dell'arte, finisce per proiettare sull'operatore un obbligo di diligenza particolarmente intenso, che tende ad avvicinarsi, sul piano sostanziale a una responsabilità di risultato.

Una forma di responsabilità dunque che, senza configurarsi come oggettiva in senso stretto, si colloca in una posizione intermedia, caratterizzata da un elevato livello di prevenzione imposto all'operatore e da una tutela rafforzata del danneggiato.

In tale contesto, l'applicazione dell'art. 2050 c.c. al rischio cibernetico, se da un lato appare coerente con una lettura evolutiva della norma e con le esigenze di anticipazione della tutela proprie del principio di precauzione, dall'altro solleva rilevanti interrogativi circa la sua effettiva capacità di adattarsi a fenomeni nei quali il controllo del rischio non può dirsi mai totale e la prevenzione non può realisticamente tradursi nell'eliminazione del pericolo.

Ne deriva una tensione strutturale tra l'obiettivo di rafforzare la tutela del danneggiato e la necessità di evitare che l'estensione interpretativa della responsabilità finisca per eccedere la funzione propria dell'art. 2050 c.c.,

trasformandolo in uno strumento di imputazione pressoché automatica del danno in presenza di eventi cibernetici avversi.

Sempre facendo riferimento agli strumenti offerti dal nostro ordinamento, un ulteriore regime che potrebbe venire in rilievo è quello previsto dall'art. 2051 c.c., il quale dispone che "*Ciascuno è responsabile del danno cagionato dalle cose che ha in custodia, salvo che provi il caso fortuito*".

Si tratta di una forma di responsabilità oggettiva, in quanto anch'essa prescinde dall'accertamento dell'elemento soggettivo e consente al colui che ha il governo della *res* di andare esente da responsabilità solo dimostrando il caso fortuito.[102]

I presupposti affinché possa applicarsi l'art. 2051 c.c. è che il danno sia causato dalla cosa in quanto tale, e non da una condotta umana, e che vi sia un rapporto di custodia inteso come relazione tra il soggetto e la cosa che si sostanzia nel potere del primo di controllo su di essa e nella possibilità di governare i rischi ne derivano.

I principi fondamentali in tema di responsabilità da cose in custodia sono stati recentemente definiti dalle Sezioni Unite della Suprema Corte di cassazione con l'ordinanza n. 20943 del 2022.

---

[102] Cass. civ. n. 26533/2017 ove si specifica che il caso fortuito deve essere inteso in senso molto ampio, tale da ricomprendere anche il fatto naturale (la c.d. forza maggiore), il fatto del terzo ed il fatto dello stesso danneggiato, purché costituisca la causa esclusiva del danno.

In particolare, la Suprema Corte ha chiarito che "*l'art. 2051 c.c., nel qualificare responsabile chi ha in custodia la cosa per i danni da questa cagionati, individua un criterio di imputazione della responsabilità che prescinde da qualunque connotato di colpa, sicché incombe al danneggiato allegare, dandone la prova, il rapporto causale tra la cosa e l'evento dannoso, indipendentemente dalla pericolosità o meno o dalle caratteristiche intrinseche della prima; la deduzione di omissioni, violazioni di obblighi di legge di regole tecniche o di criteri di comune prudenza da parte del custode rileva ai fini della sola fattispecie dell'art. 2043 c.c., salvo che la deduzione non sia diretta soltanto a dimostrare lo stato della cosa e la sua capacità di recare danno, a sostenere allegazione e prova del rapporto causale tra quella e l'evento dannoso; il caso fortuito, rappresentato da fatto naturale o del terzo, è connotato da imprevedibilità ed inevitabilità, da intendersi però da un punto di vista oggettivo e della regolarità causale (o della causalità adeguata), senza alcuna rilevanza della diligenza o meno del custode; peraltro le modifiche improvvise della struttura della cosa incidono in rapporto alle condizioni di tempo e divengono, col trascorrere del tempo dall'accadimento che le ha causate, nuove intrinseche condizioni della cosa stessa, di cui il custode deve rispondere; il caso fortuito, rappresentato dalla condotta del danneggiato, è connotato dall'esclusiva efficienza causale nella produzione dell'evento; a tal fine, la condotta del danneggiato che entri in interazione con la cosa si atteggia diversamente a seconda del grado di incidenza causale sull'evento dannoso, in*

applicazione anche ufficiosa dell'art. 1227 c.c., comma 1; e deve essere valutata tenendo anche conto del dovere generale di ragionevole cautela riconducibile al principio di solidarietà espresso dall'art. 2 Cost. Pertanto, quanto più la situazione di possibile danno è suscettibile di essere prevista e superata attraverso l'adozione da parte dello stesso danneggiato delle cautele normalmente attese e prevedibili in rapporto alle circostanze, tanto più incidente deve considerarsi l'efficienza causale del comportamento imprudente del medesimo nel dinamismo causale del danno, fino a rendere possibile che detto comportamento interrompa il nesso eziologico tra fatto ed evento dannoso, quando lo stesso comportamento, benché astrattamente prevedibile, sia da escludere come evenienza ragionevole o accettabile secondo un criterio probabilistico di regolarità causale; con specifico riferimento al tema della rilevanza, all'interno della responsabilità di cui all'art. 2051 c.c., degli obblighi di diligenza incombenti in capo al custode e del loro rilievo ai fini dell'esonero della responsabilità, deve ritenersi che, una volta che il danneggiato abbia prospettato e provato il nesso causale tra cosa custodita ed evento dannoso, la colpa o l'assenza di colpa del custode resta del tutto irrilevante ai fini della sua responsabilità ai sensi dell'art. 2051 c.c.".

All'interno di tale modello di imputazione della responsabilità, l'esonero non può fondarsi esclusivamente sulla prova dell'adozione di tutte le cautele tecnicamente esigibili per prevenire l'evento dannoso.

È invece necessario che il soggetto onerato dimostri l'intervento di un fattore esterno idoneo a interrompere il nesso causale, riconducibile alla nozione di caso fortuito nei termini sopra delineati.

Sebbene tale impostazione risulti indubbiamente più favorevole alla posizione dei danneggiati rispetto a quella precedentemente esaminata, essa presenta rilevanti criticità sul piano sistemico.

In particolare, il carico di responsabilità che ne deriva rischia di risultare sproporzionato per le imprese operanti in contesti caratterizzati da un'elevata esposizione al rischio informatico, conducendo a una sostanziale automatizzazione della responsabilità ogniqualvolta il danno trovi origine nelle infrastrutture tecnologiche da esse controllate.

Una simile soluzione normativa presenta, inoltre, il pericolo di incidere negativamente sui processi di sviluppo e adozione dell'innovazione tecnologica, potendo scoraggiare gli operatori economici dall'impiego di strumenti avanzati per il timore di un'elevata probabilità di imputazione di responsabilità per i danni eventualmente derivanti dal loro utilizzo.

In definitiva, l'analisi dei diversi regimi di responsabilità, dall'art. 2050 c.c. per le attività pericolose all'art. 2051 c.c. per le cose in custodia, mostra come il diritto civile italiano offra strumenti flessibili per la tutela del danneggiato, ma che al contempo pongono importanti limiti agli operatori, soprattutto in ambiti ad elevato rischio informatico.

L’applicazione di tali istituti al rischio cibernetico evidenzia una tensione intrinseca tra la necessità di rafforzare la protezione dei soggetti lesi e quella di evitare un’eccessiva automatizzazione della responsabilità, che potrebbe incidere negativamente sull’innovazione tecnologica e sullo sviluppo economico. Ne consegue che l’interpretazione giurisprudenziale e dottrinale deve operare un delicato bilanciamento, calibrando l’onere di diligenza richiesto agli operatori e la responsabilità effettiva in funzione della prevedibilità e del controllo dei rischi informatici.

1.2. Responsabilità per prodotti difettosi

Nel contesto della cybersicurezza, un profilo di responsabilità di crescente rilevanza è rappresentato dalla responsabilità da prodotto difettoso.

Dopo aver considerato le possibilità di inquadramento in termini di responsabilità extracontrattuale ex artt. 2043, 2050 e 2051 c.c., con la conseguente individuazione dei limiti e delle criticità, l’attenzione si sposta su un modello di responsabilità che pone al centro la sicurezza del prodotto immesso sul mercato e le legittime aspettative dell’utilizzatore finale.

Nella società moderna, caratterizzata da processi produttivi complessi e standardizzati e dalla produzione e fabbricazione su larga scala, il propagarsi di danni legati ai prodotti è un fenomeno diffuso e rilevante che ha reso necessario non solo assicurare un efficace risarcimento a coloro che subiscano

dei pregiudizi, ma anche distribuire in maniera razionale gli alti oneri economici connessi a tali danni.[103]

Storicamente, prima dell'introduzione di discipline speciali in materia di prodotti difettosi, la responsabilità per i danni cagionati da beni immessi sul mercato era ricondotta alle norme generali della responsabilità civile, fondate in via prevalente sull'accertamento dell'elemento soggettivo. In tale contesto, la dottrina civilistica italiana ha a lungo sostenuto il principio secondo cui *non può esservi responsabilità senza colpa*, ritenendo che l'imputazione del danno dovesse necessariamente fondarsi su un comportamento colposo o doloso dell'autore.

Questa impostazione, pur rispettando fedelmente il dato letterale, rischiava di non tener conto di tutti i limiti della sua applicazione e ha gradualmente incrementato la necessità di rivedere le regole tradizionali, al fine di trovare un delicato equilibrio tra la tutela dei cittadini, titolari di diritti e libertà fondamentali, e gli interessi delle imprese.[104]

---

[103] Sul punto si veda, R. PARDOLESI, D. CARUSA, in *Per una storia della Direttiva 1985/374/CEE*, in *Danno e resp.,* 2012.

[104] G. ALPA, A. CATRICALÀ, in *Il diritto dei consumatori,* Il mulino, p. 423 ove è autorevolmente messo in luce che " *a*) ogni sistema fondato sulla colpa è viziato da veri e propri *pregiudizi*, di natura storica e di natura ideologica; *b*) il ricorso a tecniche di colpa «presunta» è frutto di un'anacronistica *fictio juris*, e comporta, pertanto, un errore «logico» nell'interpretazione delle norme giuridiche; *c*) il sistema fondato sulla colpa esclude ogni tentativo di assicurare una razionale distribuzione del rischio; *d*) il sistema fondato sulla colpa ha un costo «sociale» molto più alto del costo dei sistemi fondati su altri criteri di imputazione, in particolare dei

Tale revisione, come già anticipato, ha condotto all'affermazione di principi di responsabilità che accollano il rischio connesso al danno da prodotto direttamente all'impresa.

Il ricorso a criteri oggettivi di imputazione non è certamente estraneo all'esperienza giuridica italiana, nonostante se ne rinvengano già nel Codice civile significative manifestazioni.

Anche nella specifica materia della circolazione di prodotti difettosi le ricostruzioni volte ad allinearsi ai criteri di responsabilità senza colpa sono rimaste isolate per lungo tempo.

Parte della dottrina ha per esempio ancorato la responsabilità oggettiva alle sole imprese di grandi dimensioni [105] oppure ha proposto di applicare il criterio oggettivo solo in caso di danni derivanti da difetti di produzione o per omessa

---

sistemi informati al principio del rischio d'impresa (responsabilità oggettiva). Sulla problematica del bilanciamento tra la tutela dei consumatori e l'interesse dell'impresa, nel primo considerando della Direttiva 85/374/CEE si legge che "il ravvicinamento delle legislazioni nazionali in materia di responsabilità del produttore per i danni causati dal carattere difettoso dei suoi prodotti è necessario perché le disparità esistenti fra tali legislazioni possono falsare il gioco della concorrenza e pregiudicare la libera circolazione delle merci all'interno del mercato comune determinando disparità nel grado di protezione del consumatore contro i danni causati alla sua salute e ai suoi beni da un prodotto difettoso".

Sul punto, si veda anche G. ALPA, in *L'attuazione della direttiva nei Paesi della CEE,* in *La responsabilità del produttore (a cura di Alpa, Bin, Cendon),* XIII, in *Trattato di diritto commerciale di diritto pubblico dell'economia diretto da Galgano,* Padova, 1989, pp. 17 e ss.

[105] C. GHIDINI, in *Prevenzione e risarcimento nella responsabilità del produttore,* in *Riv. Soc.,* 1975, pp. 1530 e ss; M. FRANZONI, in *L'illecito*, in *Trattato della responsabilità civile*, 2010, p. 648.

informazione, escludendo i difetti di progettazione per non rendere l'onere dell'impresa eccessivamente gravoso. [106]

Diverso è stato l'approccio dell'Unione europea che, a seguito di diversi tentativi, ha elaborato la Direttiva 85/374/CEE, concepita per rafforzare il mercato unico attraverso un equilibrato bilanciamento tra gli interessi dei consumatori e quelli dei produttori.

Tale Direttiva è stata successivamente recepita nell'ordinamento italiano nel Codice del consumo (d.lgs. n. 206/2005), in particolare negli artt. 114 e ss., che disciplinano la responsabilità del produttore per i danni cagionati da prodotti difettosi, delineando un regime speciale volto a rafforzare la tutela dei soggetti danneggiati, il cui principio cardine della è che "il produttore è responsabile del danno causato da un difetto del suo prodotto". Intendendo per prodotto "ogni bene mobile, ad eccezione dei prodotti agricoli naturali e dei prodotti della caccia, anche se forma parte di un altro bene mobile o immobile" (art. 2) e per produttore il "fabbricante di un prodotto finito, il produttore di una materia prima o il fabbricante di una parte componente, nonché ogni persona che, apponendo il proprio nome, marchio o altro segno distintivo sul prodotto, si presenta come produttore dello stesso." (art. 3).

---

[106] Così U. CARNEVALI, in *La responsabilità del produttore,* Milano, 1974. P. TRIMARCHI, in *Istituzioni di diritto privato,* Milano, 1973, p. 160.

Secondo l'orientamento dottrinale maggioritario tale sistema introduce una vera e propria responsabilità oggettiva e diretta del produttore, e non già una responsabilità per colpa presunta: il danneggiato è tenuto a provare il pregiudizio subito, il difetto del prodotto e il nesso causale tra difetto e danno, ma non anche l'elemento soggettivo. [107]

La colpa del produttore non è mai menzionata, non è ammessa la possibilità di prova liberatoria, né la dimostrazione di aver adottato tutte le misure necessarie per evitare il danno.

Gli unici contemperamenti della responsabilità sono rappresentati dalle cause di esclusione o esonero di responsabilità [108] previste dal legislatore.

Per quanto riguarda il campo soggettivo di applicazione, la normativa si rivolge principalmente ai consumatori definiti, ai sensi dell'art. 18 Cod. cons., le persone fisiche che agiscono per scopi estranei all'attività commerciale, industriale, artigianale o professionale eventualmente svolta. Il legislatore ha dunque inteso tutelare il contraente debole nei rapporti B2C, prevedendo

---

[107] Sul punto si veda F. MACIOCE, in *Responsabilità del produttore, armonizzazione dei mercati e prospettive di riforma nell'ottica della tutela del consumatore,* in *Responsabilità, Comunicazione, Impresa,* 2005, 1, p. 28; G. SIMONINI, in *La responsabilità da prodotto e l'interpretazione conforme al diritto comunitario,* in *Contratto e impresa,* 2013, 1, p. 220.

[108] P. TRIMARCHI, in *La responsabilità del fabbricante nella direttiva comunitaria,* in *Riv. Soc.,* 1986, p. 596. L'Autore sottolinea come l'area della responsabilità oggettiva possa essere in parte ridimensionata contemperando il principio generale con le regole di sicurezza del prodotto, richiedibili al produttore secondo criteri di ragionevolezza e considerazioni di tutti i costi di produzione e dei prezzi per il pubblico.

strumenti di protezione rafforzata rispetto al diritto comune della responsabilità civile.

Elemento cardine della disciplina è la nozione di difettosità del prodotto, prevista dall'art. 117 Cod. cons e dall'art. 6 della Direttiva, per cui un prodotto è difettoso quando non offre la sicurezza che ci si può legittimamente attendere, tenuto conto di tutte le circostanze. Così viene superata la concezione tradizionale di vizio materiale o strutturale: un prodotto può risultare formalmente integro e funzionante, ma comunque inidoneo a garantire il livello di sicurezza che l'utilizzatore può ragionevolmente aspettarsi. [109]

La giurisprudenza ha ulteriormente precisato che la valutazione della difettosità si fonda, in particolare, su tre profili: i difetti di fabbricazione, i difetti di progettazione e i difetti di informazione, comprendendo in quest'ultima categoria anche l'inadeguatezza o la carenza di avvertenze o istruzioni adeguate circa l'uso sicuro del prodotto.[110]

Quanto all'oggetto del risarcimento, la responsabilità del produttore copre i danni derivanti dalla morte o da lesioni personali, nonché dalla distruzione o

---

[109] Per una definizione si veda anche CGUE C-503/13 in *https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62013CJ0503* e Cass. 8224/2025 in cui si specifica che la nozione di difetto esprime un significato ambivalente "che si traduce sia nella sicurezza del prodotto da apprezzarsi rispetto agli standards richiesti dalla normativa di settore sia in una concezione in termini relazionali, da apprezzarsi in base alle legittime aspettative del consumatore".

[110] Sul punto, si veda Cass. civ. n. 33984/2024.

dal deterioramento di cose diverse dal prodotto difettoso, purché normalmente destinate all'uso o al consumo privato e principalmente utilizzate dal danneggiato a tale scopo. [111]

Si tratta, dunque, di un concetto di danno più ampio rispetto al tradizionale vizio del bene, poiché riconosce rilevanza anche agli effetti indiretti del difetto sulla sfera personale del soggetto.

