Essays

Cibersicurezza e dispositivi medici: la tutela della salute e della sicurezza dei pazienti dalle vulnerabilità informatiche nel Regolamento (UE) 2017/745 e nell'*Artificial Intelligence Act*

Elena Scalcon*

CYBERSECURITY AND MEDICAL DEVICES: THE PROTECTION OF PATIENTS' HEALTH AND SAFETY FROM CYBER VULNERABILITIES IN REGULATION (EU) 2017/745 AND ARTIFICIAL INTELLIGENCE ACT

ABSTRACT: Cybersecurity is an increasingly crucial issue with healthcare, especially due to the sector's growing digitization and the rise of cyber threats that endanger the protection of personal data and, more generally, the health and physical integrity of patients. This paper focuses on a circumscribed aspect, namely the cybersecurity of medical devices, viewed as an essential component within the broader issue of cyber resilience in the healthcare sector. The analysis starts with Regulation (EU) 2017/745 on medical devices, aiming to clarify the defining aspects and, especially, the meaning of the term software, which allows to include AI-based products within its scope. Indeed, the definition and classification of medical devices represent crucial elements to determine the applicability or not to the specific device not only of the sectoral legislation, but also of the Artificial Intelligence Act. Finally, the contribution will focus on the measures aimed at ensuring the cybersecurity of medical devices, starting with those established in Regulation (EU) 2017/745, and ending with an examination of the novelties introduced by the AI Act.

KEYWORDS: Cybersecurity; medical devices; AI-based medical devices; protection of patients' health and safety; artificial intelligence

ABSTRACT: La cibersicurezza è una questione sempre più centrale in ambito sanitario, soprattutto a fronte della crescente digitalizzazione del settore e dell'incremento delle minacce informatiche a danno della tutela dei dati personali e, più in generale, della salute e integrità fisica dei pazienti. Il presente contributo si focalizza su un profilo circoscritto, ovvero la cibersicurezza dei dispositivi medici, quale parte integrante del più ampio tema della resilienza informatica del settore sanitario. L'analisi prende avvio dal Regolamento (UE) 2017/745 sui dispositivi medici, al fine di chiarire gli aspetti definitori e, in particolar modo, il significato del termine *software,* che consente di estendere il campo di applicazione anche ai prodotti *AI-based.* La definizione di dispositivo medico e la relativa classificazione rappresentano, infatti, elementi cruciali per determinare l'applicabilità o meno allo specifico *device* non solo della legislazione di settore,

* *Dottoranda in Diritto costituzionale, Università degli studi di Modena e Reggio Emilia e Università di Parma. Mail: elena.scalcon@unipr.it.* *Contributo sottoposto a doppio referaggio anonimo.*

Essays

ma anche – come si vedrà – dall'*Artificial Intelligence Act.* Infine, il contributo si concentrerà sulle misure a garanzia della cibersicurezza dei dispositivi medici, partendo da quelle stabilite nel Regolamento (UE) 2017/745, fino ad esaminare le novità introdotte dall'*AI Act.*

PAROLE CHIAVE: Cibersicurezza; dispositivi medici; dispositivi medici *AI-based;* tutela della salute e sicurezza dei pazienti; intelligenza artificiale

1. Introduzione. La cibersicurezza nel settore sanitario

L'impiego sempre più massiccio di tecnologie digitali e la crescente digitalizzazione permeano oramai molteplici ambiti della nostra vita quotidiana[1], portando con sé innumerevoli benefici e opportunità prima impensabili ma anche nuove sfide sul piano etico e giuridico. Da questo fenomeno non è esente nemmeno il settore sanitario che per sua natura costituisce terreno d'elezione dell'innovazione scientifica e tecnologica.

