Eunomia. Rivista di studi su pace e diritti umani
Eunomia XIV n.s. (2025), n. 2, 139-159
e-ISSN 2280-8949
DOI 10.1285/i22808949a14n2p139
http://siba-ese.unisalento.it, © 2025 Università del Salento

GIUSEPPE GIOFFREDI
UNIVERSITÀ DEL SALENTO

*Cybersicurezza e diritto alla salute nella sanità digitale**

Cybersecurity and the Right to Health in Digital Healthcare

Abstract: Il contributo analizza l'impatto della trasformazione digitale sul diritto alla salute, evidenziando come la cybersicurezza rappresenti oggi una componente strutturale della tutela dei diritti fondamentali nel settore sanitario. Muovendo da una prospettiva multilivello che integra diritto internazionale dei diritti umani, diritto dell'Unione europea e ordinamenti nazionali, lo studio esamina l'evoluzione del quadro normativo europeo – dalla protezione dei dati alla resilienza digitale – con particolare riferimento alla direttiva NIS2, al regolamento sui dispositivi medici e al Cyber Resilience Act. L'analisi si concentra inoltre sulle criticità attuative nel contesto italiano, mettendo in luce il divario tra armonizzazione normativa e implementazione sostanziale. Il contributo sostiene che la sicurezza delle infrastrutture sanitarie digitali costituisca una precondizione dell'effettività del diritto alla salute, configurandosi come espressione contemporanea degli obblighi positivi dello Stato nella tutela della dignità della persona.

Abstract: This article examines the impact of digital transformation on the right to health, arguing that cybersecurity has become a structural component of fundamental rights protection in the healthcare sector. Adopting a multilevel perspective that integrates international human rights law, European Union law and national legal systems, the study analyses the evolution of the EU regulatory framework – from data protection to digital resilience – with particular reference to the NIS2 Directive, the Medical Devices Regulation and the Cyber Resilience Act. It also explores the implementation challenges in the Italian context, highlighting the gap between formal harmonisation and effective enforcement. The article argues that the security of digital health infrastructures is a precondition for the effective enjoyment of the right to health, reflecting contemporary positive obligations of the State in safeguarding human dignity.

Keywords: Diritto alla salute; cybersicurezza; sanità digitale; diritto fondamentali; governance multilivello

Keywords: Right to health; Cybersecurity; Digital health; Fundamental rights; Multilevel governance

1. *Sanità digitale e trasformazione del diritto alla salute.*

Muovendo dall'intreccio tra diritto dell'Unione, obblighi internazionali in materia di diritti fondamentali e recepimento nazionale, lo studio mira ad esaminare la nuova costellazione normativa delineata, in particolare, dalla direttiva NIS2, dal regolamento sui dispositivi medici e dal Cyber Resilience Act, valutando criticamente il grado di implementazione nell'ordinamento italiano. L'analisi si propone di dimostrare come la sicurezza informatica non possa più essere considerata un profilo meramente tecnico, ma si configuri quale precondizione giuridica per l'accesso equo, sicuro e continuativo alle prestazioni sanitarie digitali, con ricadute dirette sulla responsabilità delle amministrazioni pubbliche e sulla governance multilivello dei diritti fondamentali.

La progressiva digitalizzazione dei sistemi sanitari europei ha infatti prodotto un mutamento strutturale delle modalità di erogazione delle prestazioni, della gestione dei dati clinici e dell'organizzazione dei servizi pubblici della salute. Tale trasformazione, accelerata dalla pandemia da COVID-19[1] e consolidata attraverso gli investimenti del Next Generation EU[2], ha reso la sanità uno degli ambiti più esposti alle vulnerabilità cibernetiche, collocandola al centro delle politiche europee di sicurezza delle reti e dei sistemi informativi.

In questo contesto, la cybersecurity[3] cessa di essere una questione settoriale per assumere una dimensione sistemica, che interseca direttamente il diritto alla salute, la protezione dei dati personali e il principio di continuità dei servizi pubblici essenziali. La

---

*Il contenuto del presente scritto è anche destinato al volume, in corso di pubblicazione per Carocci editore (collana sulla *Cittadinanza digitale*), che raccoglie i risultati delle attività di ricerca del progetto PNRR ILACY-Italian Law for a Cyber-physical Ecosystem (partenariato esteso *Security and RIghts in the CyberSpace* (*SERICS*), spoke 8 *Risk Management and Governance*).

[1] E. Sorrentino, A.F. Spagnuolo, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in "Federalismi.it", 30, 2020, p. 242 ss.

[2] V. https://next-generation-eu.europa.eu/index_it.

[3] La cybersecurity si riferisce alla pratica di proteggere i sistemi informatici, le reti e i dati da attacchi informatici, accessi non autorizzati e altre forme di minacce informatiche. Essa comprende un'ampia gamma di strategie, tecnologie, processi e pratiche progettate per salvaguardare le informazioni sensibili, mantenere l'integrità dei sistemi e garantire la disponibilità di risorse critiche. Cfr. G.M. Ruotolo, *Intelligenza artificiale e cybersecurity*, in V. Lorubbio-S. De Vido, *Diritto internazionale delle emergenze*, Pacini, Pisa, 2026, p. 161 ss.

crescente interdipendenza tra infrastrutture digitali, dispositivi medici connessi e piattaforme di interoperabilità sanitaria impone, infatti, una rilettura delle tradizionali categorie giuridiche alla luce di un nuovo paradigma di rischio, nel quale la compromissione informatica può tradursi immediatamente in pregiudizio fisico, discriminazione nell'accesso alle cure o interruzione delle prestazioni.

Un esempio emblematico è rappresentato dall'attacco ransomware che ha colpito i sistemi della Regione Lazio nell'agosto del 2021. Questo incidente non è stato un semplice data breach[4], ma ha paralizzato un'infrastruttura pubblica critica nel pieno di un'emergenza sanitaria, bloccando servizi essenziali per i cittadini come la prenotazione dei vaccini. L'evento ha messo a nudo la vulnerabilità sistemica delle nostre istituzioni e ha dimostrato come un attacco cyber possa minacciare direttamente la continuità dei servizi pubblici e la sicurezza dei dati sensibili di milioni di persone[5].

La cybersecurity dunque riveste oggi un ruolo fondamentale. Essa è una priorità assoluta per le organizzazioni di ogni dimensione – quindi anche per lo Stato nel suo complesso e per i suoi asset strategici – considerando che, con l'aumento della dipendenza dalle tecnologie digitali, cresce anche il rischio di attacchi informatici che possono mettere a repentaglio dati sensibili, reputazione e, in casi estremi, la sopravvivenza stessa di un'organizzazione[6].

[4] Si tratta di una violazione della sicurezza che comporta la distruzione, perdita, modifica, divulgazione non autorizzata o accesso accidentale/illecito a dati personali, sensibili o riservati. Spesso causato da attacchi informatici (hacking), furti di dispositivi o errori umani, richiede la notifica all'autorità garante entro 72 ore (GDPR) se comporta rischi per gli interessati. Per approfondimenti sulle violazioni di dati personali in base alle previsioni del Regolamento (UE) 2016/679 v. https://www.garanteprivacy.it/data-breach.