Tale regime presenta significative differenze rispetto alla responsabilità per l'esercizio di attività pericolose di cui all'art. 2050 c.c., che configura una presunzione di responsabilità sostanzialmente oggettiva. In tale ambito, infatti, per andare esente da responsabilità non è sufficiente per il danneggiante dimostrare il rispetto della normativa vigente o l'assenza di negligenza, essendo invece necessario provare di aver adottato tutte le misure idonee a prevenire il danno. L'obbligo di prevenzione si estende anche all'impiego di soluzioni tecniche astrattamente disponibili secondo lo stato dell'arte, comprese quelle non ancora concretamente applicate o riconoscibili al momento dell'esercizio dell'attività o dell'immissione in commercio del prodotto.

Il giudizio di responsabilità si fonda, pertanto, su una valutazione *ex post* delle conoscenze tecnico-scientifiche del settore, imponendo un dovere di massima

[111] Art. 123 d.lgs. 206/2005.

cautela, di costante aggiornamento e, in presenza di incertezza scientifica, persino di astensione dall'immissione del bene sul mercato. [112]

Diversamente, nell'ambito della responsabilità del produttore, il legislatore ha previsto una più equilibrata ripartizione dei rischi connessi all'immissione del prodotto sul mercato, individuando all'art. 118 Cod. cons. una serie di cause tipiche di esonero dalla responsabilità.

Tra queste, assume particolare rilievo l'esimente cd. "rischio da sviluppo" che "*conforta la nozione di difettosità, fonte di responsabilità, come una difettosità originaria, sia da un punto di vista ontologico, ma anche da quello della percezione che di essa, in quel momento ragionevolmente abbia il produttore*".[113]

---

[112] Cass. civ. n. 32498/2019 che sottolinea come "*la prova liberatoria si identifica indirettamente nel caso fortuito*".

[113] Cass. civ. n. 8224/2025 che prosegue "*Il produttore beneficia di una mitigazione dell'onere probatorio a suo carico, potendo sottrarsi alla responsabilità, se gli studi disponibili al momento della messa in circolazione del prodotto non consentissero di risalire alla matrice dei potenziali danni connessi all'uso dello stesso, in ragione di una situazione di incertezza scientifica. In questo contesto l'assenza di leggi scientifiche o esperienziali esplicative dei nessi tra i potenziali danni e l'impiego del prodotto, non si ripercuote sul produttore. Infatti, non gli preclude l'immissione in commercio del prodotto, che sulla base di un'analisi comparativa rischi-benefici, risulti complessivamente più sicuro che pericoloso, non potendo ridondare a suo danno lo sviluppo delle conoscenze scientifiche sul punto. (...) Dunque, il concetto di difettosità, delineato dal codice del consumo, e quello di pericolosità ai sensi dell'art. 2050 c.c., non coincidono necessariamente. Un prodotto può essere considerato pericoloso a causa della sua natura intrinsecamente dannosa, ma al contempo risultare sicuro secondo i parametri stabiliti dall'art. 117 cod. cons*."

Questa esonera il produttore quando il difetto non poteva essere rilevato con le conoscenze scientifiche e tecniche disponibili al momento dell'immissione del prodotto sul mercato, profilo particolarmente significativo per i prodotti digitali e i sistemi informatici nei quali il difetto può consistere in vulnerabilità di sicurezza emerse successivamente, anche in relazione all'evoluzione delle tecnologie.

La questione dell'applicabilità della responsabilità da prodotto difettoso nel settore della cybersicurezza, e più in generale nel settore dei prodotti tecnologicamente avanzati, rappresenta uno dei temi maggiormente dibattuti nella riflessione dottrinale contemporanea.

L'emersione delle nuove tecnologie solleva, infatti, problematiche inedite che incidono profondamente sulle modalità di regolazione della società, imponendo di volta in volta l'elaborazione di nuove regole ovvero l'adattamento di quelle esistenti. [114]

In tale contesto, ci si interroga sul ruolo che la disciplina della responsabilità da prodotto difettoso può svolgere nell'affrontare le criticità connesse all'utilizzo delle tecnologie emergenti.

Occorre, in primo luogo, considerare come la fiducia riposta dalle istituzioni europee in tale strumento normativo sembri entrare in tensione, da un lato, con

---

[114] Sul tema del rapporto tra sistema giuridico ed evoluzione tecnologica, si veda S. RODOTÀ, in *Tecnologie dell'informazione e frontiere del sistema socio-politico,* in *Pol. Dir.,* 1982, pp. 25 e ss.

le soluzioni adottate da diversi Stati membri, spesso orientati verso una sorta di *fuga* dalla disciplina del prodotto difettoso,[115] dall'altro con il crescente ricorso alla *soft law*, la quale negli ultimi anni è stata privilegiata in quanto ritenuta maggiormente idonea a reagire alla rapida evoluzione delle condizioni di mercato e alle nuove esigenze regolatorie. [116]

Tuttavia, l'impiego della *soft law* incontra limiti significativi, primo fra tutti l'assenza di efficacia giuridicamente vincolante, nonché il rischio di disallineamenti rispetto alle scelte operate dal legislatore.

Ne consegue la necessità di preservare il primato della fonte legislativa, pur dotando gli interpreti di strumenti flessibili e adeguati a confrontarsi con l'innovazione tecnologica. [117]

---

[115] Si fa riferimento all'orientamento invalso nelle corti italiane ad utilizzare altre forme di responsabilità (quale ad esempio quella prevista dall'art. 2050 c.c.) per offrire soluzioni ai problemi che emergono con la produzione di massa. Sul punto si vedano, A. PARZIALE, in *Art. 2050 c.c.: dieci anni vissuti… pericolosamente*., in *Danno resp.,* 2019, pp. 118 e ss; A. FUSARO, in *Attività pericolose e dintorni. Nuove applicazioni dell'art. 2050 c.c.*, in *Riv. dir. civ.,* 2013, pp. 1339 e ss.

[116] C. ROSSELLO, in *Commercio elettronico. La governance di internet tra diritto statuale, autodisciplina e soft law,* Giuffrè Editore, Milano, 2006.

[117] N. IRTI, in *Una generazione di giuristi,* in *La cultura del diritto civile,* Torino, 1990, pp. 70 e ss.

Parallelamente, si assiste alla progressiva emersione di discipline settoriali che, attraverso linee guida e buone pratiche, mirano a fronteggiare rischi specifici, come avviene nel caso della cybersicurezza.[118]

Uno dei nodi centrali della riflessione riguarda, tuttavia, la definizione stessa di "prodotto", tradizionalmente riferita a beni materiali, e la possibilità di estendere l'ambito applicativo della disciplina ai danni causati da prodotti tecnologicamente sofisticati di natura digitale.

La complessità deriva dal fatto che tali prodotti sono spesso costituiti non solo da componenti materiali, ma anche da *software*, applicazioni, sistemi cloud e altre soluzioni tecnologiche immateriali, talvolta integrate con servizi. [119]

A ciò si aggiunge che tali prodotti sono caratterizzati da un'elevata dinamicità, essendo soggetti a continui aggiornamenti e modificazioni, spesso indispensabili per garantirne il corretto funzionamento.

Ancora più problematico è il caso dei cosiddetti prodotti intelligenti, capaci di assumere decisioni autonome: in tali ipotesi le difficoltà riguardano non solo

---

[118] A.M. GAMBINO, in *Diritti fondamentali e Cybersecurity,* in M. BIANCA, A.M. GAMBINO, R. MESSINETTI, *Libertà di manifestazione del pensiero e diritti fondamentali,* 2016, pp. 21 e ss

[119] G. ALPA, in *La responsabilità del produttore*, Milano, 1999, p. 246. In argomento, v. anche, J.P. TRIAILLE**,** in *L'applicazione della Direttiva comunitaria sulla responsabilità del produttore nel campo del* software, in *Dir. inf.*, 1990, 2, p. 725.

l'individuazione del soggetto giuridicamente responsabile, ma anche l'intrinseca imprevedibilità delle interazioni con l'ambiente esterno. [120]

Ci si interroga, dunque, se la nozione di "prodotto" accolta dalla Direttiva sulla responsabilità per danno da prodotti difettosi, e conseguentemente recepita negli ordinamenti nazionali, sia ancora idonea a governare le profonde innovazioni introdotte dallo sviluppo tecnologico, in particolare con riferimento a beni digitali, software e sistemi caratterizzati da elevata complessità e autonomia funzionale.

Una prima impostazione, ancorata al dato letterale della normativa, tende a circoscrivere il concetto di prodotto ai soli beni materiali, anche in ragione del timore che un'eccessiva estensione dell'ambito applicativo della Direttiva possa condurre a uno sconfinamento rispetto alla sua originaria *ratio*.

Tale lettura restrittiva, tuttavia, rischia di risultare inadeguata rispetto alle trasformazioni della realtà economica e tecnologica, finendo per limitare l'operatività della disciplina ai soli beni tradizionali.[121]

Parte autorevole della dottrina ha infatti evidenziato come un simile approccio determini un evidente scollamento tra la normativa e la società contemporanea

---

[120] Per una riflessione elaborata sul tema della responsabilità dei prodotti intelligenti, si veda U. RUFFOLO, in *Intelligenza artificiale e responsabilità (a cura di U. RUFFOLO)*, Giuffrè Editore, 2017.

[121] A. ZACCARIA, in *La responsabilità del produttore di software,* in *Contr. e impr.,* 1993, p. 302; A. ALBANESE, in *La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione*, in *Europa e diritto privato*, 4/2019, p. 1023.

nella quale il valore economico e funzionale del prodotto risiede sempre più spesso in componenti immateriali.

Emblematico è il caso del *software*, rispetto al quale l'interesse del consumatore non è rivolto al supporto materiale che eventualmente lo incorpora, bensì all'informazione e alle funzionalità che garantiscono il conseguimento di un determinato risultato pratico.

Condizionare l'applicabilità della disciplina della responsabilità da prodotto difettoso alla presenza di un supporto materiale, peraltro talvolta del tutto evanescente o non identificabile, appare oggi una soluzione eccessivamente limitativa e difficilmente sostenibile.

Risulta pertanto preferibile un'interpretazione evolutiva della nozione di prodotto, idonea a ricomprendere anche beni immateriali, indipendentemente dal fatto che essi siano o meno incorporati in un bene materiale.

Ciò che rileva non è la natura tangibile del bene ma il fatto che tali elementi siano concepiti e percepiti come parte integrante del prodotto, tanto dal produttore o fabbricante quanto dall'utilizzatore finale.

In questa prospettiva, l'estensione della disciplina della responsabilità da prodotto difettoso ai danni cagionati da componenti immateriali non rappresenta uno stravolgimento del sistema, bensì un necessario adattamento funzionale volto a preservarne l'effettività nel contesto attuale.

Un'interpretazione estensiva della nozione di prodotto incide inevitabilmente anche sulla configurazione soggettiva della responsabilità, consentendo un

ampliamento della nozione stessa di produttore. Qualora il prodotto venga inteso come un insieme funzionale di componenti materiali e immateriali, risulta coerente ricomprendere tra i soggetti responsabili anche coloro che, pur non avendo fabbricato il bene fisico, esercitano un ruolo determinante nella progettazione, nello sviluppo, nella fornitura o nell'aggiornamento delle componenti digitali che ne condizionano la sicurezza.

In tale prospettiva, l'attribuzione della responsabilità non si fonda più esclusivamente sulla materiale fabbricazione del bene, ma sul controllo effettivo del rischio tecnologico e sulla capacità di incidere sulle caratteristiche del prodotto.

Una spinta significativa, seppur non ancora pienamente risolutiva, verso l'inclusione dei beni digitali nell'ambito della responsabilità da prodotto difettoso proviene dalla Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 che, abrogando la Direttiva 85/374/CEE, prende atto delle trasformazioni del mercato e dell'emersione di nuovi fattori di rischio connessi alla digitalizzazione e alla crescente centralità della sicurezza informatica.

Il Considerando n. 13 chiarisce infatti che "*I prodotti nell'era digitale possono essere tangibili o intangibili. Sul mercato è sempre più diffuso il software, come i sistemi operativi, il firmware, i programmi per computer, le applicazioni o i sistemi di IA, e la sua importanza a fini di sicurezza dei prodotti è sempre maggiore. Il software può essere immesso sul mercato come prodotto a sé*

stante o può essere poi integrato in altri prodotti come componente e può causare danni dovuti al suo funzionamento. Per garantire la certezza del diritto è opportuno chiarire nella presente direttiva che, ai fini dell'applicazione della responsabilità oggettiva, il software è un prodotto, a prescindere dalle modalità con cui viene fornito o usato, e quindi dal fatto che il software sia integrato in un dispositivo, utilizzato tramite una rete di comunicazione o tecnologie cloud oppure sia fornito attraverso un modello software-as-a-service. Le informazioni, invece, non devono invece essere considerate un prodotto e le norme sulla responsabilità per danno da prodotti difettosi non dovrebbero pertanto applicarsi al contenuto dei file digitali, quali file multimediali, e-book o il mero codice sorgente dei software. Il produttore o lo sviluppatore di software, compreso il fornitore di sistemi di IA ai sensi del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, dovrebbe essere considerato un fabbricante."

Pur avendo una rilevanza sistematica evidente, tale Direttiva non è ancora recepita nell'ordinamento interno.

Ne consegue che, allo stato attuale, l'applicazione della responsabilità da prodotto difettoso ai danni derivanti da violazioni della cybersicurezza rimane affidata a un'interpretazione evolutiva della disciplina vigente, la quale mette in luce i limiti del modello tradizionale nella gestione di rischi digitali caratterizzati da immaterialità, dinamicità e continua evoluzione.

Tale scenario solleva alcune questioni giuridiche centrali.

In tale prospettiva, il concetto di prodotto, tradizionalmente riferito a beni materiali, risulta sempre meno adeguato a descrivere sistemi digitali complessi, dispositivi connessi e infrastrutture interattive, nei quali componenti immateriali quali software e firmware incidono in modo determinante sul funzionamento e, soprattutto, sulla sicurezza complessiva del bene. Un difetto in tali componenti può infatti provocare danni analoghi a quelli derivanti da un vizio fisico tradizionale.

Dal punto di vista giuridico, si pone dunque la questione se tali componenti possano essere considerati parte integrante del prodotto e se, conseguentemente, la responsabilità del produttore possa estendersi anche a difetti non tangibili, ma funzionali alla sicurezza complessiva del bene.

In questo contesto, la nozione di sicurezza, fondamento della responsabilità del produttore, assume un significato ampliato che coincide con la cybersicurezza: non più soltanto protezione fisica del prodotto, ma tutela dei sistemi, dei dati e delle reti da accessi non autorizzati, manipolazioni o attacchi informatici.

Un difetto può dunque consistere nella vulnerabilità di un componente digitale o nella carenza di misure di sicurezza adeguate, compromettendo la protezione dell'utilizzatore anche in assenza di difetti materiali. Ne deriva che la valutazione della difettosità deve tenere conto non solo delle caratteristiche intrinseche del prodotto, ma anche della prevedibilità dei rischi informatici, della probabilità di attacco e della diligenza tecnologica esigibile dal produttore.

Ulteriore profilo problematico concerne il momento in cui valutare la difettosità.

Nel caso dei beni tradizionali, tale valutazione si fonda sul prodotto così come immesso sul mercato; i sistemi digitali, invece, possono essere aggiornati, modificati o gestiti dinamicamente anche dopo la commercializzazione.

Resta da valutare se, e in quale misura, il produttore possa essere ritenuto responsabile per difetti che si manifestino successivamente all'immissione del prodotto sul mercato, pur in presenza di una originaria conformità agli standard tecnici e alle conoscenze scientifiche disponibili in quel momento

Si tratta qui di rivoluzionare la prospettiva tradizionale secondo cui il produttore/fabbricante è tenuto al controllo sino al momento dell'immissione in commercio e di considerare che anche i prodotti più sofisticati comunque si limitano a mansioni e compiti per cui sono stati progettati.

A ciò si aggiunga la complessità inerente all'onere della prova.[122]

Nei contesti caratterizzati da elevata complessità tecnologica risulta infatti particolarmente difficile per il danneggiato dimostrare sia il danno subito sia il nesso causale tra il difetto del prodotto e il pregiudizio.

---

[122] Sul profilo relativo alla prova del danno in relazione alle nuove tecnologie del danno, F. PÜTZ, F. MURPHY, M. MULLINS, K. MAIER, R. FRIEL, T. ROHLFS, in *Reasonable, Adequate and Efficient Allocation of Liability Costs for Automated Vehicles*, in *European Journal of Risk Regulation*, 2018, pp. 559 e ss.

Tuttavia, occorre considerare che molti di questi prodotti sono, o dovrebbero essere, dotati di sistemi di registrazione dei dati e di informazioni relative al loro funzionamento e alla manutenzione, strumenti che possono facilitare l'accertamento della responsabilità e ridurre le difficoltà probatorie.

Altro aspetto nodale concerne la distribuzione dei rischi e degli oneri economici.

Il modello tradizionale della responsabilità del produttore, fondato sulla presunzione oggettiva di responsabilità, presuppone un unico soggetto economicamente in grado di sopportare il rischio e di implementare misure di prevenzione. Nei sistemi digitali complessi, in cui la produzione e la gestione del bene coinvolgono più attori, sviluppatori di componenti, fornitori di piattaforme, integratori di sistemi, il principio di responsabilità oggettiva deve confrontarsi con la frammentazione delle funzioni, richiedendo criteri più sofisticati per individuare il soggetto responsabile e la misura del suo obbligo di sicurezza.