L'introduzione del fascicolo sanitario elettronico, la telemedicina, l'implementazione di sistemi informatici per la gestione delle strutture sanitarie, così come di robot chirurgici, di farmaci digitali, di *wearable* per il rilevamento di diversi parametri o il monitoraggio a distanza, e di *software* creati per supportare il medico nella decisione terapeutica sono soltanto alcuni esempi di come, negli ultimi decenni, gli orizzonti della sanità abbiano subito un notevole ampliamento grazie a soluzioni digitali sempre più sofisticate e performanti, il cui fine ultimo – pur a fronte delle rispettive caratteristiche e peculiarità – è rappresentato dalla cura e dal benessere del paziente. Il processo di trasformazione in corso verso la salute digitale è, infatti, frutto della commistione tra la diffusione della rete Internet, le *Information*

[1] Basti pensare che nell'ambito del *Next Generation EU* (NGEU) – il piano di ripresa messo in campo dall'Unione Europea a seguito della crisi pandemica – la transizione digitale costituisce uno degli obiettivi centrali, assieme alla sostenibilità ambientale, a cui sono indirizzati ingenti finanziamenti. La maggior parte dei fondi del NGEU, per una quota che ammonta a circa 723,8 miliardi di euro (dei 806,9 miliardi totali), verrà impiegata nel programma *Recovery and Resilience Facility* (RRF) che prevede tra le sue azioni anche il sostegno finanziario alla digitalizzazione e alla promozione dell'innovazione tecnologica. Per maggiori dettagli si veda https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/2021-2027/whats-new_en. A livello nazionale, il *Piano Nazionale di Ripresa e Resilienza* (PNRR) dedica particolare attenzione alla promozione della trasformazione digitale dell'Italia, come si evince chiaramente dalle missioni e dalle relative componenti in cui è articolato. Oltre a riservare espressamente al tema una delle sue missioni (la Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura"), l'impegno per l'innovazione e digitalizzazione dei settori chiave del Paese assume in realtà carattere trasversale e rappresenta una sorta di filo rosso che accomuna tutte le linee programmatiche del PNRR (vedi *Piano Nazionale di Ripresa e Resilienza – Italia domani*, https://www.italiadomani.gov.it/it/strumenti/documenti/archivio-documenti/piano-nazionale-di-ripresa-e-resilienza.html, 87).

and Communication Technologies (ICTs), l'*Internet of Things* (IoT) o meglio l'*Internet of Medical Things* (IoMT), l'Intelligenza Artificiale (IA) e i *big data* a tutela della salute in senso lato[2].