[5] In argomento v. L. Bolognini, *Privacy e diritto dei dati sanitari*, Milano, Giuffrè, 2024; S. Corso, A. Thiene (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, Jovene, 2023; V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019; G.M. Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Cacucci Editore, Bari, 2021; G.M. Ruotolo, *Intelligenza Artificiale e trattamento dei dati tra diritto internazionale e ordinamenti interni*, in AI Law 2/2025.

[6] L'aumento vertiginoso di attacchi informatici sempre più sofisticati e mirati è dovuto a una serie di fattori, che assumono una connotazione specifica: l'aumento quantitativo di tali attacchi; lo sfruttamento delle vulnerabilità emergenti; l'aumento degli attacchi basati sull'intelligenza artificiale; la crescente superficie di attacco (con l'aumento dell'utilizzo di dispositivi mobili, cloud computing e *Internet of Things-IoT*, la superficie di attacco per i cybercriminali si è ampliata esponenzialmente); la carenza di competenze in materia di sicurezza informatica; la crescente mole di dati (la quantità esponenziale di dati generati e archiviati richiede soluzioni di sicurezza in grado di proteggerli e analizzarli in modo efficiente, anche in tempo reale); la crescente complessità normativa (le normative sulla privacy e la protezione dei dati in

L'obiettivo del presente contributo è analizzare tale mutamento attraverso una prospettiva multilivello, che muove dal diritto internazionale dei diritti umani, si sviluppa nel quadro normativo dell'Unione europea e approda al recepimento nazionale, anche con riferimento al ruolo del procurement pubblico sanitario quale strumento di attuazione concreta degli obblighi di sicurezza. In questa prospettiva, l'ordinamento italiano viene assunto come caso di studio per verificare la distanza, tuttora significativa, tra armonizzazione formale e implementazione sostanziale delle nuove prescrizioni europee.

2. *Il diritto alla salute quale diritto fondamentale.*

La progressiva digitalizzazione dei sistemi sanitari europei ha determinato un mutamento strutturale delle modalità di erogazione delle prestazioni, della gestione delle informazioni cliniche e dell'organizzazione complessiva dei servizi pubblici della salute. Tale trasformazione, già in atto da oltre un decennio, ha conosciuto un'accelerazione significativa nel periodo pandemico, consolidandosi successivamente attraverso gli investimenti del Next Generation EU e le strategie europee in materia di sanità digitale.

In questo contesto, l'ambito della tutela della salute è progressivamente emerso come uno dei settori maggiormente esposti alle minacce digitali, assumendo un rilievo centrale nelle strategie dell'Unione europea volte al rafforzamento della resilienza delle infrastrutture critiche e alla protezione delle reti informative. L'interconnessione crescente tra infrastrutture digitali, piattaforme di interoperabilità e dispositivi medici collegati ha infatti ampliato in modo considerevole la superficie di attacco dei sistemi sanitari, rendendo evidente come la compromissione informatica possa tradursi immediatamente in pregiudizio fisico, interruzione delle cure o violazione dei diritti

continua evoluzione, come il GDPR, aumentano la complessità per le aziende nel rispettare le normative e proteggere i dati sensibili); il fattore umano (gli esseri umani, nonostante i progressi nella tecnologia della sicurezza, rimangono uno degli anelli più deboli della sicurezza informatica, ed infatti gli attacchi di phishing, ingegneria sociale e altre forme di manipolazione continuano ad avere successo a causa dell'errore umano e della mancanza di consapevolezza di questi rischi); la crescente minaccia da parte degli insider (le minacce interne, come dipendenti malintenzionati o ex dipendenti con accesso ai dati aziendali, rappresentano un rischio significativo per la sicurezza informatica).

fondamentali della persona.

Ad esempio, il già citato attacco informatico che ha paralizzato i sistemi della Regione Lazio ha rappresentato un attacco diretto a un'infrastruttura pubblica critica, interrompendo servizi essenziali per la comunità – come le prenotazioni sanitarie in piena pandemia – e colpendo il patto di fiducia tra cittadini e istituzioni che è il fondamento del patrimonio sociale e culturale collettivo[7].

Ne deriva una trasformazione profonda del significato giuridico della cybersecurity, che cessa di essere una questione settoriale o meramente tecnica per assumere una dimensione sistemica, strettamente intrecciata al diritto alla salute, alla protezione dei dati personali e al principio di continuità dei servizi pubblici essenziali. La sicurezza informatica diviene così parte integrante del contenuto sostanziale del diritto alla salute, incidendo direttamente sulla possibilità per gli individui di accedere a prestazioni sanitarie sicure, affidabili e non discriminatorie.

Lo sviluppo vorticoso della tecnologia ha fatto si che in tale settore l'attenzione per il tema della sicurezza fosse prioritario. Secondo il rapporto 2025 di CLUSIT (*Associazione Italiana per la Sicurezza Informatica*)[8], per quanto riguarda i target e gli obiettivi degli attacchi, il trend - già registrato a partire dallo scorso anno[9] - mostra un'attenzione particolare verso le strutture del comparto sanitario. I dati in esse contenuti sono molto ricercati dagli attori ostili, in quanto hanno un mercato fiorente sul dark web, essendo molto richiesti e venduti facilmente a un prezzo elevato e sicuramente maggiore rispetto a dati di altra natura. Queste informazioni, una volta che entrano nella disponibilità delle *crew* criminali, costituiscono una fonte di lucro considerevole, rivelando dati sensibili dei

[7] L'attacco è stato perpetrato sfruttando le credenziali di un dipendente che lavorava in smart working in un momento storico in cui non si erano ancora affermate delle pratiche di sicurezza adeguate, evidenziando per la prima volta, in Italia, il rischio associato al "fattore umano" e alla sicurezza degli accessi remoti. L'attacco ha avuto un fortissimo impatto locale, paralizzando il Centro Elaborazione Dati (CED) della Regione e mandando offline il portale regionale.

[8] V. https://clusit.it/rapporto-clusit.