Queste riflessioni evidenziano la necessità di ridefinire i criteri di "sicurezza legittimamente attesa" nel contesto digitale, tenendo conto della rapidità dei cambiamenti tecnologici e dei rischi informatici emergenti, e aprono un dibattito sulla compatibilità tra il modello tradizionale di *product liability* e la protezione dei cittadini nei confronti dei beni digitali interconnessi.

Tali questioni non trovano ancora risposta definitiva nella normativa vigente e sollevano interrogativi centrali: la disciplina della responsabilità da prodotto

difettoso può essere realmente estesa ai beni digitali e ai rischi legati alla cybersicurezza? In che misura essa è in grado di garantire la tutela dell'utilizzatore, tenendo conto della complessità dei sistemi e della dinamicità delle componenti digitali?

Questi interrogativi costituiscono la base per un'analisi più approfondita e aprono la strada alla valutazione critica di possibili strumenti normativi complementari.

1.3. Responsabilità del prestatore di servizi digitali

La funzione della responsabilità civile varia a seconda delle prospettive da cui la si considera e in base ai settori e alle materie che si prendono in considerazione, ma sottende una *ratio* comune a tutti i casi in cui si verifica una perdita di valore, la lesione di un bene o di un interesse tutelato dall'ordinamento: la selezione dei danni risarcibili, la prevenzione o *deterrence* dei comportamenti illeciti e, in definitiva, la tutela della vittima dell'atto illecito.[123]

In materia di responsabilità civile, quindi, il percorso logico deve muovere dalla considerazione della finalità riparatoria e del livello di tutela che si intende garantire al danneggiato, per risalire alla costruzione del modello di responsabilità più adeguato al caso di specie.

---

[123] L. DI DONNA, in *Il principio di responsabilità nel settore dei beni e dei servizi*, in *Rivista italiana per le scienze giuridiche*, vol. speciale, 2014.

Questo ragionamento si applica sia alla responsabilità del produttore di beni sia a quella del prestatore di servizi digitali.

Nel caso del produttore, il modello oggettivo fondato sulla difettosità del prodotto si sta evolvendo per includere beni immateriali, software e componenti tecnologiche complesse. Tuttavia, anche in questa prospettiva, l'approccio *ex ante* basato sul difetto non sempre è sufficiente a fronteggiare rischi cibernetici che emergono a valle della commercializzazione, come vulnerabilità, aggiornamenti errati o attacchi sofisticati.

Diversamente, la responsabilità del prestatore di servizi digitali non rientra nel campo di applicazione della Direttiva sulla responsabilità del produttore. Infatti, il prestatore non "immette sul mercato" un bene finito, ma eroga un'attività continuativa, dinamica e gestita attivamente, che richiede l'adozione di misure tecniche, organizzative e procedurali per prevenire e gestire i rischi, inclusi quelli informatici. A differenza del prodotto, la sicurezza del servizio non è intrinseca e immutabile, ma il risultato di un processo operativo complesso.[124]

[124] Si evidenzia la Proposta della Commissione europea del 9 novembre 1990, inattuata, in cui si proponeva, vista la lacuna normativa, una specifica direttiva relativa alla responsabilità del prestatore di servizi, nell'ambito della normativa a tutela dei consumatori, seguendo il modello della Direttiva 85/374/CEE) (Proposal for a Council Directive on the liability of suppliers of services).

Il prodotto è generalmente definito come un bene materiale, finito e destinato alla commercializzazione, e la responsabilità del produttore si fonda sulla difettosità del bene, indipendentemente dalla diligenza del produttore stesso.

Il servizio, che viene di solito definito in negativo come tutto ciò che non ricade nella nozione di prodotto, è caratterizzato dalla dinamicità, continuità e gestione attiva e richiede al prestatore di adottare tutte le misure tecniche, organizzative e gestionali, idonee a prevenire e gestire i rischi, compresi quelli informatici.

La normativa europea e nazionale riconosce tale distinzione.

La Direttiva 2000/31/CE sul commercio elettronico, il Digital Services Act (Regolamento UE 2022/2065) e il GDPR (Regolamento UE 2016/679) attribuiscono al prestatore di servizi digitali obblighi di gestione, sicurezza, trasparenza e tutela dei dati, imponendo una responsabilità fondamentalmente colposa.

Il GDPR (Regolamento UE 2016/679, artt. 5 e 32) impone ai titolari e ai responsabili del trattamento dei dati di implementare misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali; il mancato rispetto di tali obblighi può dar luogo a responsabilità civile in capo al prestatore.[125]

---

[125] Art. 82 (Regolamento UE 2016/679) "1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del

Analogamente, il Digital Services Act (Regolamento UE 2022/2065) prevede obblighi di *risk assessment*, mitigazione e trasparenza, introducendo criteri concreti per valutare la diligenza del prestatore e determinare eventuali responsabilità.

Ancora a livello nazionale, il Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005) all'art. 30 stabilisce obblighi di responsabilità per i prestatori di servizi qualificati, prevedendo che ove cagionino danni ad altri nello svolgimento della loro attività siano tenuti al risarcimento del danno.

La disciplina sugli hosting provider (d.lgs. n. 70/2003) precisa che il prestatore può essere chiamato a risarcire danni derivanti dalla propria attività.

Sul piano dogmatico, la responsabilità del prestatore si ricondurrebbe dunque alla colpa, presunta o concreta, fondata sulla violazione dei doveri di diligenza e degli obblighi di settore.

---

trattamento o dal responsabile del trattamento. 2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile."

Tuttavia, l'applicazione di questo modello incontra limiti strutturali che investono la stessa idoneità di tale modulo a governare rischi tecnologici sistemici, dinamici e opachi senza produrre effetti fortemente distorsivi.

Tradizionalmente, la colpa presuppone tre elementi fondamentali: l'imputabilità del comportamento a un soggetto determinato, la prevedibilità del danno e la possibilità di evitarlo mediante un'azione diligente.

Nei servizi digitali complessi, quali quello della cybersicurezza, tuttavia, ciascuno di questi pilastri entra in crisi.

Il danno informatico può emergere da una molteplicità di fattori interconnessi: vulnerabilità di *software,* aggiornamenti difettosi, errori di configurazione, incidenti nelle reti o attacchi esterni.

In tali scenari, il concetto di "chi è responsabile?" si dissolve. [126]

La frammentazione dei ruoli, la molteplicità degli attori e la complessità tecnica rendono quasi impossibile individuare un singolo soggetto la cui condotta possa essere considerata colposa.

Il danno si manifesta spesso a valle di processi dinamici, di cui nessun singolo attore detiene piena cognizione, ponendo il problema della imputazione

---

[126] Per l'orientamento dottrinale maggioritario, l'imputabilità costituisce il presupposto indefettibile perché possa essere mosso un rimprovero morale al soggetto per non aver fatto uso delle proprie capacità per non evitare il danno. Sul punto, si veda U. RUFFOLO, in *La colpa*, in *Diritto civile, IV, Attuazione e tutela dei diritti. La responsabilità e il danno, a cura di N. LIPARI e P. RESCIGNO*, *coordinato da A. ZOPPINI,* Milano, 2009, 72; F. D. BUSNELLI, in *Illecito civile*, *in Enc. giur*., XV, Roma, 1991.

individuale sotto forte stress concettuale. L'evento lesivo non è giuridicamente riconducibile ad un unico soggetto né ad unica condotta, essendo il frutto di relazioni dinamiche difficilmente osservabili.

Parallelamente, il principio di prevedibilità del danno, fondamento della colpa, risulta compromesso. Le minacce evolvono rapidamente e in maniera spesso imprevedibile. Attacchi sofisticati, bug latenti e vulnerabilità emergenti sfuggono a qualsiasi valutazione *ex ante* basata su esperienze passate.

La colpa presuppone che il soggetto potesse prevedere l'evento dannoso. Nel cyberspazio, tale presupposto si confronta con limiti profondi: la complessità dei sistemi e l'evoluzione rapida delle tecnologie rendono il danno spesso non prevedibile e, quindi, non evitabile secondo criteri tradizionali.

Questa crisi del modello classico ha implicazioni teoriche e pratiche significative. Non si tratta solo di difficoltà probatorie, ma di un problema strutturale del diritto civile: il paradigma tradizionale fatica a governare rischi distribuiti, dinamici e interconnessi. La valutazione della responsabilità si sposta quindi dall'errore individuale all'adeguatezza complessiva delle misure tecniche, organizzative e procedurali adottate, pur restando formalmente ancorata alla colpa.

In altre parole, la responsabilità del prestatore si misura non solo sugli errori commessi, ma sull'adeguatezza complessiva delle misure organizzative, tecniche e procedurali implementate, anticipando una visione proattiva ed *ex ante.*

In definitiva, il modello di responsabilità per colpa, pur trovando applicazione anche ai prestatori di servizi digitali, mostra limiti strutturali di fronte alla complessità dei sistemi e alla dinamicità dei rischi cibernetici.

Rimane quindi aperto il quesito se tale modello tradizionale di responsabilità possa continuare a fornire un riferimento adeguato per i prestatori di servizi digitali oppure se la complessità dei sistemi e la natura dinamica dei rischi richiedano un ripensamento concettuale più profondo, alla stregua di quanto avvenuto per la responsabilità dei produttori.

È in questa tensione tra continuità e innovazione normativa che si colloca il tema centrale: comprendere fino a che punto gli strumenti esistenti siano effettivamente idonei a tutelare gli interessi dei destinatari dei servizi digitali, senza rinunciare ai principi fondamentali della responsabilità civile.

1.4. Il danno informatico

L'espressione "danno cyber", ampiamente utilizzata nel linguaggio tecnico e nel dibattito regolatorio, non individua una categoria autonoma di danno giuridicamente rilevante, ma costituisce una formula descrittiva idonea a ricomprendere una pluralità di pregiudizi derivanti da incidenti di sicurezza informatica.

In ambito civilistico, il problema centrale non è dunque quello di individuare un nuovo tipo di danno, quanto piuttosto di verificare in che modo le categorie tradizionali del danno risarcibile siano in grado di assorbire e disciplinare le

conseguenze pregiudizievoli degli attacchi informatici, alla luce delle peculiarità del rischio tecnologico.

In conformità all'impostazione codicistica prevalente, l'attacco informatico non può essere qualificato come danno in sé, bensì come fatto lesivo.

Il danno risarcibile resta il danno-conseguenza, rilevante nei limiti tracciati dagli artt. 1223 e 2056 c.c., e deve consistere in una perdita o mancata utilità giuridicamente apprezzabile.[127]

---

[127] *Ex multis*, sulla distinzione tra danno evento e danno conseguenza, in tema di responsabilità aquiliana, Cass. n. 576/2008, in cui si legge "… ai fini della responsabilità civile ciò che si imputa è il danno e non il fatto in quanto tale. E tuttavia un "fatto" è pur sempre necessario perché la responsabilità sorga, giacché l'imputazione del danno presuppone l'esistenza di una delle fattispecie di cui agli artt. 2043 e segg. C.c. (…). Il "danno" rileva così sotto due profili diversi: come evento lesivo e come insieme di conseguenze risarcibili, retto il primo dalla causalità materiale ed il secondo da quella giuridica. Il danno oggetto dell'obbligazione risarcitoria aquiliana è quindi esclusivamente il danno conseguenza del fatto lesivo (di cui è un elemento l'evento lesivo). Se Sussiste solo il fatto lesivo, ma non vi è un danno-conseguenza, non vi è l'obbligazione risarcitoria. Proprio in conseguenza di ciò si è consolidata nella cultura giuridica contemporanea l'idea, sviluppata soprattutto in tema di nesso causale, che esistono due momenti diversi del giudizio aquiliano: la costruzione del fatto idoneo a fondare la responsabilità (per la quale la problematica causale, detta causalità materiale o di fatto, presenta rilevanti analogie con quella penale, artt. 40 e 41 c.p., ed il danno rileva solo come evento lesivo) e la determinazione dell'intero danno cagionato, che costituisce l'oggetto dell'obbligazione risarcitoria. A questo secondo momento va riferita la regola dell'art. 1223 c.c (richiamato dall'art. 2056 c.c.), per il quale il risarcimento deve comprendere le perdite "che siano conseguenza immediata e diretta" del fatto lesivo (c.d. causalità giuridica), per cui esattamente si è dubitato che la norma attenga al nesso causale e non piuttosto alla determinazione del quantum del risarcimento, selezionando le conseguenze dannose risarcibili."

Tale distinzione assume un rilievo particolare nel contesto cyber, ove il rischio potrebbe essere quello di confondere l'evento tecnico (intrusione, *malware*, *data breach*) con il pregiudizio giuridico, anticipando indebitamente la soglia della responsabilità.

Sotto il profilo patrimoniale, il danno da attacco informatico si manifesta in forme molteplici, riconducibili tanto al danno emergente quanto al lucro cessante.[128]

Rientrano nel primo, ad esempio, i costi sostenuti per il ripristino dei sistemi informativi compromessi, per la messa in sicurezza delle infrastrutture digitali, per l'adozione di misure correttive e organizzative, nonché le spese relative al (necessario) ricorso a consulenti informatici e legali specializzati.

Il lucro cessante può invece consistere nella perdita di profitti conseguente all'interruzione o al rallentamento dell'attività economica, alla sospensione di servizi digitali essenziali o alla temporanea perdita di accesso ai dati necessari per l'esercizio dell'impresa.

Inoltre, è possibile anche immaginare che il danno da attacco informatico possa assumere la forma della cd perdita di chance [129], in particolare quando

---

[128] Art. 1223 c.c. "Il risarcimento del danno per l'inadempimento o per il ritardo deve comprendere così la perdita subita dal creditore come il mancato guadagno, in quanto ne siano conseguenza immediata e diretta."

[129] Per la ricostruzione civilistica del danno da perdita di chance e sul superamento delle teorie eziologica ed ontologica v., *ex multis*, Cass. n. 18568/2024, in *italgiure.it.*

l'incidente comprometta la capacità dell'operatore di competere efficacemente sul mercato o di partecipare a future opportunità economiche.

Accanto ai profili patrimoniali, assume rilievo crescente il danno non patrimoniale (e cioè quel danno determinato dalla lesione di interessi della persona non connotati da rilevanza economica[130]), configurabile soprattutto nei casi in cui l'attacco informatico determini una violazione dei dati personali.

Sul punto, sembra opportuno il riferimento all'art. 82 del Regolamento (UE) 2016/679 (GDPR), rubricato *Diritto al risarcimento e responsabilità,* il quale disciplina, per l'appunto, il diritto al risarcimento dei danni materiali e immateriali subiti a causa di una violazione della normativa in materia di protezione dei dati personali e limita a definire gli elementi principali del regime di responsabilità, senza tuttavia definire la natura della stessa.[131]

In tale prospettiva, il danno non patrimoniale viene ricondotto alla lesione dei diritti della personalità, quali il diritto alla riservatezza, all'identità personale e all'autodeterminazione informativa, e si sostanzia, in particolare, nella perdita di controllo sui propri dati. [132]

---

[130] Cass. civ. Sez. Un. n. 26972 del 2008, in *italgiure.it.*

[131] M. RATTI, in *La responsabilità da illecito trattamento di dati personali nel nuovo Regolamento,* in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali (a cura di G. Finocchiaro),* Zanichelli, Bologna, 2017, pp. 615 e ss.

[132] Art. 82 Reg. (UE) 2016/679 "1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento

La giurisprudenza della Corte di Giustizia europea ha progressivamente definito i confini del pregiudizio immateriale derivante dalla violazione dei dati personali, escludendo una risarcibilità *in re ipsa* dello stesso.

In particolare, nella pronuncia del 4 settembre 2025 (causa C- 655/23)[133], considerata una pietra miliare nella costruzione dogmatica europea in tema di risarcimento del danno non patrimoniale, la CGUE chiarisce che la nozione di danno immateriale include anche i sentimenti negativi provato dalla persona interessata a seguito di un'intrusione non autorizzata dei suoi dati personali;

---

o dal responsabile del trattamento. 2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile. 4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato. 5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2. 6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2."

[133] Testo disponibile in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:62023CJ0655.*

d’altra parte, richiede che la stessa persona interessata provi la presenza di tali sentimenti e le loro conseguenze negative, a causa della violazione del regolamento.

Tuttavia, la Corte precisa che il riconoscimento del danno non patrimoniale non può essere subordinato alla dimostrazione di una soglia minima di gravità del pregiudizio, pur restando esclusa la risarcibilità di pregiudizi meramente futili o bagatellari.

Tale orientamento, è evidente, contribuisce a rafforzare la tutela dei soggetti interessati, ma solleva al contempo interrogativi in ordine alla prova del danno e alla sua concreta quantificazione, soprattutto in contesti caratterizzati da violazioni massive e seriali dei dati personali.

Uno dei profili maggiormente problematici del danno da attacco informatico concerne, infatti, proprio la ricostruzione del nesso causale e la quantificazione del pregiudizio.

La natura immateriale dei beni lesi, la possibile distanza temporale tra l’evento lesivo e la manifestazione del danno, nonché la diffusività degli effetti dell’incidente cyber rendono complessa l’applicazione dei criteri tradizionali di accertamento causale.

In tali ipotesi, il danno tende ad assumere una dimensione sistemica, coinvolgendo una pluralità indeterminata di soggetti e ponendo problemi di imputazione che mettono alla prova gli schemi classici della responsabilità civile.

In tale contesto, particolare rilievo assume il danno reputazionale, frequentemente evocato in relazione agli incidenti di sicurezza informatica.[134]

Gli attacchi cyber, soprattutto quando comportano violazioni dei dati personali o disservizi prolungati, sono idonei a incidere negativamente sull'immagine, sull'affidabilità e sulla credibilità dell'organizzazione colpita, con possibili ricadute nei rapporti con clienti, utenti e partner commerciali.[135]

La sua rilevanza nel contesto cyber è tuttavia segnata da rilevanti difficoltà probatorie, sia con riferimento alla dimostrazione del nesso causale tra l'incidente informatico e il pregiudizio lamentato, sia in ordine alla sua quantificazione.

Alla luce di tali considerazioni, il danno derivante da attacchi informatici non può essere qualificato come una nuova ed autonoma categoria di danno, ma

---

[134] In generale sul danno reputazionale, *ex multis,* Cass. civ. 18174 del 2014: " Il danno recato alla reputazione, da inquadrare nell'ambito della categoria del danno non patrimoniale di cui all'art. 2059 cod. civ., deve essere inteso in termini unitari, senza distinguere tra "reputazione personale" e "reputazione professionale", non concepibili alla stregua di beni diversi e pertanto non suscettibili di distinte domande risarcitorie, trovando la tutela di tale diritto - a prescindere dall'entità e dall'intensità dell'aggressione o dal differente sviluppo del percorso lesivo - il proprio fondamento nell'art. 2 Cost. e, in particolare, nel rilievo che esso attribuisce alla dignità della persona in quanto tale."

[135] Si sottolinea come i danni reputazionali "sono la maggiore preoccupazione per il 65% delle aziende, seguiti dalla violazione di normative (64%), dalle perdite finanziarie direttamente derivanti dalla frode informatica (60%), dall'interruzione dei servizi (59%) a causa di attacchi a sistemi informativi centralizzati (hacking), dal furto o perdita di dati personali degli utenti (58%), dal furto di informazioni e dati riservati (55%).", in *https://www.ictsecuritymagazine.com/articoli/cyber-risks-social-network-e-rischi-reputazionali/*

deve essere ricondotto alle tradizionali figure del danno patrimoniale e non patrimoniale, lette però alla luce delle caratteristiche proprie del rischio tecnologico.

Ciò che caratterizza il danno cyber non è la natura del pregiudizio in sé quanto il contesto in cui esso si manifesta, segnato da complessità tecnica, asimmetria informativa e difficoltà di controllo e prevenzione da parte dei soggetti esposti. Gli attacchi informatici evidenziano, in modo particolarmente acuto, tutti i limiti di un modello di responsabilità civile fondato esclusivamente sull'accertamento della colpa e sulla riparazione *ex post* del pregiudizio.

La frequente difficoltà di individuare una condotta colposa specifica, nonché di ricostruire con precisione il nesso causale, impone di valorizzare criteri di imputazione fondati sull'organizzazione dell'attività e sulla gestione del rischio connesso all'utilizzo di sistemi informatici complessi.

In questo senso, il danno cyber assume un rilievo sistematico, poiché contribuisce a una progressiva trasformazione della funzione della responsabilità civile: essa non può più limitarsi a svolgere una funzione compensativa ma deve iniziare a svolgere un ruolo preventivo e allocativo del rischio tecnologico.

In tale prospettiva, gli obblighi di sicurezza e le misure organizzative assumono una funzione centrale quale parametro di valutazione della diligenza e dell'imputazione della responsabilità, anticipando un modello di tutela

maggiormente orientato alla prevenzione del danno piuttosto che alla sola riparazione delle sue conseguenze, come già osservato nei paragrafi precedenti. In definitiva, il danno informatico evidenzia che la responsabilità civile da sola, pur indispensabile, non basta a governare i rischi della società digitale.

La sua analisi mostra come il diritto debba integrarsi con strumenti anticipatori e organizzativi, capaci di guidare comportamenti prudenti e ridurre gli effetti degli incidenti prima che si verifichino. Il "quadro tradizionale" delle categorie di danno resta valido, ma assume un significato nuovo: serve come parametro per misurare e orientare la prevenzione, non solo per indennizzare.

Questo apre la strada a strumenti privatistici complementari che trasformano il concetto di tutela: da mero risarcimento a gestione proattiva del rischio, combinando funzione economica, incentivo alla sicurezza e governance tecnologica.

2. Intelligenza artificiale: potenzialità e rischi nella protezione dei sistemi informatici

L'attuale realtà è caratterizzata da una rapida diffusione di tecnologie innovative, dall'elaborazione di prodotti digitale sempre più sofisticati e dall'impiego crescente di strumenti di intelligenza artificiale, capaci di elaborare e supportare dati e processi complessi e automatizzati. [136]

[136] U. RUFFOLO, in *Le responsabilità da Intelligenza Artificiale e le questioni di libertà d'espressione e copyright,* in *Contr. Impr.,* 2025, pp. 488 e ss. L'Autore autorevolmente riflette su come "La rivoluzione

L’Intelligenza Artificiale (AI) rappresenta oggi uno degli strumenti più promettenti nella cybersecurity, offrendo capacità avanzate di rilevamento e prevenzione delle minacce. Algoritmi di *machine learning* e sistemi predittivi consentono di individuare comportamenti anomali, rilevare intrusioni e malware in tempo reale, riducendo significativamente i tempi di risposta e aumentando la resilienza dei sistemi.

Dal punto di vista operativo, questo significa poter anticipare gli attacchi, migliorare l’efficienza delle difese e ottimizzare le risorse dedicate alla sicurezza informatica.

Tuttavia, l’adozione dell’AI porta con sé profili problematici significativi.

Gli algoritmi possono essere sensibili a manipolazioni dei dati o attacchi avversari, generare falsi positivi o negativi e introdurre *bias* che influenzano le decisioni automatizzate.

Sul piano etico e legale, rimangono aperte questioni di responsabilità: chi risponde in caso di errore dell’AI o di mancata prevenzione?

---

innescata dalla AI come machina sapiens rappresenta un vero e proprio salto della specie rispetto alla mera digitalizzazione. E non è dunque con essa confondibile ancorché si sia sviluppata evolvendo in quel contesto; che, proseguendo nell’immaginifico parallelismo, era ancora machina Neanderthal. Tale salto della specie, che differenzia l’AI dal contesto digitale nel quale nasce, è rappresentato dall’avere la macchina “imparato ad imparare”: il machine learning (e le sue evoluzioni in deep learning, sistema di reti neurali…) le ha conferito la attitudine a saper imparare, e crescere imparando, rendendola così capace di concepire modelli sempre più perfezionati di sé stessa, fino – si sostiene – al raggiungimento della singolarità.”.

A livello organizzativo, una dipendenza eccessiva dall'AI senza supervisione umana potrebbe indebolire la governance della sicurezza.

Infine, ed è questo il risvolto della medaglia, l'AI non è solo uno strumento difensivo: può essere sfruttata anche dai cybercriminali, aumentando la complessità del rischio strategico e le difficoltà nel combatterlo.

Il rischio che la stessa venga utilizzata come uno strumento offensivo è sempre più palpabile.[137]

In conflitti recenti, l'uso di tecnologie avanzate ha evidenziato come l'AI generativa possa automatizzare attacchi sofisticati, personalizzandoli per singoli individui o organizzazioni e rendendo più difficoltoso il loro rilevamento e contrasto.

In risposta a queste sfide, l'Unione europea ha adottato un approccio integrato che combina strategie tecnologiche, normative e geopolitiche. [138]

---

[137] Nel Rapporto Clusit del 2020 sulla sicurezza ICT in Italia si legge "Le osservazioni degli ultimi mesi descrivono un contesto di attacchi in costante evoluzione con un contemporaneo abbassamento della soglia di difficoltà per realizzare gli attacchi. La disponibilità di molti strumenti e malware sui marketplace nel dark web, a volte anche gratuiti, e l'utilizzo dell'intelligenza artificiale generativa per la costruzione di attacchi sempre più efficaci non può che aprire la strada all'aumento del numero e della complessità degli attacchi. È evidente la necessità di implementare soluzioni in grado di adattarsi rapidamente e automaticamente ad una minaccia estremamente mutevole. Documento disponibile in *https://www.mmn.it/wp-content/uploads/2024/04/Rapporto_Clusit_2024.pdf.*

[138] A partire dall'insediamento della Commissione von der Leyen nel dicembre 2019, l'UE ha posto una crescente enfasi sulla sovranità digitale come risposta alle vulnerabilità percepite nei confronti di attacchi esterni, che provengono non solo da Stati ma anche da attori privati il cui comportamento potrebbe non

La Comunicazione congiunta del 16 dicembre 2020 al Parlamento e al Consiglio europeo ha delineato la strategia europea per la cybersicurezza nel decennio digitale, sottolineando la necessità di rafforzare la sovranità digitale dell'UE e ridurre la dipendenza dalle potenze straniere nell'approvvigionamento di prodotti high-tech. La governance tecnologica è diventata così un pilastro dell'azione esterna dell'UE, con l'obiettivo di proteggere le infrastrutture critiche, prevenire minacce ibride e garantire la resilienza digitale a livello continentale.

In questo quadro, il Regolamento (UE) 2024/1689 (*Ai Act),* che stabilisce regole armonizzate in materia, rappresenta uno strumento chiave per disciplinare l'uso dell'intelligenza artificiale all'interno dell'UE, garantendo sia la protezione dei cittadini da rischi informatici, sia l'adozione di standard internazionali che riflettano i valori europei.

---

allinearsi ai valori fondamentali dell'Unione. Sintomatici sono tutti gli interventi in materia quali la Comunicazione congiunta al Parlamento europeo e al Consiglio, del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020); il Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, *relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE*; il Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, *relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828*.

L'AI Act si inserisce in un ecosistema normativo più ampio, strettamente connesso al Regolamento (UE) 2022/2065 sulle piattaforme digitali (DSA) e al Regolamento (UE) 2022/1925 sui mercati digitali (DMA), volti tutti a garantire trasparenza, prevenzione delle pratiche anticoncorrenziali e tutela della libertà di scelta degli utenti.

L'interazione tra questi strumenti normativi evidenzia la volontà dell'UE di adottare un approccio coeso e integrato alla regolazione del digitale nel quale innovazione, sicurezza e protezione dei diritti fondamentali si intrecciano in una strategia complessiva di governance tecnologica e resilienza strategica.

Inoltre, la strategia europea affronta la dualità intrinseca dell'AI: se da un lato essa potenzia la sicurezza cibernetica e la gestione proattiva delle minacce, dall'altro può essere sfruttata come arma nei conflitti informatici e nelle campagne di disinformazione. Le istituzioni europee sottolineano quindi l'importanza di combinare strumenti tecnologici avanzati con supervisione umana e regolamentazione etica, promuovendo un approccio *human-in-the-loop* che minimizzi i rischi derivanti da automatismi incontrollati.

Nonostante le complessità e le minacce emergenti, le prospettive sono positive: l'integrazione efficace tra AI, governance normativa e supervisione umana può trasformare la cybersecurity europea in un sistema proattivo, resiliente e adattivo.

In questo contesto, l'AI non solo potenzia la rilevazione e la prevenzione degli attacchi, ma contribuisce alla definizione di modelli di responsabilità digitale e

standard internazionali, rafforzando la leadership globale dell'UE nella regolamentazione tecnologica e nella difesa della sovranità digitale.

La sfida principale rimane governare l'adozione di questo strumento in modo consapevole, massimizzando benefici e mitigando rischi, per costruire sistemi di sicurezza affidabili, sostenibili e coerenti con i valori fondamentali dell'Unione

3. Verso una riconfigurazione della responsabilità civile nel cyberspazio

Nel corso dell'indagine svolta è stata analizzata in modo sistematico la complessa interazione tra cybersicurezza, responsabilità civile e gestione del rischio digitale, approfondendo tanto i profili normativi applicabili ai prodotti e ai servizi digitali quanto i modelli giuridici astrattamente idonei a regolare gli eventi lesivi connessi all'impiego delle nuove tecnologie.

L'attenzione si è concentrata, in particolare, sui punti di forza e sulle criticità dei diversi criteri di imputazione, messi alla prova da architetture tecnologiche sempre più complesse e da sistemi caratterizzati da autonomia decisionale.

Dall'analisi emerge come la normativa europea e nazionale, pur imponendo obblighi sempre più stringenti in materia di sicurezza, conformità tecnica e gestione del rischio, non abbia introdotto autonomi regimi di responsabilità civile.

Il legislatore ha preferito intervenire sul piano regolatorio e preventivo, lasciando spazio all'applicazione dei principi civilistici tradizionali, chiamati

tuttavia a confrontarsi con realtà tecnologiche profondamente mutate, incluse le catene di fornitura digitali e i sistemi di intelligenza artificiale.

La trasformazione tecnologica ha inciso non solo sui processi produttivi, comunicativi e cognitivi, ma anche sulle fondamenta teoriche del diritto civile, mettendo in discussione l'adeguatezza delle categorie classiche della responsabilità. In particolare, il mutamento ontologico e funzionale dei sistemi tecnologici rende sempre più problematica l'applicazione di modelli fondati sulla colpa, sull'imputazione soggettiva e su una concezione lineare del nesso causale. [139]

Tale difficoltà si accentua con l'emergere di sistemi di intelligenza artificiale dotati di capacità di autodeterminazione, in grado di operare attraverso processi decisionali opachi e difficilmente ricostruibili anche per i loro stessi sviluppatori. Le categorie tradizionali della responsabilità presuppongono, infatti, un soggetto dotato di *voluntas* e di consapevole agency, presupposto che risulta fortemente indebolito in presenza di algoritmi autonomi inseriti in ecosistemi socio-tecnici complessi.

---

[139] A. BERTOLINI, in *Intelligenza Artificiale e responsabilità civile. Problema, sistema, funzioni*, Bologna, 2025. L' Autore riflette proprio sulla adeguatezza dei modelli normativi autonomi di responsabilità civile del nostro ordinamento dinanzi alla complessità dei sistemi di intelligenza artificiale

In questo contesto, il rischio è duplice: da un lato, l'attribuzione della responsabilità può risultare arbitraria o eccessivamente semplificata; dall'altro, il soggetto danneggiato può rimanere privo di una tutela effettiva.

La frammentazione della vicenda lesiva in una pluralità di possibili matrici causali, corrispondenti ai diversi soggetti che intervengono nella progettazione, implementazione, utilizzo e aggiornamento del sistema, ostacola l'individuazione di una soluzione organica, inducendo al contempo a sottovalutare la complessità dei processi decisionali sottesi all'output tecnologico.

Queste criticità impongono un ripensamento delle categorie fondanti della responsabilità civile e, più in generale, della sua funzione. Tradizionalmente concepita come strumento sanzionatorio e compensativo operante *ex post*, la responsabilità è oggi chiamata a svolgere anche una funzione regolativa *ex ante*.

In questa prospettiva, si delinea un possibile passaggio dal modello del soggetto responsabile al modello del sistema responsabile, nel quale i doveri non gravano più esclusivamente sui soggetti, ma vengono distribuiti tra architetture tecniche, procedure decisionali, modelli computazionali e assetti organizzativi. La responsabilità tende così a configurarsi come una proprietà emergente di ecosistemi complessi, operando non solo come reazione al danno ma anche quale strumento di progettazione e governance del rischio.

Tale impostazione appare coerente con l'evoluzione del diritto europeo che, attraverso l'AI Act, il Cyber Resilience Act e la riforma della Product Liability Directive, ha spostato l'asse verso obblighi di sicurezza, conformità e gestione del rischio, senza introdurre autonomi meccanismi risarcitori.

La "responsabilità" che emerge da queste discipline assume prevalentemente una connotazione amministrativa e regolatoria, traducendosi in obblighi organizzativi e tecnici, sanzioni e misure correttive, mentre la riparazione del danno resta affidata a strumenti diversi dalla responsabilità civile tradizionale.

In questo scenario ibrido, la responsabilità civile è chiamata a rinnovarsi, non come mera applicazione di schemi normativi predeterminati, ma come infrastruttura capace di cogliere la dimensione relazionale e ambientale dei sistemi tecnologici.

Ciò implica l'incorporazione della tracciabilità sin dalla fase di progettazione, la distribuzione della responsabilità lungo l'intera catena del valore digitale, l'attenuazione del paradigma della causalità deterministica in favore di modelli probabilistici e un ripensamento dell'onere della prova, calibrato sulle asimmetrie informative.[140]

In tale prospettiva si collocano i principali modelli elaborati dalla dottrina nel dibattito contemporaneo: la teoria dell'allocazione efficiente del rischio, che

---

[140] L. FLORIDI, in *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide,* Milano, 2022, il quale evidenzia la cd natura ambientale dell'IA.

assegna il costo dei danni a chi meglio può prevenirli[141]; la accountability computazionale[142], che reinterpreta la responsabilità *ex ante* come obbligo di progettazione, tracciabilità e contestabilità; la teoria delle presunzioni riequilibratrici[143], che sposta l'onere probatorio per riequilibrare asimmetrie informative.

Nell'ambito del dibattito sulla responsabilità come presidio da utilizzare in maniera preventiva, si innesta anche la possibilità di rivedere, in chiave tecnologica e con ampia visione su quelli che sono i nuovi sistemi digitali, il paradigma della cd responsabilità vicaria, disciplinata dall art. 2049 c.c., che trasferisce l'onere della responsabilità sul soggetto dominante, produttore o prestatore di servizi, indipendentemente dall'azione diretta di altri agenti o sistemi.[144]

---

[141] G. CALABRESI, in *The Costs of Accidents: A Legal and Econimic Analysis*, New Haven, 1970.