[9] Il settore della sanità ha registrato 624 attacchi cyber a livello globale, oltre il doppio del 2022 quando erano stati "solo" 304, con il 90% degli incidenti di sicurezza che ha avuto impatti gravi (58%) o gravissimi (32%) sulle organizzazioni colpite. Medesima accelerazione, in Italia, dove – considerando quelli di pubblico dominio nel settore *healthcare* – si sono contate il 67% delle violazioni in più che nel 2023 (da 9 a 15) con il 60% che ha avuto impatti che si sono rivelati particolarmente gravi.

pazienti in cura, la cui violazione può avere conseguenze molto gravi. Da tali dati è possibile sottolineare che le strutture sanitarie oggi stanno progressivamente adeguando il livello di protezione cyber richiesto dai processi di digitalizzazione della nostra società. Occorre tuttavia incentivare campagne di sensibilizzazione da parte di queste istituzioni, che risultano maggiormente esposte, ovverosia far in modo che esse dimostrino concretamente di possedere le *skills* per gestire questi dati sensibili, strutturando al loro interno processi affidabili e disponendo di un'organizzazione interna in grado di risolvere problemi di gestione di attacchi in tempi rapidi. Dati analoghi emergono anche dal Check Point Report 2025 (*Centro Risorse per la Sicurezza Informatica*) secondo cui il settore dell'istruzione è il più colpito dagli attacchi informatici, seguito dal settore governativo/militare e da quello, appunto, sanitario[10].

Sul piano internazionale, il diritto alla salute è riconosciuto quale diritto fondamentale della persona, strettamente connesso alla dignità umana e al principio di non discriminazione, configurandosi come presupposto imprescindibile per l'esercizio effettivo di tutti gli altri diritti e libertà fondamentali[11]. Esso trova un primo riconoscimento solenne nell'art. 25 della Dichiarazione universale del 1948 e riceve una consacrazione giuridicamente vincolante nell'art. 12 del Patto internazionale sui diritti economici, sociali e culturali del 1966, che impegna gli Stati parti ad adottare misure volte ad assicurare «il godimento del più alto livello possibile di salute fisica e mentale». Tale disposizione è stata progressivamente arricchita di contenuto dal Comitato delle Nazioni

[10] Il rapporto rivela che nel 2025 le organizzazioni hanno subito in media 1.968 attacchi informatici alla settimana, con un aumento del 70% rispetto al 2023, poiché gli aggressori sfruttano sempre più l'automazione e l'intelligenza artificiale per muoversi più rapidamente, scalare più facilmente e operare su più superfici di attacco contemporaneamente. In Italia nel 2025 il numero di attacchi settimanali è superiore al dato mondiale del 18%: sono stati, infatti, registrati in media ogni settimana 2.334 cyber attacchi alle aziende e alle organizzazioni (+17% rispetto al dato del 2024), colpendo principalmente il settore governativo (4.764 attacchi), il settore dei servizi e dei beni di consumo (2.884 attacchi) e quello dei servizi finanziari con 2.011 attacchi.

[11] V., per tutti, Aa.Vv, *La tutela della salute nel diritto internazionale ed europeo tra interessi globali e interessi particolari*, Napoli, Editoriale Scientifica, 2017; B.C.A. Toebes, *The Right to Health as a Human Right in International Law*, Antwerpen-Oxford-New York, Intersentia, 2015; B.M. Meier, L.O. Gostin, *Human Rights in Global Health. Rights-Based Governance for a Globalizing World*, Oxford University Press, Oxford, 2018; C. O Neill, C. Foster, J. Herring, J. Tingle (*eds.*), *Routledge Handbook of Global Health Rights*, London-New York, Routledge, 2021.

Unite sui diritti economici, sociali e culturali (CESCR), in particolare attraverso il Commento generale n. 14 (2000), che ha chiarito come il diritto alla salute non si esaurisca nell'accesso alle cure mediche, ma comprenda un insieme articolato di condizioni materiali e istituzionali – tra cui la disponibilità, accessibilità, accettabilità e qualità dei servizi sanitari – indispensabili per una vita dignitosa.

In questa prospettiva, il diritto alla salute assume una dimensione strutturalmente relazionale, in quanto richiede agli Stati non solo obblighi negativi di non interferenza, ma anche obblighi positivi di protezione e di attuazione, che si traducono nella predisposizione di sistemi sanitari funzionanti, inclusivi e resilienti. Tali obblighi comportano la necessità di affrontare le determinanti sociali della salute e di prevenire forme dirette e indirette di discriminazione nell'accesso ai servizi, con particolare riguardo ai gruppi vulnerabili; parallelamente, nel diritto internazionale dei diritti umani si è affermata una lettura evolutiva del diritto alla salute, che ne valorizza la dimensione preventiva e sistemica, estendendone l'ambito applicativo anche ai profili organizzativi e infrastrutturali dei servizi pubblici[12].

Questa impostazione è stata progressivamente recepita anche nella giurisprudenza regionale, in particolare nell'ambito della Convenzione europea dei diritti dell'uomo, dove il diritto alla salute emerge in via mediata attraverso gli artt. 2, 3 e 8, dando luogo a un corpus di obblighi positivi in capo agli Stati in materia di tutela dell'integrità fisica e psichica delle persone e di organizzazione adeguata dei servizi sanitari. Ne risulta un quadro multilivello nel quale la salute non è più concepita come mera prestazione assistenziale, ma come diritto complesso[13], intimamente connesso alla qualità delle istituzioni pubbliche e alla capacità degli ordinamenti di governare i rischi contemporanei, inclusi quelli derivanti dalla trasformazione digitale.

In tale contesto, la sicurezza delle infrastrutture sanitarie digitali si configura sempre

[12] Cfr. P. Acconci, *Tutela della salute e diritto internazionale*, Padova, Cedam, 2011; R. Cadin, V. Zambrano, P. Acconci, I.R. Pavone et al. (a cura di), *The Day After: le Organizzazioni internazionali di fronte alle minacce globali alla salute*, in *Ordine Internazionale e diritti umani*, 2024, p. 1 ss.

[13] L'evoluzione tecnologica ha progressivamente ampliato il contenuto di tale diritto, includendo profili quali l'accesso alle informazioni sanitarie, la sicurezza dei dati clinici e la disponibilità di infrastrutture adeguate.

più come componente intrinseca del diritto alla salute, poiché l'affidabilità dei sistemi informativi, la protezione dei dati clinici e la continuità operativa delle strutture ospedaliere costituiscono condizioni essenziali per garantire cure efficaci, accessibili e non discriminatorie. La cybersicurezza entra così a pieno titolo nel perimetro degli obblighi statali di tutela dei diritti fondamentali, rafforzando l'idea che la protezione tecnologica dei servizi sanitari non rappresenti un obiettivo meramente tecnico, ma una declinazione contemporanea del dovere di garantire la dignità della persona[14].

3. *La "resilienza digitale" nel quadro normativo europeo.*

L'attuale assetto regolatorio europeo in materia di sanità digitale e cybersecurity è il risultato di un progressivo ampliamento del perimetro di intervento dell'Unione, che ha affiancato alla tradizionale tutela della riservatezza nuove esigenze di sicurezza e resilienza delle infrastrutture critiche. Se una prima fase è stata dominata dalla costruzione di un solido regime di protezione dei dati personali[15], con particolare attenzione ai dati sanitari[16], una seconda fase ha visto emergere la necessità di garantire la continuità

[14] In questo scenario, la cybersecurity emerge quale elemento di raccordo tra le diverse dimensioni della governance sanitaria digitale. Essa rappresenta, al tempo stesso, uno strumento di protezione dei diritti individuali e una componente essenziale della sicurezza collettiva, in quanto garantisce la continuità operativa delle strutture sanitarie e l'affidabilità dei dispositivi medici connessi. La sua centralità impone una rilettura del ruolo delle amministrazioni pubbliche, chiamate non soltanto a conformarsi formalmente alle prescrizioni europee, ma a integrare la sicurezza informatica nei processi decisionali, organizzativi e contrattuali.