[142] M. HILDEBRANDT, in *Law for computer scientists and other folk*, Oxford, 2020.

[143] A. VASUDEVAN, in *Addressing the liability gap in artificial intelligence*, CIGI Policy Brief n. 177, Waterloo, 2023.

[144] Sul tema, nella dottrina italiana, si veda: U. RUFFOLO, in *La responsabilità vicaria*, Milano, 1976; D. CARUSI, in *L'attuazione e tutela dei diritti, III. La responsabilità e il danno*, Capitolo inserito nel *Trattato di diritto civile diretto da Lipari, Rescigno e coordinato da Zoppini*, vol. IV Milano, 2009, 484 ss.; A.M. GALOPPINI, in *La responsabilità dei padroni e dei committenti*, in Cendon (a cura di), *La responsabilità civile*, XI, Torino, 1998, 107 ss.; C. DE MENECH, in *La responsabilità vicaria nel diritto vivente*, in *Nuova giur. civ. comm*., 2017, pp. 1604 e ss.

Si tratta dell'unica vera e propria responsabilità oggettiva che il nostro ordinamento conosce in cui viene ritenuto responsabile non chi ha agito ma chi, per posizione, controllo e beneficio, deve rispondere degli effetti provocati dall'altrui azione. [145]

Per interpretazione giurisprudenziale consolidata, la responsabilità vicaria poggia sul "solo fatto della altrui utilizzazione strumentale": non è necessario qualificare giuridicamente il rapporto tra autore materiale e soggetto responsabile, essendo sufficiente dimostrare che per volontà di un soggetto un altro esplichi un'attività per conto del primo.

Il requisito "nell'esercizio delle incombenze" è soddisfatto ogniqualvolta sia possibile registrare un rapporto di "occasionalità necessaria" tra il fatto illecito e l'esercizio delle mansioni, mentre si esclude laddove il preposto agisca per finalità private.[146]

Il problema si acuisce nella misura in cui oggi le azioni delegate non sono più quasi mai affidate a esseri umani, ma a sistemi autonomi di IA, utilizzati prevalentemente in contesti professionali o imprenditoriali, data la complessità e i costi elevati di tali sistemi. In entrambi i casi, le "incombenze" vengono

---

[145] Così, G. MONATERI, in *La responsabilità civile*, Torino, 1998; G. ALPA, in *La responsabilità civile*, in *Trattato di diritto civile*, vol. IV, Milano, 1999; M. FRANZONI, in *L'illecito*, Milano, 2004; U. RUFFOLO, in *La responsabilità vicaria*, cit., pp. 73 e ss.

[146] *Ex multis*, Cass. civ. n. 28852/2021.

svolte nell'interesse di un altro soggetto, implicando una capacità decisionale autonoma in contesti di incertezza.

Sul piano strutturale, l'art. 2049 c.c. appare dunque per alcuni un modello adeguato a individuare il fatto generatore del danno direttamente nella decisione del sistema di IA, recidendo segmenti causali complessi e assorbendo criticità che ostacolano l'applicazione dei modelli di responsabilità tradizionali.

Tuttavia, anche in questo caso, la responsabilità si concentra su un singolo soggetto, creando una presunzione di custodia che non risolve pienamente il problema teorico, considerato che spesso non esiste una logica binaria tra utilizzatore e soggetto dominante.

La responsabilità deve essere concepita come presidio collettivo, organizzativo e progettuale, capace di distribuire il rischio in un ecosistema digitale, garantendo governance preventiva e progettazione responsabile.

Il nodo interpretativo centrale resta quello tra l'introduzione di regimi speciali di responsabilità per le tecnologie digitali e l'adattamento evolutivo delle categorie civilistiche esistenti.

In particolare, occorre comprendere se gli interrogativi posti in tema di responsabilità dalle nuove tecnologie siano effettivamente nuovi o, seppur non

facilmente, risolvibili in via interpretativa per mezzo degli strumenti normativi esistenti "senza dover necessariamente reinventare la ruota". [147]

Parte della dottrina propende per una "giuridificazione" *ad hoc* dei fenomeni digitali, ritenendo inadeguati gli strumenti tradizionali a fronte di sistemi autonomi e opachi.

Tuttavia, una simile impostazione rischia di produrre una frammentazione normativa e di indebolire la coerenza sistemica del diritto civile, moltiplicando regimi speciali difficilmente coordinabili e spesso incapaci di offrire una tutela effettiva ai soggetti danneggiati.[148]

In ordinamenti di civil law, la forza delle categorie tradizionali risiede proprio nella loro elasticità. Modelli come la responsabilità da rischio, le presunzioni di imputazione e le forme di responsabilità oggettiva consentono un adattamento evolutivo capace di governare anche fenomeni tecnologicamente inediti, senza sacrificare i principi di fondo dell'ordinamento.

Un'eccessiva rigidità normativa o l'introduzione di schemi iper-specializzati rischierebbero, al contrario, di cristallizzare soluzioni destinate a diventare rapidamente obsolete e di ostacolare l'innovazione tecnologica.[149]

---

[147] *no need to rinvent the wheel*" come afferma LEVY, in *No need to reinvent the wheel: shy existing liability law does not neet to be preemptively altered to cope with the debut of the driverless car*, pp. 355 e ss

[148] L. DI DONNA, in *Intelligenza artificiale e rimedi risarcitori*, CEDAM, 2022.

[149] U. RUFFOLO, in *Responsabilità da A.I. e da algoritmo*, in ID. (a cura di) *Intelligenza artificiale. Il diritto, i diritti e l'etica,* Milano, 2020, p. 94 , il quale ha evidenziato che "equivoco semplicistico quanto diffuso è

In questo grado di sviluppo tecnologico e normativo, una progressiva oggettivizzazione della responsabilità civile appare la soluzione più coerente per fronteggiare i rischi sistemici connessi ai prodotti e ai servizi digitali, nonché ai sistemi di intelligenza artificiale. Tale approccio consente di superare le evidenti difficoltà di accertamento della colpa e del nesso causale in contesti caratterizzati da elevata complessità tecnica, opacità decisionale e asimmetrie informative strutturali, rafforzando la tutela dei soggetti danneggiati e rendendo il rischio giuridicamente governabile.

L'oggettivizzazione della responsabilità, tuttavia, non può essere intesa come soluzione autosufficiente né come risposta indifferenziata a tutte le criticità poste dalle nuove tecnologie.

Essa deve operare in coordinamento con la normativa di settore, la quale è chiamata ancora a svolgere una funzione distinta e complementare: non tanto

---

credere che il fenomeno nuovo debba trovare eminente disciplina in nuove norme; e così sottovalutare- soprattutto negli ordinamenti continentali di *civil law* – sia la elevata capacità di risposta della evoluzione interpretativa, sia i pericoli di inquinamento sistemico connessi ad una "iperfetazione legislativa" che risponda sempre con nuove e settoriali norme ai mutamenti del reale. Merita, dunque, rinnovata considerazione l'idoneità dello strumento interpretativo a dare risposta ai nuovi fenomeni, soprattutto negli ordinamenti ad elevata codificazione. Non va dimenticata, infatti, la pretesa di completezza dell'ordinamento come caratteristica connaturata a tali sistemi, che si considerano strutturalmente idonei a regolare anche il futuro meno prossimo, con diversi possibili livelli di ricorso all'interpretazione (…) Il che, per converso, rende tali sistemi alterabili ed inquinabili dai potenziali effetti sistemici, anche non previsti, di ogni non indispensabile nuova norma".

quella di riparare il danno, quanto quella di definire standard comuni di sicurezza, obblighi di progettazione, procedure di aggiornamento, tracciabilità e gestione del rischio.

In tal senso, strumenti come l'AI Act, il Cyber Resilience Act e la disciplina europea sulla sicurezza dei prodotti digitali incidono prevalentemente sul piano della prevenzione e della conformità *ex ante,* senza sostituirsi ai meccanismi civilistici di imputazione del danno.[150]

Così, la responsabilità civile conserva un ruolo centrale ma circoscritto: essa non è chiamata a regolare in modo diretto il funzionamento tecnico dei sistemi, né a supplire alle carenze della regolazione amministrativa, bensì a operare come presidio residuale ed essenziale di allocazione del rischio, intervenendo quando il danno si è già verificato e quando gli obblighi di sicurezza, pur formalmente rispettati, si rivelano insufficienti a prevenire l'evento lesivo. Tale distinzione evita il rischio di una sovrapposizione impropria tra piani normativi e consente di preservare la funzione tipica della responsabilità civile, adattandola alle esigenze di un ecosistema digitale complesso.

In questo quadro, l'inevitabile incremento dei costi organizzativi, contrattuali e assicurativi gravanti sulle imprese rappresenta non un effetto distorsivo, ma

[150] "sistema del doppio binario" di cui parla A. AMIDEI, in R*obotica intelligente e responsabilità: profili e prospettive evolutiva del quadro normativo europeo*, in U. RUFFOLO, in *Intelligenza artificiale e Responsabilità*, cit, pp. 63 e ss.

il riflesso fisiologico di una redistribuzione del rischio coerente con il principio di chi trae beneficio dall'attività tecnologica.

La responsabilità civile, così reinterpretata, non abdica ai propri principi fondamentali, ma li declina in una dimensione adattiva e sistemica, contribuendo a un equilibrio sostenibile tra innovazione tecnologica, tutela dei diritti e sicurezza del cyberspazio.

Capitolo III

La copertura del rischio *cyber* nel diritto civile

Sommario: 1. La rilevanza dello strumento assicurativo nel governo del rischio digitale 1.1. Assicurazione e rischio *cyber*: le nuove prospettive; 1.2. Il rischio come elemento strutturale del contratto di assicurazione; 1.3. Le polizze *cyber;* 1.4. Insurtech

1. La rilevanza dello strumento assicurativo nel governo del rischio digitale

Nel contesto della società del rischio digitale la tradizionale architettura del diritto civile, fondata sul nesso illecito–responsabilità–risarcimento, è sottoposta a una tensione crescente.

La progressiva pervasività delle tecnologie informatiche e la centralità dei sistemi digitali nello svolgimento delle attività economiche e sociali hanno determinato l'emersione di nuove tipologie di rischio, caratterizzate da elevata complessità tecnica, rapidità di propagazione e potenziale diffusività degli effetti dannosi.

Come già messo in luce nel capitolo precedente, la responsabilità civile conserva un ruolo essenziale nella definizione degli standard di diligenza e nell'imputazione delle conseguenze dell'illecito.

Tuttavia, nel cyberspazio, essa mostra limiti strutturali che ne riducono l'efficacia quale strumento esclusivo di tutela.

Il rischio cyber, infatti, si colloca in una dimensione nella quale la prevenzione assume un valore primario e la reazione *ex post* risulta spesso tardiva o insufficiente.

Da un lato, la natura immateriale dei beni giuridici coinvolti e la frequente irreversibilità degli effetti lesivi rendono problematica la piena reintegrazione del pregiudizio subito. La perdita o la compromissione di dati, l'interruzione dei servizi digitali e il danno reputazionale connesso a un incidente informatico producono conseguenze che difficilmente possono essere compensate attraverso lo strumento risarcitorio.

Dall'altro lato, la ricostruzione del nesso causale e l'individuazione del soggetto responsabile risultano particolarmente complesse, in ragione della molteplicità degli attori coinvolti nella catena digitale e della frequente dimensione transnazionale degli eventi dannosi.

A ciò si aggiunge che il danno cyber presenta spesso una dimensione cumulativa, idonea a incidere simultaneamente su una pluralità di soggetti e a generare effetti a catena difficilmente circoscrivibili.

È evidente allora che la funzione compensativa della responsabilità civile rischia di entrare in crisi, sia per l'entità complessiva del danno sia per la difficoltà di garantire un'effettiva soddisfazione delle pretese risarcitorie.

In questo scenario, emerge con particolare evidenza l'esigenza di affiancare alla tutela risarcitoria strumenti capaci di operare in una logica *ex ante*, orientata alla gestione, alla riduzione o alla copertura del rischio.

È in tale prospettiva che lo strumento assicurativo assume una rilevanza crescente nel governo del rischio digitale.

L'assicurazione consente, infatti, non solo di distribuire collettivamente le conseguenze economiche degli eventi dannosi, ma anche di introdurre meccanismi di selezione e valutazione del rischio che incidono sulle modalità di organizzazione e gestione della sicurezza informatica.

Sebbene l'assicurazione non possa essere considerata un sostitutivo della responsabilità civile, essa si configura come uno strumento complementare idoneo a colmare le lacune evidenziate e a contribuire alla costruzione di un modello di gestione del rischio cyber più efficiente e sostenibile.

In tal senso, la rilevanza dell'assicurazione nel contesto digitale non si esaurisce nella funzione indennitaria, ma si inserisce in un più ampio processo di razionalizzazione del rischio, che trova il suo sviluppo nei paragrafi successivi.

1.1. Assicurazione e rischio *cyber*: le nuove prospettive

L'assicurazione può essere definita, in termini generali, come il contratto mediante il quale un soggetto (assicuratore) si obbliga a fornire una prestazione

ad un altro soggetto (assicurato), al verificarsi di un evento futuro ed incerto, a fronte del pagamento di un premio.[151]

Considerando la sua struttura fondamentale, l'assicurazione si distingue in due principali categorie: assicurazioni sulla vita e assicurazioni contro i danni.

Nel caso delle assicurazioni sulla vita, l'assicuratore, dietro il pagamento del premio, si obbliga a corrispondere un capitale o una rendita al verificarsi di un evento relativo alla vita dell'assicurato. Tale evento può riguardare la morte dell'assicurato, nel qual caso la prestazione è dovuta solo se l'evento si verifica nel periodo previsto dal contratto, oppure la sopravvivenza, quando la prestazione è dovuta esclusivamente se l'assicurato è ancora in vita al termine del periodo contrattuale.

Le assicurazioni contro i danni, invece, hanno lo scopo di proteggere il patrimonio dell'assicurato da eventi futuri e incerti che possano determinare perdite economiche di diverse tipologie.

Questa distinzione, seppur sommaria, risulta utile per comprendere le funzioni che lo strumento assicurativo ha nel tempo svolto nella società.

Storicamente, le assicurazioni contro i danni furono le prime a svilupparsi e con esse si consolidò una solida elaborazione teorica incentrata sulla funzione

[151] Art. 1882 c.c., in particolare, prevede che "L'assicurazione è il contratto col quale l'assicuratore, verso il pagamento di un premio, si obbliga a rivalere l'assicurato, entro i limiti convenuti, del danno ad esso prodotto da un sinistro, ovvero a pagare un capitale o una rendita al verificarsi di un evento attinente alla vita umana"

indennitaria del contratto. In tali casi, l'obbligo dell'assicuratore di corrispondere l'indennità sorge solo al verificarsi del sinistro previsto dal contratto e nella misura del danno effettivamente subito dall'assicurato.

L'avvento delle assicurazioni sulla vita, estranee al concetto tradizionale di danno, ha invece messo in discussione la funzione classica del contratto assicurativo. Alcuni autori hanno tentato di individuare una "conseguenza dannosa" negli eventi morte o sopravvivenza, mentre altri hanno elaborato la teoria del "bisogno eventuale" secondo la quale il bisogno economico futuro non deve necessariamente realizzarsi, ma è sufficiente sia prevedibile al momento della stipula del contratto, esaltando così la funzione previdenziale dell'assicurazione. Nell'assicurazione vita, infatti, la motivazione che spinge un soggetto alla stipula del contratto si identifica con la preoccupazione di costituirsi una risorsa finanziaria da utilizzare nel futuro se e nella misura ne necessiterà.

Tuttavia, autorevole dottrina ritiene che ogni tentativo di ricostruzione unitaria sia insoddisfacente, a causa della sostanziale differenza dei rischi tra le due tipologie di assicurazioni.

Pur rimanendo centrale il concetto di rischio, esso si manifesta con caratteristiche differenti a seconda che si tratti di assicurazioni sulla vita o contro i danni.[152]

Questa pluralità di configurazioni del rischio non si esaurisce nella dimensione contrattuale, ma riflette una più ampia trasformazione del modo in cui il rischio viene percepito e gestito nella società contemporanea.

In questo senso, il dibattito giuridico sull'assicurazione si inserisce nel più ampio contesto della cd società del rischio, concetto sociologico che descrive un assetto sociale moderno sempre più esposto a rischi incerti, diffusi e spesso di origine tecnologica.

Nella società contemporanea, la progressiva digitalizzazione delle attività economiche e sociali ha determinato una crescente dipendenza da infrastrutture informatiche e sistemi informativi complessi, con la conseguente emersione di nuove tipologie di rischio.

Come già analizzato, si tratta di rischi che non esauriscono in eventi isolati o occasionali, ma che possono assumere una dimensione sistemica e interconnessa, incidendo simultaneamente su una pluralità di interessi giuridicamente rilevanti. Un attacco informatico, ad esempio, può generare

---

[152] L. FARENGA, in *Manuale di diritto delle assicurazioni private,* VII, Giappichelli, 2025, p. 147 e ss. In particolare, l'Autore riconduce la duplicità delle prestazioni dell'assicuratore e dei tipi contrattuali, rispettivamente, al principio indennitario e al principio previdenziale.

danni economici diretti, responsabilità verso terzi e pregiudizi di natura reputazionale, rendendo complessa la ricostruzione del danno e la sua allocazione.

In tale contesto, nella prassi delle polizze cyber, gli assicuratori non si limitano alla sola copertura indennitaria, ma verificano (o quantomeno dovrebbero verificare) *ex ante* che l'organizzazione assicurata sia adeguatamente preparata a fronteggiare eventuali incidenti informatici.

La valutazione pre-polizza può inoltre incentivare comportamenti virtuosi da parte del soggetto assicurato, contribuendo a migliorare la gestione del rischio digitale e a ridurre la probabilità o l'impatto di un sinistro.

Attraverso la previsione di obblighi di condotta, controlli organizzativi e tecnici, meccanismi premiali o sanzionatori, il contratto assicurativo può orientare le pratiche dell'assicurato verso standard idonei a mitigare i rischi cyber, rafforzando sia la prevenzione sia la resilienza complessiva dell'organizzazione.[153]

---

[153] ENISA, *Cyber Insurance: Recent Advances, Good Practices and Challenges*, in https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges, p. 16. In proposito, si legge "An Incident Response program defines the processes and resources that an organisation engages for addressing any Information Security incidents. Insurers validate the existence of a potential clients' Incident Response program in a formal form, and evaluate their tolerance level towards withstanding several incidents. Incident notification is a key component of NIS Directive that requires the establishment of an Incident Response function within an organisation. Similar to other functions, testing the capabilities of a defence mechanism is critical to the success of it; hence, confirmation of the presence of

Ciò testimonia come l'assicurazione sia chiamata a confrontarsi con rischi che presentano caratteristiche diverse rispetto a quelli tradizionalmente considerati, pur rimanendo ancorata alla struttura contrattuale tipica del modello assicurativo.

La funzione dell'assicurazione resta infatti essenzialmente indennitaria in quanto il rapporto contrattuale continua a fondarsi sulla corresponsione di una prestazione economica al verificarsi di un sinistro assicurato.

Tuttavia, con riferimento ai rischi digitali emergenti, l'assicurazione sembra destinata ad assumere anche una valenza gestionale e preventiva.

In tal senso, l'assicurazione non si limita a trasferire le conseguenze economiche dell'evento dannoso ma può incidere indirettamente sulla gestione del rischio, imponendo o incentivando l'adozione di comportamenti virtuosi da parte del soggetto o dell'impresa assicurata.

Tali profili non si pongono in alternativa alla funzione indennitaria, ma ne rappresentano una possibile declinazione nel più ampio quadro della governance del rischio in cui l'assicurazione concorre, insieme ad altri strumenti giuridici e organizzativi, alla regolazione dell'incertezza propria dei contesti economici e tecnologici contemporanei.

---

regular exercises in support of an existing Incident Response program is recommended. A valuable finding is that the presence of an incident response team has the top positive impact on the per capita cost of a data breach",

Alla luce di queste considerazioni, il presente capitolo si propone di approfondire gli aspetti strutturali del contratto di assicurazione, analizzandone gli elementi costitutivi fondamentali e la posizione giuridica del concetto di rischio. Particolare attenzione sarà dedicata al rischio cyber, al fine di esaminarne la qualificazione giuridica, i profili di assicurabilità e le modalità attraverso cui le soluzioni assicurative possono rispondere alle esigenze concrete dei soggetti assicurati.

1.2. Il rischio come elemento strutturale del contratto di assicurazione

Il contratto di assicurazione è uno strumento fondamentale del diritto civile con cui un soggetto si obbliga a fornire una prestazione economica a fronte del pagamento di un premio da parte dell'assicurato, al verificarsi di un evento futuro e incerto.

Si tratta di un contratto bilaterale e a prestazioni corrispettive: l'assicurato corrisponde un premio certo, mentre l'obbligazione dell'assicuratore è condizionata al verificarsi dell'evento assicurato.

Quanto alla bilateralità, è sufficiente osservare che essa permane anche nel caso in cui il contraente sia persona diversa dall'assicurato.

Maggiore attenzione richiede il requisito della corrispettività.

L'obbligazione principale dell'assicurato, consistente nel pagamento del premio, è certa e anticipata, mentre quella dell'assicuratore è subordinata al verificarsi del sinistro o di un evento attinente alla vita umana. Ne consegue

che, qualora l'evento non si verifichi, l'assicurato non riceve alcuna prestazione economica, con il rischio che il contratto possa apparire, ad una prima lettura, come un negozio con prestazione a carico di una sola delle parti.

In realtà, la dottrina ha chiarito come la prestazione dell'assicuratore non si esaurisca nel pagamento dell'indennità, della rendita o del capitale.[154]

La prestazione principale si sostanzia piuttosto nella predisposizione delle condizioni tecniche, organizzative e giuridiche idonee a garantire l'adempimento dell'obbligazione finale, ove dovuta.

L'inserimento del contratto nella massa dei rischi assicurati comporta, infatti, l'accantonamento del premio a riserva, il mantenimento di adeguati margini di solvibilità e l'organizzazione di strutture idonee a neutralizzare i rischi, realizzando così l'interesse dell'assicurato.

Il pagamento dell'indennità, della rendita o del capitale rappresenta pertanto una prestazione accessoria, sospensivamente condizionata al verificarsi dell'evento assicurato, che si aggiunge a quella principale. In questa prospettiva deve essere letto il requisito della corrispettività del contratto di assicurazione.

Il contratto di assicurazione è altresì un contratto consensuale, perfezionandosi con il mero scambio dei consensi tra le parti.

Resta infine da interrogarsi sulla qualificazione del contratto di assicurazione come contratto aleatorio.

---

[154] L. FARENGA, op.cit., p. 172.

Secondo l'impostazione maggioritaria, l'assicurazione sarebbe infatti contraddistinta da un elemento di incertezza (alea), in quanto al momento della stipulazione non è possibile prevedere quale delle parti sopporterà il sacrificio economico maggiore e quale, invece, trarrà il beneficio dalla prestazione, con la conseguenza di un potenziale squilibrio tra le prestazioni contrattuali.

Una parte significativa della dottrina ha tuttavia messo in discussione tale ricostruzione, ritenendola non pienamente soddisfacente ove venga estesa l'analisi all'intera operazione assicurativa e non si arresta alla singola relazione sinallagmatica. [155]

In questa prospettiva, non sarebbe tecnicamente corretto parlare di una vera e propria "alea contrattuale".

Dal punto di vista dell'assicuratore, infatti, il verificarsi dei sinistri e l'obbligo di corrispondere le indennità non costituiscono eventi imprevedibili, ma fenomeni statisticamente previsti e calcolati mediante strumenti attuariali. Ciò che rimane incerto non è l'esistenza del sinistro in sé, ma quale tra i molteplici rischi assicurati si concretizzerà.

Analogamente, anche con riferimento all'assicurato, l'eventuale pagamento dell'indennità non rappresenta un vantaggio, bensì il ristoro di un danno subito; il mancato verificarsi del sinistro non integra una perdita, nonostante il pagamento del premio, poiché l'interesse perseguito dall'assicurato non è la

[155] Ibidem, pp. 14-15

realizzazione dell'evento dannoso, ma la sicurezza e la tranquillità derivanti dalla copertura del rischio.

In questa prospettiva, la tradizionale rappresentazione dell'assicurazione come strumento di trasferimento del rischio appare riduttiva e deve essere corretta alla luce della funzione di neutralizzazione del rischio che il contratto è chiamato a svolgere. [156]

Proprio la centralità del rischio, inteso come elemento strutturale del rapporto assicurativo e criterio di delimitazione dell'oggetto contrattuale, impone di soffermarsi sulle sue caratteristiche giuridicamente rilevanti e sulle modalità attraverso cui esso viene convenzionalmente perimetrato dalle parti.[157]

Il rischio, ossia la possibilità che si verifichi un evento futuro e incerto, è misurabile secondo criteri che incidono sia sulla assicurabilità sia sulla determinazione del premio. In generale, quanto più elevata è la probabilità o l'entità del rischio, tanto maggiore sarà il premio richiesto; al contrario, i rischi eccessivi o imprevedibili possono condurre alla cd inassicurabilità del rischio.[158]

---

[156] Sulla neutralizzazione del rischio, v. N. DE LUCA, in *Diritto ed economia delle assicurazioni*, Bologna, Il Mulino, 2022; M. ROSSETTI, in *Il diritto delle assicurazioni*, I, Padova, Cedam, 2011.

[157] Il rischio è l'elemento centrale del contratto di assicurazione, tanto che la sua mancanza produce la nullità del contratto ex art. 1895 c.c.

[158] Art. 1898, co 1, c.c. (Aggravamento del rischio) "Il contraente ha l'obbligo di dare immediato avviso all'assicuratore dei mutamenti che aggravano il rischio in modo tale che, se il nuovo stato di cose fosse esistito

Gli elementi che concorrono a definirne l'entità del rischio possono di natura generale, come il tipo di rischio e le condizioni economiche generali, o di natura particolare quali le caratteristiche del bene assicurato, le modalità di conservazione del bene o le circostanze specifiche in cui il rischio può manifestarsi.

La corretta individuazione di questi elementi consente di delimitare con precisione l'oggetto del contratto e di orientare la valutazione dell'esposizione dell'assicurato, al fine di regolare in modo proporzionato l'impegno dell'assicuratore.

In questo modo, il rischio non è ridotto a concetto astratto ma diviene criterio di organizzazione del contratto, fondamentale per la determinazione delle prestazioni e guida per le misure preventive che l'assicuratore può richiedere o incentivare, ad ulteriore conferma della duplice funzione che il contratto può assumere: indennitaria ma anche preventiva e gestionale.

Gli elementi costituitivi del rischio comprendono inevitabilmente il danno e il nesso causale: l'evento deve essere previsto nel contratto e deve essere idoneo a produrre il sinistro, ossia ciò che concretamente attiva gli obblighi dell'assicuratore. [159]

---

e fosse stato conosciuto dall'assicuratore al momento della conclusione del contratto, l'assicuratore non avrebbe consentito l'assicurazione o l'avrebbe consentita per un premio più elevato."

[159] L. FARENGA, op. cit., p. 156.

La centralità di tali elementi diventa particolarmente evidente quando più eventi concorrono alla produzione del danno, rendendo necessario individuare quale di essi sia determinante ai fini della copertura assicurativa.

Proprio tale complessità, unita alla necessità di gestire l'incertezza temporale, ha portato il mercato assicurativo a sviluppare clausole contrattuali specifiche volte a delimitare lo spazio temporale dell'efficacia del contratto.

In particolare, si tratta delle clausole *claims made* e le clausole *loss occurence.*[160]

Le *claims made* prevedono che l'assicuratore sia obbligato all'indennizzo solo per i danni il cui risarcimento venga richiesto da terzi danneggiati durante il periodo di vigenza della polizza nei confronti dell'assicurato.

In alcuni casi, dette clausole sono "pure" e la copertura opera per tutte le richieste inoltrate dal danneggiato nel periodo di copertura della polizza, a prescindere dalla data del fatto illecito. In altri casi, invece, sono "impure" operando solo quando tanto il fatto illecito che la richiesta risarcitoria intervengano nel periodo di efficacia polizza.

[160] IVASS, in *Le clausole loss occurrence e claims made*, 2019.

La giurisprudenza ha a lungo discusso sulla natura di quest'ultime, ritenendo che per effetto delle stesse il contratto di assicurazione perdesse la sua tipicità.[161]

Le clausole *loss occurence,* meno utilizzate, limitano invece l'operatività della garanzia ai soli eventi dannosi verificatisi durante il periodo di vigenza della polizza, a prescindere dalla data di richiesta del risarcimento.

Tali strumenti permettono di definire con precisione l'ambito della copertura e di gestire l'esposizione al rischio.

---

[161] Da ultimo, tuttavia, Cass. Sez. Un. n. 22437/2018 ha chiarito che "Il modello dell'assicurazione della responsabilità civile con clausole "*on claims made basis*", che è volto ad indennizzare il rischio dell'impoverimento del patrimonio dell'assicurato pur sempre a seguito di un sinistro, inteso come accadimento materiale, è partecipe del tipo dell'assicurazione contro i danni, quale deroga consentita al primo comma dell'art. 1917 c.c., non incidendo sulla funzione assicurativa il meccanismo di operatività della polizza legato alla richiesta risarcitoria del terzo danneggiato comunicata all'assicuratore. Ne consegue che, rispetto al singolo contratto di assicurazione, non si impone un test di meritevolezza degli interessi perseguiti dalle parti, ai sensi dell'art. 1322, secondo comma, c.c., ma la tutela invocabile dal contraente assicurato può investire, in termini di effettività, diversi piani, dalla fase che precede la conclusione del contratto sino a quella dell'attuazione del rapporto, con attivazione dei rimedi pertinenti ai profili implicati, ossia (esemplificando): responsabilità risarcitoria precontrattuale anche nel caso di contratto concluso a condizioni svantaggiose; nullità, anche parziale, del contratto per difetto di causa in concreto, con conformazione secondo le congruenti indicazioni di legge o, comunque, secondo il principio dell'adeguatezza del contratto assicurativo allo scopo pratico perseguito dai contraenti; conformazione del rapporto in caso di clausola abusiva (come quella di recesso in caso di denuncia di sinistro)."

Oltre alla determinazione della probabilità e dell'entità del rischio, il mercato assicurativo valuta la assicurabilità: rischi eccessivi, sistemici o imprevedibili possono risultare inassicurabili o richiedere premi particolarmente elevati.

Ancora, la valutazione del rischio consente di introdurre obblighi di condotta, controlli organizzativi e incentivi per miglioramento delle misure preventive, rafforzando la funzione gestionale del contratto.

In sintesi, il rischio costituisce l'elemento strutturale e organizzativo del contratto di assicurazione. La sua corretta identificazione consente di bilanciare le prestazioni tra le parti, determinare il premio in maniera proporzionata e orientare le misure preventive necessarie per ridurre l'esposizione al sinistro. Pur rimanendo centrale la funzione indennitaria, la gestione del rischio assume un ruolo strategico, ponendo le basi per strumenti assicurativi più specifici e innovativi, capaci di affrontare rischi complessi e interconnessi come quelli digitali.

1.3. Le polizze *cyber*

Si è sin d'ora compreso come l'assicurazione nasca storicamente dall'esigenza di gestire il rischio e di governarne le conseguenze economiche.

Anche dal punto di vista economico, essa rappresenta una tecnica di gestione del rischio (risk management), fondata sulla condivisione tra soggetti portatori

di rischi omogenei (risk sharing) ovvero sul trasferimento del rischio dall'assicurato all'assicuratore (risk transfer).[162]

È tuttavia necessario precisare che l'assicurazione non costituisce uno strumento di eliminazione del rischio, né è in grado, di per sé, di ridurre la probabilità che un evento dannoso si verifichi. La sua funzione consiste piuttosto nel mitigare le conseguenze patrimoniali degli eventi avversi, attraverso un meccanismo di neutralizzazione del rischio che consente all'assicurato di fronteggiare l'incertezza futura senza comprometterne la stabilità economica.

Nel contesto della sicurezza informatica, la prima linea di difesa delle imprese contro le minacce cibernetiche è rappresentata dagli investimenti in tecnologie di protezione, dall'adozione di misure organizzative adeguate e da pratiche di gestione orientate alla prevenzione del rischio.

Tuttavia, la crescente frequenza e sofisticazione degli attacchi rende evidente come tali strumenti, pur indispensabili, non siano sufficienti a garantire una protezione totale.

È in questo scenario che si colloca lo sviluppo di un mercato assicurativo dedicato al rischio cyber, caratterizzato da un numero crescente di operatori che

---

[162] N. DE LUCA, *op. cit.,* "In alternativa, la gestione del rischio può consistere nell'accettazione consapevole (*risk retention*), nell'eliminazione (*risk avoidance*) o nel controllo (*risk reduction).* La scelta sulla tecnica di gestione del rischio è soprattutto una questione di costi, dipendendo dalla comparazione tra quello per evitarlo o mitigarlo e il danno temuto".

cercano di offrire coperture specifiche mediante modelli di valutazione del rischio sempre più articolati.

A differenza dei rischi tradizionali, il rischio cyber presenta caratteristiche che ne rendono particolarmente complessa la valutazione e la gestione assicurativa. Si tratta di un rischio dinamico e in continua evoluzione, influenzato dal rapido progresso tecnologico, dall'emergere di nuove vulnerabilità e dalla crescente interconnessione dei sistemi digitali. A ciò si aggiunge il potenziale di correlazione delle perdite: un singolo evento informatico può colpire simultaneamente una pluralità di soggetti, generando danni cumulativi difficilmente circoscrivibili.

L'attività assicurativa si fonda tradizionalmente su un giudizio di probabilità statistica circa il verificarsi di un determinato evento futuro, elaborato osservando la frequenza di eventi analoghi verificatisi in passato. Grazie ai modelli attuariali, l'assicuratore è in grado di stimare il numero di sinistri attesi e di determinare il premio in modo da rendere sostenibile l'operazione assicurativa nel suo complesso.

Diverse criticità rendono più complessa l'applicazione di questo approccio al rischio cyber. [163]

---

[163] M. BAVIELLO, G. GUARDASCIONE, S. TEDESCO, in *"Rischio cyber" e soluzioni assicurative*, in (a cura di) S. CALÌ, F. CAPPARELLI, M. HAZAN, F. MARTINI, Cybersecurity: tra rischio e responsabilità. Profili operativi in un settore in continua evoluzione, Milano, Giuffrè, 2025, pp. 252 e ss.

Innanzitutto, si registra una carenza di dati storici affidabili e omogenei: molti incidenti informatici non vengono denunciati o sono comunicati in modo incompleto, anche per ragioni reputazionali. Tale mancanza limita la costruzione di modelli predittivi accurati e condiziona la capacità delle compagnie di quantificare il rischio in modo proporzionato.