[15] In particolare, il Regolamento (UE) 2016/679 (GDPR), Protezione dei dati personali e diritti delle persone fisiche, è il Regolamento Generale sulla Protezione dei Dati che stabilisce le norme per la protezione dei dati personali, inclusi i dati sanitari. Il regolamento va integrato con le delibere del Garante *privacy* nazionale, per esempio la n. 55 del 7 marzo 2019, «Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario».

[16] I dati personali trattati dalle strutture ospedaliere rientrano tra le categorie più sensibili dell'intero ecosistema informativo, in quanto attengono direttamente allo stato di salute, alla storia clinica e, più in generale, alla sfera più intima della persona. Essi costituiscono non soltanto informazioni ad alto valore economico nei circuiti illeciti, ma rappresentano anche elementi essenziali per la continuità delle cure e per il corretto funzionamento dei servizi sanitari. La loro compromissione può determinare conseguenze particolarmente gravi, sia sotto il profilo della riservatezza individuale, sia in termini di sicurezza dei pazienti, esponendo gli interessati a rischi di discriminazione, stigmatizzazione o uso improprio delle informazioni. È anche per tale ragione che il diritto dell'Unione qualifica i dati relativi alla salute come categoria speciale di dati personali, sottoponendoli a un regime di tutela rafforzata, e che la protezione dei

operativa dei servizi essenziali e la sicurezza dei prodotti digitali immessi sul mercato.

In tale prospettiva si colloca l'adozione della direttiva (UE) 2022/2555 (NIS2), che segna un passaggio decisivo verso un modello di cybersecurity fondato su obblighi di gestione del rischio, responsabilità degli organi di amministrazione e meccanismi rafforzati di supervisione. Rispetto alla precedente direttiva NIS[17], il nuovo testo estende in modo significativo l'ambito soggettivo di applicazione, includendo espressamente il settore sanitario tra quelli essenziali, e introduce un insieme articolato di misure tecniche e organizzative che gli enti interessati sono tenuti ad adottare.

Essa prevede il rafforzamento delle misure previste dalla Direttiva NIS, con un focus su infrastrutture critiche. Mira a eliminare le ampie divergenze tra gli Stati membri, in particolare stabilendo norme minime riguardanti il funzionamento di un quadro normativo coordinato, istituendo meccanismi per una cooperazione efficace tra le autorità responsabili in ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza e prevedendo mezzi di ricorso e misure di esecuzione effettivi che siano funzionali all'efficace applicazione di tali obblighi.

Le strutture sanitarie, i fornitori di servizi digitali e gli operatori della filiera tecnologica sono così chiamati a implementare sistemi di gestione della sicurezza, procedure di segnalazione degli incidenti e piani di continuità operativa, in un'ottica di prevenzione e resilienza. La direttiva attribuisce inoltre un ruolo centrale alle autorità nazionali competenti, chiamate a esercitare poteri di vigilanza e sanzione, rafforzando il carattere cogente degli obblighi introdotti.

A tale disciplina si affianca il regolamento sui dispositivi medici, che impone requisiti di sicurezza lungo l'intero ciclo di vita del prodotto, dalla progettazione alla messa in servizio, introducendo obblighi di valutazione del rischio e di vigilanza post-

sistemi informativi sanitari assume una valenza che travalica la dimensione patrimoniale, per collocarsi pienamente nel perimetro della tutela dei diritti fondamentali.

[17] Direttiva (UE) 2016/1148 (Direttiva NIS): Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi. Essa mirava a sviluppare le capacità di cibersicurezza in tutta l'Unione, a mitigare le minacce ai sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave e a garantire la continuità di tali servizi in caso di incidenti, contribuendo in tal modo alla sicurezza dell'Unione e al funzionamento efficace della sua economia e della sua società.

commercializzazione. In particolare, il Regolamento (UE) 2017/745 (MDR - Medical Device Regulation), disciplina l'introduzione, la sorveglianza e l'uso di dispositivi tecnologici in ambito sanitario. Questo regolamento stabilisce le norme per l'immissione sul mercato e la messa in servizio dei dispositivi medici nell'UE, inclusi i *software* e le app medicali. L'entrata in vigore del MDR è stata posticipata dapprima dal Regolamento UE 2020/561, emesso a seguito dell'epidemia Covid, e, successivamente, dal Regolamento (UE) 2023/607, che ha esteso il periodo di transizione in modo da concedere agli operatori più tempo per condurre le necessarie procedure di valutazione della conformità per i dispositivi *legacy* certificati, cioè i dispositivi immessi sul mercato dopo il 26 maggio 2021 (data di entrata in vigore del MDR)[18]. L'MDR ha ampliato notevolmente la definizione di dispositivo medico, allargando quindi il novero dei prodotti a cui si applica la nuova normativa. A ciò bisogna aggiungere il Regolamento (UE) 2017/746 (IVDR - In Vitro Diagnostic Regulation), relativo ai dispositivi medico-diagnostici in vitro. Questo regolamento definisce le norme per l'immissione sul mercato, la messa in servizio e l'utilizzo dei dispositivi medico-diagnostici in vitro. Ha diverse disposizioni in comune con il regolamento 2017/745, disponendo alcune novità relativamente alla diagnostica *in vitro*.

Con questi regolamenti l'attenzione si sposta dunque dalla mera conformità formale del dispositivo alla sua capacità di operare in modo sicuro in contesti digitali complessi, nei quali l'interconnessione rappresenta al tempo stesso un fattore di innovazione e una fonte di vulnerabilità.

Il quadro è ulteriormente completato dal Cyber Resilience Act, che mira a garantire livelli minimi di sicurezza per tutti i prodotti con elementi digitali immessi sul mercato europeo. Adottato in via definitiva a livello UE nel 2024[19], esso introduce obblighi di sicurezza informatica per i prodotti con elementi digitali (hardware e software) immessi

[18] Si rileva come il Regolamento (UE) 2017/745, ormai pienamente applicabile dal 2021, richieda che i dispositivi connessi digitalmente soddisfino requisiti essenziali di sicurezza informatica, con ricadute dirette sui processi di valutazione tecnica nelle procedure di procurement ospedaliero.