Un ulteriore profilo critico concerne la variabilità e imprevedibilità delle perdite derivanti da un attacco informatico. Le conseguenze economiche possono differire notevolmente in base alla tipologia di attacco, agli asset coinvolti, alla durata dell'interruzione dei servizi e alla capacità di risposta dell'organizzazione colpita. Questa eterogeneità rende complessa la standardizzazione delle coperture e può condurre alla stipula di polizze non pienamente soddisfacenti né per l'assicurato né per l'assicuratore.

Inoltre, il settore della cybersicurezza richiede elevata specializzazione tecnica. Le compagnie, spesso prive di competenze interne sufficienti, devono avvalersi di soggetti terzi specializzati per la valutazione del rischio e le attività di risk assessment. Pur necessaria, tale collaborazione comporta criticità legate alla condivisione di informazioni sensibili, alla necessità di coordinamento e all'aumento dei costi complessivi del processo di sottoscrizione.

Nonostante queste difficoltà, l'assicurabilità del rischio cyber è oggi non solo possibile ma indispensabile.

In un contesto in cui l'attacco informatico non rappresenta più una mera eventualità, la preparazione delle imprese al rischio digitale diviene imprescindibile.

Tale preparazione implica, innanzitutto, l'identificazione degli asset critici, sia tangibili sia intangibili, spesso sottovalutati, e, in secondo luogo, l'adozione di strategie di gestione e mitigazione del rischio che coinvolgano l'intera organizzazione.

In questo quadro, la polizza assicurativa assume un ruolo centrale quale strumento integrato di gestione del rischio, affiancandosi alle misure preventive e organizzative adottate dall'impresa.

L'assicurazione cyber non sostituisce la gestione del rischio, ma ne è parte essenziale: la cooperazione tra imprese, assicuratori, consulenti di sicurezza informatica e professionisti legali contribuisce a ridurre l'esposizione complessiva e a garantire maggiore resilienza.

Alla luce della crescente centralità del trasferimento del rischio informatico, appare necessario interrogarsi sulla compatibilità delle polizze cyber con la disciplina civilistica vigente.

Sebbene il diritto delle assicurazioni abbia conosciuto una significativa evoluzione per effetto della prassi contrattuale, dell'intervento giurisprudenziale e della normativa di settore[164], gli articoli 1882 e ss. del

[164] Codice delle Assicurazioni Private, d.lgs. n. 209/2005

Codice civile continuano a rappresentare i capisaldi della tipicità contrattuale ai quali anche le più innovative coperture devono conformarsi.[165]

L'analisi degli elementi strutturali del contratto evidenzia come la disciplina tradizionale sia, in linea di principio, idonea a ricomprendere anche il rischio cyber, pur richiedendo un adattamento interpretativo alle peculiarità tecnologiche del fenomeno.

Il rischio mantiene la propria funzione di elemento essenziale del contratto (artt. 1882 e 1895 c.c.): anche nel contesto digitale, l'evento assicurato deve essere futuro e incerto, imponendo una delimitazione precisa dell'oggetto della copertura, soprattutto in presenza di vulnerabilità note o carenze organizzative che incidono sull'alea contrattuale.

Gli istituti codicistici relativi a diminuzione e aggravamento del rischio assumono un rilievo accentuato nel settore cyber. [166]

---

[165] Sul punto, P. CORRIAS, in *Il contratto di assicurazione, profili funzionali e strutturali,* Napoli, Edizioni Scientifiche Italiane, 2016; L. BUTTARO, in *L'interesse nell'assicurazione,* Milano, Giuffrè, 1954; A. GAMBINO, in *Contratto di assicurazione: profili generali,* in Enc. Giuridica Treccani, III, 1-20, 2010; G. SCALFI, in *I contratti di assicurazione,* Torino, 1991.

[166] Art. 1897, co 1, c.c. (Diminuzione del rischio) "Se il contraente comunica all'assicuratore mutamenti che producono una diminuzione del rischio tale che, se fosse stata conosciuta al momento della conclusione del contratto, avrebbe portato alla stipulazione di un premio minore, l'assicuratore, a decorrere dalla scadenza del premio o della rata di premio successiva alla comunicazione suddetta, non può esigere che il minor premio, ma ha facoltà di recedere dal contratto entro due mesi dal giorno in cui è stata fatta la comunicazione."

Art. 1898, co 1, c.c. (Aggravamento del rischio) "Il contraente ha l'obbligo di dare immediato avviso all'assicuratore dei mutamenti che aggravano il rischio in modo tale che, se il nuovo stato di cose fosse esistito

Il rischio può diminuire grazie all'adozione di misure di sicurezza più efficaci o aggravarsi per l'intensificazione delle minacce o l'evoluzione delle tecniche di attacco. Tali mutamenti richiedono un continuo riequilibrio delle prestazioni contrattuali, sottolineando il carattere dinamico della disciplina.

Gli obblighi informativi precontrattuali e la disciplina delle dichiarazioni inesatte o reticenti assumono particolare importanza.[167]

L'asimmetria informativa tra assicuratore e assicurato è spesso accentuata, anche per la limitata consapevolezza delle imprese circa il proprio livello di esposizione. Questionari tecnici, audit e valutazioni specialistiche consentono di delineare correttamente lo stato del rischio, determinando premi proporzionati e accesso a coperture adeguate.

L'interesse all'assicurazione si configura pienamente anche nelle polizze cyber, comprendendo la tutela del patrimonio materiale e immateriale, dati, continuità operativa e reputazione. La principale difficoltà riguarda la titolarità dell'interesse che può riferirsi a beni e informazioni localizzati in infrastrutture digitali esterne.

---

e fosse stato conosciuto dall'assicuratore al momento della conclusione del contratto, l'assicuratore non avrebbe consentito l'assicurazione o l'avrebbe consentita per un premio più elevato."

[167] Art. 1892, co 1, c.c. (Dichiarazioni inesatte e reticenze con dolo o colpa grave) "Le dichiarazioni inesatte e le reticenze del contraente, relative a circostanze tali che l'assicuratore non avrebbe dato il suo consenso o non lo avrebbe dato alle medesime condizioni se avesse conosciuto il vero stato delle cose, sono causa di annullamento del contratto quando il contraente ha agito con dolo o con colpa grave".

Dal punto di vista funzionale, l'assicurazione cyber rientra tra le assicurazioni contro i danni e rispetta il principio indennitario.

Tuttavia, il danno cyber presenta caratteristiche peculiari con perdite economiche indirette difficili da delimitare. In questo contesto assume rilievo l'istituto del profitto sperato, che consente forme di indennizzo per mancato guadagno, come nel caso di interruzioni dell'attività causate da incidenti informatici. Esso viene definito dalla dottrina *come l'insieme di utilità economiche che l'assicurato attendeva di conseguire secondo ragionevoli aspettative, riferendosi agli incrementi patrimoniali divenuti impossibili e persi dall'assicurato in conseguenza del sinistro*.[168]

Questa definizione attribuisce al profitto sperato un significato sostanzialmente analogo a quello del lucro cessante, individuando nella fondata aspettativa di ottenere beni o utilità economiche che, in assenza del sinistro, sarebbero entrati con ragionevole certezza e secondo l'esperienza comune a far parte del patrimonio dell'assicurato, l'oggetto della tutela assicurativa.[169]

Un ulteriore profilo critico riguarda la possibile qualificazione del rischio cyber come rischio catastrofale o sistemico.

---

[168] G. FANELLI, in *Trattato Cicu-Messineo di diritto civile e commerciale* (a cura di) A. CICU, F. MESSINEO, L. MENGONI, vol. XXXVI: "Le assicurazioni", Milano, 2004, p. 154.

[169] F. PECCENINI, in *Commentario del Codice Civile Scialoja-Branca (*a cura di) F. GALGANO - "Libro Quarto - Delle Obbligazioni - Dell'Assicurazione art. 1882 - 1932", Bologna, 2011, p. 116.

L’art. 1912 c.c. disciplina eventi che non sono ordinariamente suscettibili di copertura, escludendo l’obbligo di indennizzo da parte delle imprese.

La diffusività potenziale degli attacchi informatici pone interrogativi simili ed è dunque necessario che le polizze cyber prevedano di coprire simili rischi.

Per tale ragione, le polizze cyber dovrebbero ricorrere a limiti di copertura, esclusioni selettive, coassicurazione e riassicurazione, tutti strumenti che permettono di distribuire l’impatto economico di eventi gravi tra più operatori e di preservare la sostenibilità del sistema assicurativo.

Dunque, un’efficace integrazione della disciplina civilistica con la pratica assicurativa impone di chiarire le attese operative nei confronti delle compagnie.

Esse devono adottare strumenti di valutazione del rischio sofisticati e strutturati, potenziare la raccolta e la condivisione di dati incidentali, rafforzare l’informativa precontrattuale con questionari dettagliati, audit indipendenti e obblighi di disclosure, e offrire servizi integrati di supporto tecnico e consulenziale. Tali azioni consentono di calibrare premi e coperture in modo più aderente alle esigenze del mercato.

In questo contesto si inserisce l’indagine IVASS del 2023 sulle polizze cyber[170] italiane, condotta su circa cinquanta polizze assicurative per la protezione dal

[170] IVASS, in *Indagine sulle polizze a copertura del cyber risk,* 2023, disponibile sul sito internet dell’IVASS. Si legge “L’IVASS ha svolto un’indagine per approfondire le polizze assicurative contro il rischio cyber, c.d.

"polizze cyber", offerte dalle compagnie di assicurazione a protezione dei singoli individui/famiglie (clienti retail) e delle Piccole e Medie Imprese (PMI). L'indagine trae spunto dalla crescente esposizione al rischio cyber riconducibile a più fattori, tra cui: diffusione di nuove tecnologie e crescente interconnessione digitale tra cose, persone, processi e dati; utilizzo della rete Internet a scopi relazionali o per acquisti e vendite online o per usufruire di servizi Home banking; aumento di attacchi informatici anche a seguito di tensioni geopolitiche legate al conflitto in Ucraina. Fattori che rendono gli utenti – famiglie, imprese, enti pubblici – sempre più vulnerabili sotto il profilo della sicurezza informatica. L'indagine si è basata sull'analisi dei contratti e non entra nella valutazione sulla bontà o convenienza delle polizze e prescinde dal successo commerciale delle medesime e dal livello della raccolta premi a esse associato. Il riferimento alle polizze o iniziative commerciali menzionate nel presente Report non implica un'approvazione da parte dell'Istituto.

Il cyber risk è la combinazione della probabilità che si verifichino incidenti cyber e del loro impatto, intendendo per incidente cyber una violazione della sicurezza informatica di un sistema informativo o delle informazioni che il sistema elabora, memorizza o trasmette indipendentemente dal fatto che sia frutto di un'attività dolosa o meno. In particolare, il cyber risk può derivare da incidenti che comportano la violazione, la perdita o la diffusione di dati sensibili, di natura personale ma anche finanziaria, truffe ed estorsioni, cyberbullismo/cyberstalking, furto di identità, lesioni alla reputazione o all'immagine, frodi su acquisti/vendite e-commerce, clonazione di carte di credito/debito, ecc. Per le imprese, inoltre, il cyber risk può a sua volta generare rischi operativi e legali per interruzione dell'attività, violazioni della normativa, richieste estorsive (ransomware), ecc. Le principali evidenze dell'indagine suggeriscono la crescente diffusione di polizze cyber, destinate in particolare alle PMI e, in misura al momento minore, ad individui e famiglie. Le coperture per le PMI sono piuttosto articolate, con garanzie che mirano a coprire le aziende sia dai danni dovuti ad attacchi informatici, sia dai danni causati a terzi per effetto degli attacchi, sia le spese legali. Diverse polizze offrono servizi accessori prima del verificarsi di un attacco informatico (identificazione di vulnerabilità, implementazione di presidi di protezione) e nella gestione post-evento (ristabilimento dell'operatività informatica, gestione danno reputazionale, ecc.). Le coperture sono al momento per lo più standardizzate: a tendere potrebbero beneficiare di una maggiore flessibilità, in modo da calibrare e personalizzare maggiormente le garanzie in funzione della specifica operatività ed esigenza di copertura delle aziende. Nell'ambito delle polizze destinate a individui e famiglie sono coperti i danni conseguenti a furto o clonazione di carte di credito/debito e carte prepagate, furto di identità digitale, acquisti fraudolenti online. Spesso viene

rischio cyber rivolte a individui, famiglie e PMI in commercio al 30 luglio 2023, di tipo stand alone, ossia polizze espressamente disegnate per la copertura del rischio cyber; e modulari, vale a dire polizze che offrono un'ampia gamma di garanzie per il cliente, a copertura della persona o dei beni, organizzate in moduli variamente combinabili e che hanno coperture cyber opzionabili, da acquistare in abbinamento ad altre garanzie.

L'analisi conferma che i rischi legati a violazioni, furto di dati, identità digitale e interruzione dell'attività sono in crescita per la maggiore esposizione degli utenti alle reti informatiche. Evidenzia anche che la diffusione delle polizze cyber è ancora limitata con concentrazione sulle PMI e margini di sviluppo per garanzie più adeguate e maggiore trasparenza su esclusioni e limitazioni.

In particolare, l'IVASS evidenzia la necessità di evolvere verso soluzioni più *consumer-centric*, calibrate sulle specifiche esigenze e sul profilo di rischio dei clienti. La standardizzazione attuale delle polizze potrebbe essere superata

---

fornita all'individuo e al suo nucleo familiare assistenza telefonica e digitale, attraverso un servizio di monitoraggio online che, in caso di sospetto attacco informatico sui device dell'assicurato, consente alla compagnia di contattare un tecnico specializzato per attivare tutte le procedure di analisi e ripristino. Sono presenti coperture anche nella forma della consulenza psicologica a seguito di eventi traumatici legati all'attacco cyber quali cyberbullismo e cyberstalking e dell'assistenza prestata in occasione di frodi nella prenotazione online di un viaggio all'estero. Per entrambe le tipologie si tratta di un mercato destinato a crescere rapidamente, in parallelo al rafforzamento della cultura della sicurezza informatica presso aziende ed individui. L'assistenza di intermediari assicurativi professionisti, adeguatamente aggiornati sui rischi cyber e sugli aspetti molto tecnici di queste polizze, è cruciale per lo sviluppo ulteriore dell'offerta. (…)"

attraverso una maggiore personalizzazione, considerando fattori quali l'operatività digitale dell'azienda, il volume di dati sensibili gestiti e la dipendenza dalla tecnologia.

Risulta in tal senso fondamentale una profilazione accurata del *Target Market* per definire coperture coerenti con l'esposizione effettiva al rischio, includendo anche una revisione delle esclusioni e l'adozione di definizioni uniformi per garantire chiarezza e certezza contrattuale.

L'indagine sottolinea inoltre l'importanza di formazione e aggiornamento della rete distributiva, vista la complessità tecnica delle polizze cyber, e della consulenza professionale per le imprese, al fine di individuare il livello di copertura più adeguato, considerando la natura dell'azienda, la normativa di settore e le condizioni di assicurabilità.

In sintesi, lo sviluppo del mercato delle polizze cyber richiede un approccio integrato che sia in grado di combinare personalizzazione, trasparenza e adeguata gestione del rischio.

Queste evidenze empiriche rafforzano la necessità di un mercato assicurativo cyber più maturo, con prodotti calibrati e trasparenti, supportato da una vigilanza efficace. Solo attraverso l'impegno congiunto di compagnie, regolatori e operatori sarà possibile sviluppare coperture non solo compatibili con la disciplina civilistica, ma efficaci, sostenibili e adeguate alle sfide del rischio digitale emergente.

In conclusione, l'analisi conferma il ruolo tradizionale dell'assicurazione come strumento di gestione del rischio idoneo a offrire protezione patrimoniale contro eventi incerti e potenzialmente devastanti. Al contempo, esercita una funzione di incentivo e regolazione, promuovendo comportamenti organizzativi più attenti alla sicurezza e incoraggiando investimenti in misure preventive. In questa duplice prospettiva, la polizza cyber non si limita a trasferire il rischio, ma diventa un elemento strutturale di governance del rischio digitale, integrando gestione tecnica, organizzativa e assicurativa in un approccio coerente e sostenibile.

1.4. Insurtech

Negli ultimi anni, accanto alle logiche tradizionali, il settore assicurativo ha vissuto una trasformazione profonda, guidata dall'adozione di tecnologie digitali e dall'emergere del fenomeno InsurTech.[171]

Questa evoluzione non si limita a un aggiornamento tecnico dei processi esistenti, ma ridefinisce in modo sostanziale il modello di business, le modalità di gestione del rischio e la relazione con i clienti.

La tradizionale funzione dell'assicurazione, e cioè gestire l'incertezza futura mediante la mutualizzazione dei rischi, è ora affiancata da approcci che

[171] Il sociologo francese Francois Ewald ha sottolineato che questa particolare integrazione strumenti digitali e pratiche assicurative apre una fase di trasformazione significativa per il settore, "un nuovo mondo", i cui risultati rimangono al momento incerti.

combinano dati, algoritmi predittivi e strumenti digitali, aprendo nuove opportunità ma sollevando anche sfide di natura etica, sociale e commerciale.

Storicamente, l'assicurazione ha avuto il compito di trasformare l'incertezza individuale in rischio collettivo. Pagando un premio, l'assicurato contribuisce a un fondo comune che consente di compensare i sinistri di chi è più "sfortunato", mentre la compagnia di assicurazione ottiene un margine di profitto. Questo modello tradizionale si basa sulla statistica e sulla probabilità, elementi che permettono di prevedere le perdite medie di un gruppo di assicurati, pur mantenendo un margine di incertezza residuale.

L'incertezza, lungi dall'essere un problema da eliminare, rappresenta infatti la condizione necessaria perché l'assicurazione esista: se il futuro fosse completamente prevedibile, né assicuratore né assicurato avrebbero motivo di stipulare un contratto. [172]

Con l'introduzione di dispositivi digitali, l'assicurazione entra in un'era caratterizzata dall'assicurazione delle cose e dalle polizze comportamentali.

Questi strumenti raccolgono dati in tempo reale sul comportamento degli assicurati permettendo alle compagnie di calcolare premi personalizzati basati sul comportamento individuale piuttosto che sull'evento del sinistro.

---

[172] Sul punto, si veda A. CEVOLINI, E. ESPOSITO, in *Il futuro dell'assicurazione. Opportunità e minacce delle tecnologie digitali nell'assicurazione del futuro*, in *Il futuro delle organizzazioni. Lavoro e creatività*. (A cura di R. POLI, M. DI BERARDO, R PAURA), in *Rivista Italiana di Future Studies,* p. 51.

Questa iper-personalizzazione promette vantaggi evidenti. Gli assicurati possono beneficiare di premi più equi, coerenti con la propria esposizione reale al rischio, mentre le compagnie possono ottimizzare la selezione del rischio e ridurre le perdite.

Tuttavia, il passaggio dalla mutualità tradizionale alla profilazione individuale comporta rischi rilevanti. La segmentazione algoritmica, se applicata senza adeguate regole etiche, può generare discriminazioni e minare il principio di solidarietà su cui si fonda il modello assicurativo. [173]

La disponibilità di grandi quantità di dati e l'uso di algoritmi avanzati aprono anche prospettive proattive di gestione del rischio. Le compagnie possono non solo compensare il danno post-evento, ma prevenirlo.

Con specifico riferimento al rischio cyber, l'impiego di strumenti di intelligenza artificiale può rappresentare per le imprese assicurative un supporto rilevante nella comprensione e nella gestione del rischio, nella misura in cui tali tecnologie consentono una più articolata attività di valutazione.

In particolare, mediante tecniche di machine learning e di elaborazione del linguaggio naturale, l'intelligenza artificiale può essere utilizzata per l'analisi delle minacce informatiche e per l'individuazione di anomalie nei sistemi, contribuendo a una più efficace attività di prevenzione e di governo del rischio.

---

[173] Sul punto si veda, A. CEVOLINI, in *Insurtech. Tra rischio e mutualità,* in *Insurance Review*, 2020, pp. 56-57.

È evidente che l'InsurTech non sia un fenomeno puramente tecnico, ma un cambiamento intersoggettivo e sociale. L'assicurazione, osservata dall'interno della società, interagisce con le azioni e le aspettative degli individui, modificando a sua volta i comportamenti e le percezioni di rischio. In questo senso, l'innovazione digitale modifica il ruolo dell'assicurazione come istituzione sociale, capace di influenzare le scelte economiche e individuali.

Il report "On the digitalisation of the european insurance sector" dell'EIOPA[174] conferma questa tendenza ed evidenzia in che modo l'adozione di strumenti digitali stia trasformando i processi assicurativi in tutta Europa.

L'analisi segnala che le compagnie stanno investendo massicciamente in telematica, *data analytics*, intelligenza artificiale e piattaforme digitali per migliorare la sottoscrizione, la prevenzione dei sinistri e la personalizzazione dei prodotti. Allo stesso tempo, l'EIOPA sottolinea la necessità di sviluppare un quadro normativo chiaro che tuteli la privacy dei consumatori, eviti discriminazioni algoritmiche e salvaguardi la funzione sociale dell'assicurazione.

---

[174] European Insurance and occupational pensions authority (EIOPA), in *Report on the the digitalisation of the european insurance sector,* 2024,in https://www.eiopa.europa.eu/publications/eiopas-report-digitalisation-european-insurance-sector_en, pp. 5 e ss.

La digitalizzazione non è quindi solo una questione tecnologica, ma anche regolatoria e etica, e il successo del settore dipenderà dalla capacità di integrare innovazione, gestione del rischio e tutela dei diritti degli assicurati.

In sintesi, l'Insurtech rappresenta una trasformazione dirompente per il settore assicurativo. Da un lato, le tecnologie digitali offrono opportunità senza precedenti per migliorare la gestione del rischio, ottimizzare la selezione del cliente, personalizzare il premio e prevenire danni futuri. Dall'altro, pongono questioni complesse riguardo a equità, mutualità, privacy e impatto sociale.

Anche nel settore assicurativo, la digitalizzazione impone di valorizzarne appieno le potenzialità senza compromettere i principi fondamentali dell'assicurazione, e in particolare la gestione collettiva dell'incertezza, che continua a rappresentare una risorsa sociale imprescindibile.

Bibliografia

ACN, *Cybersecurity Governance Fundamentals. La valutazione del contesto cyber di un'organizzazione*.

ACN, *Relazione al Parlamento*, 2023.

AGENDA DIGITALE, *Sicurezza delle informazioni: i tre principi per gestire il cyber risk*, 2023.

ALBANESE A., *La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione*, Europa e diritto privato, 2019.

ALPA G., *Il diritto dei consumatori*, Roma-Bari, Laterza, 1995.

ALPA G., *L'attuazione della direttiva nei Paesi della CEE*, in *La responsabilità del produttore*, a cura di G. Alpa, R. Bin, P. Cendon, Trattato di diritto commerciale e di diritto pubblico dell'economia diretto da F. Galgano, XIII, Padova, 1989.

ALPA G., *La responsabilità civile*, in *Trattato di diritto civile*, IV, Milano, 1999.

ALPA G. – BESSONE M., *La responsabilità del produttore*, Milano, Giuffrè, 1999.

ALPA G. – CATRICALÀ A., *Il diritto dei consumatori*, Bologna, Il Mulino, 2016.

AMENTA V. – DELUCA R., *L'approccio alla cybersecurity nello scenario normativo europeo*, La Comunicazione – Note, recensioni e notizie, 68, 2024.

AMIDEI A., *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, 2017.

BAVIELLO M., GUARDASCIONE G., TEDESCO S., *"Rischio cyber" e soluzioni assicurative*, in (a cura di) Calì, Capparelli, Hazan, Martini, Cybersecurity: tra rischio e responsabilità. Profili operativi in un settore in continua evoluzione, Milano, Giuffrè, 2025.

BECK U., *La società del rischio. Verso una seconda modernità*, Roma, Carocci, 2013.

BERTOLINI A., *Intelligenza artificiale e responsabilità civile. Problema, sistema, funzioni*, Bologna, Il Mulino, 2025.

BRIGHI R. – CHIARA P.G., *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione europea*, federalismi.it, 2021.

BUTTARO L., *L'interesse nell'assicurazione*, Milano, Giuffrè, 1954.

BUSNELLI F.D., *Illecito civile*, Enciclopedia giuridica, 1991.

CALABRESI G., *The Costs of Accidents: A Legal and Economic Analysis*, New Haven, 1970.

CALÌ S. – CAPPARELLI F. – HAZAN M. – MARTINI F., *Cybersecurity: tra rischio e responsabilità. Profili operativi in un settore in continua evoluzione*, Milano, Giuffrè, 2025.

CAPPELLETTI F. – MARTINO L., *Achieving robust European cybersecurity through public-private partnerships: approaches and developments*, ELF Discussion Papers, 4, 2021.

CARNEVALI U., *La responsabilità del produttore*, Milano, Giuffrè, 1974.

CARNELUTTI F., *Sulla distinzione tra colpa contrattuale e colpa extracontrattuale*, nota di commento ad App. Venezia, Rivista del diritto commerciale, 1912.

CARUSI D., *L'attuazione e tutela dei diritti*, in *Diritto civile*, III, La responsabilità e il danno, a cura di N. Lipari, P. Rescigno, coord. A. Zoppini.

CASTRONOVO C., *La nuova responsabilità civile*, Milano, Giuffrè, 2006.

CAZZETTA G., *Responsabilità aquiliana e frammentazione del diritto comune civilistico (1865–1914)*, Milano, Giuffrè, 1991.

CEVOLINI A. – ESPOSITO E., *Il futuro dell'assicurazione. Opportunità e minacce delle tecnologie digitali nell'assicurazione del futuro*, in *Il futuro delle organizzazioni. Lavoro e creatività* (a cura di R. Poli, M. Di Berardo, R. Paura), Rivista italiana di Future Studies, 2020.

CEVOLINI A., *Insurtech. Tra rischio e mutualità*, Insurance Review, 2020.

CHIARA P.G., *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, Rivista italiana di informatica e diritto, 1, 2023.

CHIARA P.G. – BRIGHI R., *La dimensione della resilienza nel diritto UE della cybersicurezza*, Il Mulino – Rivistaweb, 2024.

COMANDÉ G., *Gli strumenti della precauzione: nuovi rischi, assicurazione e responsabilità*, Milano, Giuffrè, 2016.

COMANDÉ G., *Intelligenza artificiale e responsabilità tra liability e accountability*, Analisi giuridica dell'economia, 1, 2019.

COMMISSIONE DELLE COMUNITÀ EUROPEE, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, 2001.

COMMISSIONE EUROPEA – ALTO RAPPRESENTANTE DELL'UNIONE EUROPEA PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, 2013.

COMMISSIONE EUROPEA – ALTO RAPPRESENTANTE DELL'UNIONE EUROPEA PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, 2017.

CORRIAS P., *Il contratto di assicurazione, profili funzionali e strutturali*, Napoli, Edizioni Scientifiche Italiane, 2016.

DE GREGORIO G. – DUNN P., *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, Common Market Law Review, 59, 2022.

DE LUCA N., *Diritto ed economia delle assicurazioni*, Bologna, Il Mulino, 2022.

DE MENECH C., *La responsabilità vicaria nel diritto vivente*, Nuova giurisprudenza civile commentata, 2017.

DI DONNA L., *Il principio di responsabilità nel settore dei beni e dei servizi*, Rivista italiana per le scienze giuridiche, 2014.

DI DONNA L., *Intelligenza artificiale e rimedi risarcitori*, Padova, CEDAM, 2022.

DURANTE M., *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*, in M.V. D'Alfonso (a cura di), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence*, Springer, 2019.

ECA, *Le sfide insite in un'efficace politica dell'UE in materia di cybersicurezza*, 2019.

EIOPA, *Report on the the digitalisation of the european insurance sector*, 2024.

ENISA, *Overview of Cybersecurity and Related Terminology*, 2017.

ENISA, *L'anno in rassegna da gennaio 2019 ad aprile 2020. Rapporto Clusit 2021 sulla sicurezza ICT in Italia*, 2021.

FARENGA L., *Manuale di diritto delle assicurazioni private*, Giappichelli, 2025.

FANELLI G., *Trattato Cicu-Messineo di diritto civile e commerciale*, a cura di A. Cicu, F. Messineo, L. Mengoni, vol. XXXVI: *Le assicurazioni*, Milano, 2004.

FLOR R., *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, Diritto di Internet, 3, 2019.

FLORIDI L., *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022.

FRANZONI M., *Dei fatti illeciti (2043–2059)*, in A. Scialoja – G. Branca (a cura di), *Commentario al Codice civile*, Bologna, Zanichelli, 1993.

FRANZONI M., *L'illecito*, Trattato della responsabilità civile, 2010.

GALLETTA D.U., *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini*, Ciberspazio e diritto, 3, 2018.

GALGANO F., *Le antiche e le nuove frontiere della responsabilità civile*, Contratto e impresa, 2008.

GAMBINO A., *Contratto di assicurazione: profili generali*, Enciclopedia Giuridica Treccani, III, 1-20, 2010.

GHIDINI C., *Prevenzione e risarcimento nella responsabilità del produttore*, Rivista delle società, 1975.

GIOVAGNOLI R., *Manuale di diritto civile*, vol. V, Itaedizioni, 2025.

HILDEBRANDT M., *Law for Computer Scientists and Other Folk*, 2020.

IBM, *Cos'è un Security Operations Center (SOC)*, 2025.

IRTI N., *Una generazione di giuristi. La cultura del diritto civile*, 1990.

IVASS, *Indagine sulle polizze a copertura del cyber risk*, 2023.

JONAS H., *Il principio di responsabilità. Un'etica per la civiltà tecnologica*, 1990.

LANDINI S., *Assicurazione e responsabilità*, Milano, Giuffrè, 2004.

LEVY J., *No need to reinvent the wheel: why existing liability law does not need to be preemptively altered to cope with the debut of the driverless car*, The Journal of Business, Entrepreneurship & the Law, 9, 2016.

MACIOCE F., *Responsabilità del produttore, armonizzazione dei mercati e prospettive di riforma nell'ottica della tutela del consumatore*, Responsabilità, comunicazione, impresa, 2005.

MARCHIONATTI R. – MORNATI F., *Principi di economia politica*, Torino, Giappichelli, 2011.

MIRABILE G., *Le tendenze evolutive della giurisprudenza riguardo alla nozione di attività pericolosa*, Responsabilità civile e previdenza, 2, 2018.

MONATERI G., *La responsabilità civile*, Torino, 1998.

MONTESSORO P.L., *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, Istituzioni del federalismo, 2019.

MULLIGAN D.K. – SCHNEIDER F.B., *Doctrine for Cybersecurity*, Daedalus, 104(4), 2011.

NIELES G. – DEMPSEY K. – PILLITTERI V.Y., *An Introduction to Information Security*, NIST Special Publication 800-12, 2017.

PANZA A., *La sicurezza nazionale. Innovazione e nuovi limiti*, Gnosis, 1, 2019.

PARDOLESI R. – CARUSA D., *Per una storia della Direttiva 85/374/CEE*, Danno e responsabilità, 2012.

PARZIALE A., *Art. 2050 c.c.: dieci anni vissuti… pericolosamente*, Danno e responsabilità, 2019.

PECCENINI F., *Commentario del Codice Civile Scialoja-Branca*, a cura di F. Galgano, *Libro Quarto - Delle Obbligazioni - Dell'Assicurazione art. 1882 - 1932*, Bologna, 2011.

PONTI B., *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, Rivista italiana di informatica e diritto, 2024.

PÜTZ F. – MURPHY F. – MULLINS M. – MAIER K. – FRIEL R. – ROHLFS T., *Reasonable, Adequate and Efficient Allocation of Liability Costs for Automated Vehicles*, European Journal of Risk Regulation, 2018.

RATTI M., *La responsabilità da illecito trattamento di dati personali nel nuovo Regolamento*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017.

RENNA M., *Il principio di precauzione e la sua attuabilità*, Forum di Quaderni costituzionali, 2, 2023.

RIZZI M.A. – SERINI F., *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, Rivista italiana di informatica e diritto, 2, 2024.

RODOTÀ S., *Tecnologi dell'informazione e frontiere del sistema socio-politico*, Politica del diritto, 1982.

ROSENZWEIG P., *Cybersecurity and Public Goods: The Public/Private Partnership*, in *Cyberwarfare: How Conflicts in Cyberspace are Challenging the World*, 2012.

ROSSELLO C., *Commercio elettronico. La governance di Internet tra diritto statuale, autodisciplina e soft law*, Milano, Giuffrè, 2006.

ROSSETTI M., *Il diritto delle assicurazioni*, I, Padova, Cedam, 2011.

RUFFOLO U., *La responsabilità vicaria*, 1976.

RUFFOLO U., *La colpa*, in *Diritto civile*, IV, Attuazione e tutela dei diritti. La responsabilità e il danno, a cura di N. Lipari, P. Rescigno, coord. A. Zoppini, 2009.

RUFFOLO U. (a cura di), *Intelligenza artificiale e responsabilità*, Milano, Giuffrè, 2017.

RUFFOLO U., *Responsabilità da A.I. e da algoritmo*, in *Intelligenza artificiale. Il diritto, i diritti e l'etica*, 2020.

RUFFOLO U., *Le responsabilità da Intelligenza Artificiale e le questioni di libertà d'espressione e copyright*, Contratto e impresa, 2025.

SICA S., *La responsabilità civile tra struttura, funzioni e valori*, Responsabilità civile e previdenza, 1994.

SIMONINI G., *La responsabilità da prodotto e l'interpretazione conforme al diritto comunitario*, Contratto e impresa, 2013.

SCALFI F., *I contratti di assicurazione,* 1991.

SCOGNAMIGLIO R., *Responsabilità civile*, Novissimo Digesto Italiano, vol. XV, 1982.

SORRENTINO E. – SPAGNUOLO A.F., *Cybersecurity e sovranità digitale nella protezione dei dati personali*, Rivista italiana di informatica e diritto, 2024.

TADDEO M., *Is Cybersecurity a Public Good?*, Minds and Machines, 29, 2019.

TRIAILLE J.-P., *L'applicazione della Direttiva comunitaria sulla responsabilità del produttore nel campo del software*, Diritto dell'informatica, 1990.

TRIMARCHI P., *Istituzioni di diritto privato*, Milano, Giuffrè, 1973.

TRIMARCHI P., *La responsabilità del fabbricante nella direttiva comunitaria*, Rivista di diritto societario, 1986.

TRIMARCHI P., *Responsabilità civile, atti illeciti, rischio, danno*, III ed., Milano, Giuffrè, 2021.

VASUDEVAN A., *Addressing the liability gap in artificial intelligence*, CIGI Policy Brief, 2023.

VOIGT P., *The EU General Data Protection Regulation (GDPR)*, Springer, 2017.

ZACCARIA A., *La responsabilità del produttore di software*, Contratto e impresa, 1993.

.