[19] Il Regolamento (UE) 2024/2847 – noto come *Cyber Resilience Act* (CRA) – è stato pubblicato nella Gazzetta Ufficiale dell'Unione ed è entrato in vigore il 10 dicembre 2024.

sul mercato dell'Unione europea e introduce criteri di *security by design*, gestione delle vulnerabilità e requisiti di conformità. Sebbene la piena applicabilità delle principali disposizioni sia fissata a partire dal 2027, l'atto normativo impone già obblighi giuridici vincolanti ai fabbricanti e agli operatori economici e avrà un impatto diretto sulle specifiche tecniche e contrattuali delle procedure di acquisto pubblico nel settore sanitario, imponendo alle amministrazioni acquirenti di prevedere nei capitolati requisiti certificati di sicurezza coerenti con gli standard europei. Tale intervento segna un ulteriore passo verso l'internalizzazione della cybersecurity nella progettazione dei prodotti, imponendo ai fabbricanti obblighi di secure-by-design e secure-by-default, nonché responsabilità estese in caso di vulnerabilità.

In tal modo, il Cyber Resilience Act si inserisce in un quadro regolatorio ormai chiaramente orientato alla costruzione di una filiera digitale sicura lungo l'intero ciclo di vita dei prodotti e dei servizi, affiancandosi alla direttiva NIS2 sul versante organizzativo e alla disciplina degli appalti pubblici su quello contrattuale. Ne emerge un modello integrato nel quale la cybersicurezza viene progressivamente anticipata alla fase di progettazione e di immissione sul mercato, per poi essere consolidata attraverso gli obblighi di gestione del rischio in capo agli enti essenziali e, infine, tradotta in requisiti tecnici vincolanti nelle procedure di acquisto. In particolare nel settore sanitario, tale interazione normativa è destinata a rafforzare il ruolo del procurement quale snodo di effettività del diritto europeo, imponendo alle amministrazioni acquirenti di operare come garanti indiretti della sicurezza dei sistemi clinico-assistenziali e, al tempo stesso, come attori della tutela sostanziale del diritto alla salute.

L'effetto combinato dei sopra citati strumenti normativi è dunque la creazione di una vera e propria costellazione regolatoria, nella quale la sicurezza informatica diviene requisito intrinseco del prodotto, del servizio e dell'organizzazione. Ciò comporta una ridefinizione delle responsabilità lungo la catena del valore, coinvolgendo produttori, fornitori, amministrazioni pubbliche e utenti finali. Per il settore sanitario, tale evoluzione implica il superamento di una visione puramente reattiva della sicurezza, fondata sulla gestione degli incidenti, a favore di un approccio preventivo e sistemico, orientato alla

resilienza.

4. *Diritto alla salute e procurement pubblico.*

All'interno della nuova architettura regolatoria delineata dal diritto dell'Unione, il procurement pubblico assume un ruolo centrale quale strumento di traduzione operativa degli obblighi di sicurezza informatica nel funzionamento quotidiano dei sistemi sanitari. Le procedure di acquisto di tecnologie digitali, dispositivi medici connessi e servizi informatici rappresentano infatti il principale punto di ingresso delle soluzioni tecnologiche nelle infrastrutture pubbliche, rendendo le stazioni appaltanti attori decisivi nella costruzione della resilienza complessiva del settore.

In tale prospettiva, il procurement non può più essere concepito come una mera attività amministrativa orientata alla selezione dell'offerta economicamente più vantaggiosa, ma si configura come un vero e proprio strumento di regolazione indiretta del mercato, attraverso il quale le amministrazioni pubbliche contribuiscono a definire standard di sicurezza, interoperabilità e protezione dei diritti fondamentali. La previsione, nei capitolati tecnici, di requisiti conformi alla direttiva NIS2, al regolamento sui dispositivi medici e al Cyber Resilience Act consente di orientare le scelte dei fornitori, incentivando pratiche di secure-by-design e rafforzando la responsabilizzazione degli operatori economici.

Il settore sanitario rende particolarmente evidente tale funzione regolatoria del procurement. L'introduzione di sistemi informativi clinici, piattaforme di telemedicina e dispositivi medicali interconnessi incide direttamente sulla qualità e sulla continuità delle prestazioni, oltre che sulla protezione dei dati personali dei pazienti. I sistemi informativi clinico-assistenziali possono esser definiti come "piattaforme digitali progettate per gestire, organizzare e archiviare i dati clinici e assistenziali dei pazienti, consentendo agli operatori sanitari di accedere e aggiornare le informazioni in modo sicuro e tempestivo". Questi sistemi supportano una serie di attività cruciali in ambito sanitario, come la

gestione delle cartelle cliniche elettroniche, il monitoraggio dei parametri vitali, la pianificazione dei trattamenti e la registrazione delle terapie somministrate. Essi non solo migliorano l'efficienza delle cure, ma promuovono anche la continuità assistenziale e l'integrazione tra i diversi attori coinvolti nel percorso di cura, garantendo una visione completa e aggiornata dello stato di salute del paziente[20].

La sicurezza informatica dei beni e dei servizi acquistati costituisce dunque una precondizione dell'effettività del diritto alla salute, in quanto condiziona la possibilità di erogare cure in modo affidabile, non discriminatorio e rispettoso della dignità della persona.

Ad esempio, particolare attenzione andrebbe riservata ai macchinari utilizzati nel sistema sanitario nazionale (ad esempio PET, TAC, RMN), che operano tramite sistemi gestiti dai fornitori e per i quali la sicurezza informatica è legata alla produzione di dati e all'interazione con uno o più client. In questi casi, le strutture ospitanti non hanno il controllo totale sulla sicurezza, poiché devono consentire l'accesso a segmenti della loro rete aziendale per consentire la manutenzione da remoto, e senza la registrazione di alcun log di tali operazioni (di manutenzione), è impossibile tracciare le attività svolte su questi macchinari (in quanto si tratta di attività criptate e non interpretabili)[21].

Le criticità di questi macchinari utilizzati nel sistema sanitario nazionale (i già citati PET, TAC, RMN) dunque, dal punto di vista del pieno controllo sulla loro sicurezza da parte dell'ente ospedaliero, sono: scarsa trasparenza nel funzionamento dei grandi macchinari; impossibilità di tracciare il percorso seguito dal fornitore per accedere ai dispositivi da manutenere; vulnerabilità che possono permettere l'accesso di malware nel sistema[22].

---

[20] Consip svolge un ruolo chiave nel processo di acquisto di sistemi informativi clinico-assistenziali, semplificando le procedure, garantendo la qualità e promuovendo l'innovazione nel settore sanitario. Le ASL, a loro volta, laddove vogliano acquistare sul mercato elettronico (il MEPA) i sistemi informativi, non devono necessariamente rivolgersi a Consip, ma sono comunque fortemente incentivate a farlo.

[21] Problematici, sotto questo aspetto della sicurezza informatica, sono anche i dispositivi portatili che comunicano tramite Wi-Fi con la rete aziendale, alimentando il sistema RIS-PACS. Anche questi dispositivi vengono manutenuti da remoto utilizzando una VPN nominativa, con un semplice codice fiscale come secondo fattore di autenticazione.

[22] Si tratta di un software dannoso creato con l'intento di infiltrarsi o danneggiare un computer o un sistema informatico senza il consenso dell'utente. Il termine malware racchiude un'ampia gamma di software

Nonostante questa centralità, le prassi nazionali mostrano come il potenziale del procurement quale leva di governance sia ancora largamente sottoutilizzato. Le procedure di gara continuano spesso a privilegiare criteri economici e prestazionali, relegando la cybersecurity a clausole generiche o a requisiti minimi, privi di un reale meccanismo di verifica. Tale approccio rischia di svuotare di contenuto le ambiziose prescrizioni europee, trasformando la sicurezza informatica in un adempimento formale piuttosto che in un elemento sostanziale della qualità del servizio sanitario.

Per colmare tale divario, appare necessario un rafforzamento delle competenze tecniche delle stazioni appaltanti, accompagnato dall'elaborazione di linee guida operative e modelli contrattuali standardizzati che integrino i requisiti di sicurezza fin dalle fasi preliminari della procedura. Solo attraverso una tale integrazione sistematica è possibile rendere il procurement uno strumento effettivo di tutela multilivello dei diritti fondamentali, capace di tradurre le norme europee in prassi amministrative coerenti.

In questa prospettiva, il procurement pubblico assume una funzione che travalica la dimensione meramente organizzativa per collocarsi pienamente nel perimetro della tutela multilivello dei diritti fondamentali, fungendo da cerniera tra obblighi europei, responsabilità statali e diritti della persona[23].

L'inserimento di requisiti tecnici vincolanti in materia di sicurezza informatica nelle procedure di gara costituisce infatti una modalità concreta attraverso cui gli standard

dannosi progettati per infiltrarsi nei sistemi informatici e arrecare danni. Tra le sue diverse forme, troviamo: Virus – Programmi in grado di replicarsi autonomamente, diffondendosi all'interno di un sistema e danneggiando file o programmi; Trojan – Mascherati da software legittimi, ingannano gli utenti per installarsi e consentire l'accesso remoto a criminali informatici; Worm – Simili ai virus, si diffondono autonomamente attraverso reti informatiche, sfruttando vulnerabilità per replicarsi e causare danni; Spyware – Progettati per monitorare le attività degli utenti e rubare informazioni sensibili, come password o dati bancari. Lo scopo del malware può essere rubare dati sensibili, disturbare il funzionamento del sistema o ottenere accesso non autorizzato per fini dannosi. Il malware, di solito, si diffonde attraverso e-mail, siti web compromessi, file scaricati da fonti non affidabili o dispositivi già infetti.

[23] Sul carattere multilivello della tutela del diritto alla salute e sui correlati obblighi positivi degli Stati cfr. art. 35 della Carta dei diritti fondamentali dell'Unione europea; art. 12 del Patto internazionale sui diritti economici, sociali e culturali; Comitato ONU sui diritti economici, sociali e culturali, General Comment No. 14 (2000). In ambito europeo, v. altresì la giurisprudenza della Corte europea dei diritti dell'uomo che, muovendo dagli artt. 2, 3 e 8 della CEDU, ha progressivamente affermato doveri positivi in capo agli Stati in ordine all'organizzazione dei servizi sanitari e alla protezione dell'integrità fisica delle persone. In dottrina v. M. Cartabia, *I diritti in azione*, Bologna, Il Mulino, 2007, p. 87 ss.

dell'Unione vengono calati nei contesti amministrativi nazionali, incidendo direttamente sulla qualità delle prestazioni sanitarie e sulla protezione dei dati personali dei pazienti. Ne deriva che eventuali carenze nella fase di progettazione e aggiudicazione dei contratti pubblici non si esauriscono in inefficienze gestionali, ma possono tradursi in violazioni sistemiche dei diritti alla salute, alla protezione dei dati e, più in generale, alla dignità della persona, così come riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, dalla Convenzione europea dei diritti dell'uomo e dagli strumenti internazionali in materia di diritti economici e sociali.

5. *Il caso italiano tra recepimento e criticità*.

È possibile individuare una serie di atti normativi, programmatici e regolamentari che compongono il quadro interno italiano relativo alla digitalizzazione della sanità, alla cybersicurezza e al procurement, con specifico riferimento all'adozione di linee guida da parte delle ASL/AO per definire una griglia di compliance. Tale quadro sembra articolarsi in cinque ambiti tematici, due di carattere più generale e tre più specifici. In materia di "sanità" il quadro istituzionale di riferimento è costituito dal D.Lgs. 502/1992 e dalla L. 228/2012 (norme fondamentali sull'organizzazione sanitaria). Su "privacy e protezione dei dati" il riferimento è il D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, che recepisce integralmente il Regolamento (UE) 2016/679 (GDPR). I tre ambiti più specifici sono, invece, "sanità digitale e digitalizzazione", con il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005), che recepisce in parte principi europei sulla digitalizzazione della PA, aggiornato da ultimo con il D.Lgs. 1/2024; il PNRR – Missione 6, che attua a livello interno la componente sanitaria del Regolamento UE 2021/241 (Recovery and Resilience Facility); il Decreto-legge 179/2012 e la L. 221/2012, che istituiscono il Fascicolo Sanitario Elettronico (FSE) in maniera coerente con i principi europei in tema di interoperabilità e *digital health*; le Linee guida per la telemedicina (D.M. 21 settembre 2022), che attuano le indicazioni del PNRR. In materia di "cybersicurezza" ricordiamo il

D.Lgs. 123/2023, che ha recepito la Direttiva (UE) 2022/2555 (NIS2) nell'ordinamento italiano[24]; la L. 133/2019 (PSNC) e il DPCM del 17.2.2017 (Gentiloni), che costituiscono gli strumenti per il perimetro di sicurezza nazionale; il D.L. 82/2021, convertito in L. 109/2021, che istituisce l'Agenzia per la Cybersicurezza Nazionale (ACN) in attuazione del Regolamento (UE) 2021/887; la L. 90/2024 e le Linee guida ACN (novembre 2024), che costituiscono un'attuazione nazionale avanzata in materia di cybersecurity. In tema di "public procurement", citiamo il D.Lgs. 50/2016 e il D.Lgs. 36/2023, che recepiscono le Direttive 2014/24/UE e 2014/25/UE sugli appalti pubblici; le Linee guida ANAC, che sono strumenti tecnici di *soft law*, dunque rilevanti, ma non vincolanti in tema di requisiti cyber[25].

Nel quadro del diritto dell'Unione europea, come è dunque evidente, l'evoluzione più significativa in tema di cybersecurity è stata rappresentata dalla Direttiva (UE) 2022/2555 (NIS2), che ha abrogato la precedente Direttiva NIS (2016/1148) e ha mirato a rafforzare la resilienza dei soggetti pubblici e privati che operano in settori critici, tra cui rientra espressamente anche il settore sanitario. La NIS2 è stata recepita in Italia con il Decreto legislativo 18 ottobre 2023, n. 123, entrato in vigore il 3 dicembre 2023. Il decreto attribuisce obblighi specifici anche alle strutture sanitarie pubbliche, imponendo misure tecniche e organizzative adeguate alla gestione dei rischi cyber, con particolare attenzione ai processi di approvvigionamento digitale (art. 18, d.lgs. 123/2023). Tale recepimento, tuttavia, presenta alcune criticità di coordinamento normativo rispetto alla normativa settoriale italiana sul procurement sanitario. Manca infatti, ad oggi, una disciplina organica che colleghi espressamente i requisiti di cybersecurity ai procedimenti di gara e acquisto nel settore sanitario, benché alcuni strumenti settoriali si stiano sviluppando in tale direzione. Tra questi si segnalano: le Linee Guida AGID (Agenzia per l'Italia

[24] V. il D.Lgs. 123/2023 di recepimento della Direttiva (UE) 2022/2555 (*NIS2*), Agenzia per la Cybersicurezza Nazionale (i documenti e le linee guida attuative sono disponibili sul relativo sito istituzionale).

[25] Tali strumenti, in quanto atti non vincolanti, pur rivestendo un'indubbia funzione orientativa per le stazioni appaltanti, non introducono requisiti tecnici cogenti in materia di cybersicurezza e non colmano, allo stato, le lacune regolatorie relative alla definizione di standard minimi obbligatori per il procurement sanitario digitale.

Digitale) in materia di sicurezza ICT per le pubbliche amministrazioni, applicabili anche agli enti del SSN; i capitolati tipo predisposti da CONSIP e dalle centrali di committenza regionale, che iniziano a includere clausole minime di sicurezza per la fornitura di soluzioni ICT; il Piano triennale per l'informatica nella Pubblica Amministrazione (2024–2026), che individua la sanità digitale come ambito prioritario di intervento, pur senza offrire ancora una griglia vincolante di compliance per il procurement[26].

L'ordinamento italiano ha dunque recepito la direttiva NIS2 mediante un complesso di interventi normativi e organizzativi che hanno attribuito un ruolo centrale all'Agenzia per la cybersicurezza nazionale, chiamata a coordinare il sistema di prevenzione, gestione e risposta agli incidenti informatici. Parallelamente, sono stati avviati processi di adeguamento delle amministrazioni sanitarie, con l'introduzione di obblighi di valutazione del rischio, di segnalazione degli incidenti e di adozione di misure tecniche e organizzative proporzionate.

Sotto il profilo formale, il recepimento appare in linea con le prescrizioni europee. Nel complesso, dunque, possiamo affermare che il recepimento delle fonti europee in materia di cybersecurity nel settore sanitario è in linea di principio avviato, ma ancora frammentario quanto all'effettiva trasposizione in atti vincolanti che disciplinino le fasi di approvvigionamento in modo unitario. Si evidenzia – di conseguenza – la necessità di adottare linee guida ministeriali specifiche per le aziende sanitarie; rafforzare il coordinamento tra normativa sulla cybersecurity e Codice dei contratti pubblici (d.lgs. 36/2023); garantire un sistema di auditing e monitoraggio della

[26] Per quanto riguarda gli strumenti nazionali di indirizzo tecnico, dunque, v. AGID, *Linee guida in materia di sicurezza ICT per le pubbliche amministrazioni*, nonché il *Piano triennale per l'informatica nella Pubblica Amministrazione 2024–2026*, adottato ai sensi dell'art. 14-bis del Codice dell'amministrazione digitale. Sul ruolo di Consip e delle centrali di committenza regionali nella progressiva integrazione di requisiti di sicurezza informatica negli strumenti di acquisto pubblico, in particolare attraverso accordi quadro, sistemi dinamici di acquisizione (SDAPA) e capitolati per servizi ICT, cloud e sistemi informativi, v. Consip S.p.A., *Programma di razionalizzazione degli acquisti nella PA* e relativa documentazione tecnica disponibile sul sito istituzionale (https://www.consip.it/chi-siamo/attività/programma-acquisti). In prospettiva europea, cfr. Commissione europea, *Public Procurement for Data-Driven Innovation*, Bruxelles, 2022, nonché Commissione europea, *Guidance on Secure Public Procurement in the Digital Sector*, 2023. Tali strumenti contribuiscono alla diffusione di clausole minime di sicurezza, ma conservano prevalentemente natura di indirizzo operativo e non configurano ancora un quadro vincolante e uniforme di requisiti cyber per il procurement sanitario.

compliance nelle procedure di acquisto, in coerenza con le previsioni della NIS2.

Un'analisi attenta delle dinamiche attuative evidenzia quindi la persistenza di significative criticità strutturali. In primo luogo, emerge una marcata eterogeneità territoriale nella capacità delle aziende sanitarie di conformarsi ai nuovi standard, dovuta a carenze di risorse finanziarie, competenze specialistiche e infrastrutture tecnologiche. Tale disomogeneità rischia di tradursi in una tutela diseguale del diritto alla salute, in contrasto con il principio di universalità che informa il servizio sanitario nazionale.
A ciò si aggiunge una frammentazione delle responsabilità tra livello centrale e livelli regionali, che rende complessa la costruzione di una governance unitaria della sanità digitale. La pluralità degli attori coinvolti – ministeri, agenzie, regioni, aziende sanitarie – rende difficile l'adozione di strategie coordinate, favorendo approcci settoriali e soluzioni emergenziali piuttosto che politiche strutturali di lungo periodo.

Il procurement pubblico riflette in modo emblematico tali difficoltà. L'assenza di strumenti operativi condivisi e di un supporto tecnico sistematico alle stazioni appaltanti limita la capacità delle amministrazioni di integrare efficacemente i requisiti di cybersecurity nelle procedure di gara. Ne deriva un rischio di scollamento tra l'armonizzazione legislativa e la protezione sostanziale dei sistemi sanitari, con conseguenze potenzialmente rilevanti in termini di esposizione al rischio cibernetico.

Queste criticità mettono in luce la necessità di un approccio integrato, che combini interventi normativi, formazione del personale, investimenti infrastrutturali e cooperazione interistituzionale. Solo attraverso una tale strategia è possibile colmare il divario tra recepimento formale e implementazione effettiva, trasformando la cybersecurity in una componente strutturale dell'organizzazione sanitaria.

6. *La cybersecurity come precondizione del diritto alla salute.*

Nonostante i progressi, dunque, la sanità digitale in Europa e in Italia si scontra con alcune sfide: interoperabilità dei processi; sicurezza dei dati; alfabetizzazione digitale;

disuguaglianze digitali. A fronte di tali sfide è essenziale superare il divario tra chi ha accesso alle tecnologie e chi ne è escluso. D'altro canto però le opportunità offerte dalla sanità digitale per il miglioramento del sistema sanitario sono numerose: maggiore accesso alle cure (la telemedicina facilita l'assistenza per chi vive in zone remote o ha difficoltà di mobilità); miglioramento della qualità delle cure (le tecnologie digitali supportano diagnosi, prevenzione e trattamenti più accurati); incremento dell'efficienza (la digitalizzazione dei processi riduce i costi e ottimizza l'operatività del sistema); partecipazione attiva dei cittadini (le tecnologie digitali possono coinvolgere i cittadini nella gestione della propria salute)[27].

Il livello di recepimento della normativa europea risulta nel complesso soddisfacente sotto il profilo formale, in quanto le principali direttive e regolamenti UE in materia di digitalizzazione, cybersecurity e appalti sono stati integrati nella legislazione nazionale. Tuttavia, si riscontrano ancora carenze sul piano attuativo e sistemico, in particolare per quanto riguarda: l'armonizzazione tra normative settoriali (sanitarie) e generali (appalti, sicurezza ICT); l'adozione vincolante di griglie minime di compliance per le ASL/AO nella fase di procurement; la traduzione delle strategie e linee guida in strumenti operativi obbligatori. La definizione di Linee guida nazionali vincolanti per il procurement in ambito sanitario, contenenti requisiti minimi di sicurezza informatica coerenti con la direttiva NIS2 e con la Strategia nazionale di cybersicurezza, rimane un obiettivo prioritario per colmare il divario tra recepimento normativo e implementazione effettiva[28]. Pur essendo state pubblicate varie linee guida tecniche e documenti di

[27] In tutto ciò, Consip S.p.A. gioca un ruolo centrale nell'acquisto di sistemi informativi clinico-assistenziali per le pubbliche Amministrazioni del Servizio Sanitario Nazionale (SSN) in Italia.

[28] Esistono solo strumenti parziali, complementari o non vincolanti, tra cui: capitolati tecnici e bandi-tipo predisposti da Consip o centrali regionali di acquisto, che iniziano a incorporare clausole sulla sicurezza informatica, ma senza obbligatorietà generale né standardizzazione nazionale; linee Guida AgID sulla sicurezza ICT per la PA (rilevanti anche per le ASL/AO, ma non specifiche per il procurement sanitario e non vincolanti nel settore sanitario, che dipende dal Ministero della Salute); linee guida ANAC generali sugli appalti e sulle forniture ICT, che possono essere utilizzate in ambito sanitario, ma non contengono una "griglia minima" dedicata alla compliance cyber; linee Guida ACN (novembre 2024) adottate dopo l'entrata in vigore della L. 28 giugno 2024, n. 90, che contengono indicazioni rilevanti per gli operatori critici in materia di rafforzamento della resilienza cyber, ma ancora non calate nel contesto del procurement sanitario: il Piano Triennale per l'Informatica nella PA (2024–2026), che dedica una sezione alla sanità digitale, ma non definisce standard cogenti per il procurement.

indirizzo, tali strumenti conservano in gran parte una natura raccomandatoria e non vincolante, e non esiste ancora una matrice obbligatoria di criteri tecnici e contrattuali uniformemente applicata alle stazioni appaltanti del settore[29].

L'analisi svolta consente di affermare che la cybersecurity non costituisce più un ambito accessorio della sanità digitale, ma ne rappresenta una componente strutturale. La protezione delle infrastrutture informative sanitarie incide infatti direttamente sulla possibilità per gli individui di accedere alle cure, sulla qualità e continuità delle prestazioni, nonché sul livello di fiducia riposto nei servizi pubblici, assumendo una rilevanza che travalica la dimensione puramente tecnica per collocarsi pienamente nel perimetro dei diritti fondamentali.

In questa prospettiva, le amministrazioni sanitarie sono chiamate ad assumere una responsabilità rafforzata, che non si esaurisce nel rispetto formale delle prescrizioni normative, ma si estende alla garanzia sostanziale dei diritti della persona. Il principio di buona amministrazione si declina oggi anche come dovere di progettare, acquisire e gestire tecnologie sicure, resilienti e rispettose della dignità umana, integrando la cybersicurezza nei processi decisionali, organizzativi e contrattuali. Ne deriva che il procurement pubblico, lungi dall'essere un mero strumento tecnico, diviene uno snodo essenziale di attuazione degli obblighi positivi dello Stato in materia di tutela della salute e di protezione dei dati personali.

Il diritto dell'Unione europea offre ormai un quadro articolato di strumenti normativi – dalla NIS2 al Cyber Resilience Act, fino alla disciplina dei dispositivi medici e degli appalti pubblici – idonei a sostenere questa trasformazione. Tuttavia, l'effettività di tale architettura dipende in misura decisiva dalla capacità degli Stati membri di tradurla in prassi amministrative coerenti e coordinate. L'esperienza italiana mostra come questo percorso sia ancora in fase di consolidamento, richiedendo un impegno costante sul piano

[29] Per un quadro delle principali iniziative tecniche nazionali v. Agenzia per la cybersicurezza nazionale, *Strategia nazionale di cybersicurezza 2022–2026*; AGID, *Linee guida in materia di sicurezza ICT*; Ministero della Salute e CNIPA, documenti di best practice sulla protezione dei sistemi informativi sanitari. Queste fonti contengono orientamenti e criteri, ma non costituiscono strumenti vincolanti di compliance nel procurement sanitario.

istituzionale, tecnico e culturale, nonché un rafforzamento delle competenze delle stazioni appaltanti e dei soggetti coinvolti nella governance della sanità digitale[30].

In ultima analisi, la sicurezza informatica dei sistemi sanitari non può essere ridotta a una questione di resilienza tecnologica: essa costituisce un elemento costitutivo della cittadinanza digitale europea e contribuisce a ridefinire il contenuto contemporaneo del diritto alla salute, inserendolo in una dimensione multilivello nella quale interoperano diritto dell'Unione, ordinamenti nazionali e standard internazionali di tutela dei diritti umani. È in questo spazio giuridico integrato che la cybersicurezza si afferma come precondizione dell'effettività del diritto alle cure, quale espressione attuale del dovere pubblico di protezione della dignità della persona nell'era della trasformazione digitale.

[30] Cfr. M. D'Arienzo, *La trasformazione digitale della sanità tra problemi organizzativi e profili di responsabilità professionale*, in "Il diritto dell'economia", 2, 2022, p. 135 ss.; D.U. Galetta, *Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono*, in "Federalismi.it", 12, 2023, p. 4 ss.; N. Posteraro, *Sanità digitale, Fascicolo Sanitario Elettronico e PNRR,* in "Sanità Pubblica e Privata", 2, 2023, p. 19 ss.; U. Ruffolo, *L'Intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento"*, in "Giurisprudenza italiana", 2, 2021, p. 502 ss.; F. Valentini, *La sanità digitale tra regolazione, organizzazione amministrativa e azione terapeutica*, in "Munus", 2, 2023, p. 449 ss.; L. Abba, A. Lazzaroni, M. Pietrangelo (a cura di), *La Internet governance e le sfide della trasformazione digitale*, Napoli, Editoriale Scientifica, 2022.