[2] Come sottolineato a più riprese dalla *World Health Organization*, il termine *digital health* comprende al suo interno un ampio spettro di tecnologie digitali per la salute, dove accanto all'*eHealth* (o sanità elettronica) – che si riferisce a «the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research» (cfr. WHA58.28 eHealth), così come alla *mHealth* ovvero «[t]he use of mobile wireless technologies for public health» – si collocano «developing areas such as the use of advanced computing sciences (in the fields of "big data", genomics and artificial intelligence, for example)» (così REPORT BY THE DIRECTOR-GENERAL, *mHealth. Use of appropriate digital technologies for public health,* 26 marzo 2018, punto 2; e anche WORLD HEALTH ORGANIZATION, *WHO guideline: recommendations on digital interventions for health system strengthening,* 2019, ix). Concentrandosi sul livello europeo, è a partire dall'adozione del primo piano d'azione per la sanità elettronica nel 2004 che si registra il crescente impegno delle istituzioni allo sviluppo e alla promozione negli Stati membri della digitalizzazione dei sistemi sanitari. Come specificato nella Comunicazione della Commissione europea, «gli strumenti e le soluzioni offerte dalla sanità elettronica comprendono prodotti, sistemi e servizi che vanno al di là delle semplici applicazioni Internet. Si tratta sia di strumenti destinati alle autorità e agli operatori del settore sanitario che di sistemi sanitari personalizzati per i pazienti e i cittadini. A titolo di esempio si citino le reti di informazione sanitaria, le cartelle cliniche elettroniche, i servizi di telemedicina, i sistemi di comunicazione personali portatili e indossabili, i portali salute e molti altri strumenti basati sulle tecnologie della comunicazione e dell'informazione e utilizzati per la prevenzione, la diagnosi, la cura, la sorveglianza sanitaria e la gestione dello stile di vita» (così *Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica,* COM(2004)356, 4). A questo primo sforzo a favore della sanità elettronica sono seguite numerose iniziative della Commissione europea tra cui spicca il *Piano d'azione "Sanità elettronica" 2012-2020 – Una sanità innovativa per il 21esimo secolo* (COM(2012)736), dove si sottolinea come l'*eHealth* sia «finalizzat[a] a un miglioramento della salute dei cittadini, dell'efficienza e della produttività in ambito sanitario, nonché a un maggiore valore economico e sociale della salute» (*ivi,* 4)», o ancora la *Comunicazione relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana* (COM(2018)233); nonché *policies* più settoriali che riguardano nello specifico l'assistenza sanitaria transfrontaliera – soprattutto in relazione ad alcuni profili innovativi in tema di sanità elettronica – (Direttiva 2011/24/UE); la telemedicina (*Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale europeo e al Comitato delle Regioni sulla telemedicina a beneficio dei pazienti, dei sistemi sanitari e della società*,COM(2008)689); la c.d. salute mobile o *mHealth* (*Libro verde sulla salute mobile,* COM(2014)219) e i dati sanitari (oltre al Regolamento (UE) 679/2016, meglio noto come GDPR, si vedano la *Comunicazione "Verso uno spazio comune europeo dei dati",* COM(2018)232; la *Comunicazione relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana,* COM(2018)233 e *Una strategia europea per i dati,* COM(2020)66 che ha posto le basi per l'adozione di diverse proposte aventi come obiettivo una più ampia e sicura condivisione dei dati tra cui rientrano il *Data Act* (COM(2022)68), lo *European Health Data Space* (COM(2022)197) e il *Data Governance Act* (Regolamento (UE) 2022/868), entrato in vigore il 23 giugno 2022). Da ultimo, l'interesse per la sanità digitale emerge chiaramente dal quarto programma dell'Unione europea dedicato alla salute – il c.d. *Programma UE per la salute 2021-2027 – EU4Health* – istituito dal Regolamento (UE) 2021/522 come risposta e soluzione alla fragilità dei sistemi sanitari nazionali messa in evidenza dalla pandemia da Covid-19. Tra i suoi "obiettivi specifici" rientra anche quello di «rafforzare l'uso e il riutilizzo dei dati sanitari per la prestazione di assistenza sanitaria e per la ricerca e l'innovazione, promuovere la diffusione di strumenti e servizi digitali, nonché la trasformazione digitale dei sistemi sanitari, anche sostenendo la creazione di uno spazio europeo dei dati sanitari» (art. 4, lett. f), tramite le azioni delineate nell'Allegato I, par. 6, dove si fa espressa menzione anche all'intelligenza artificiale. Anche nel *Programma strategico per il decennio digitale 2030,* istituito con Decisione (UE) 2022/2481 al fine di promuovere l'innovazione tecnologica e gli investimenti nell'Unione europea si parla di digitalizzazione della sanità. In particolare, tra le finalità generali del programma vi rientra anche garantire che «i servizi pubblici e i servizi sanitari e di assistenza siano accessibili a tutti nel quadro di un ambiente online fidato e sicuro, in particolare ai gruppi

La transizione dal mondo analogico a quello digitale in sanità non è però priva di ostacoli, e anzi si imbatte in inedite questioni connaturate alle tecnologie in uso che riguardano la *privacy* e la tutela dei dati sanitari, le ripercussioni sul principio del consenso informato e sull'autonomia decisionale dei pazienti e dei medici, l'impatto sulla relazione terapeutica, il rischio di deresponsabilizzazione e di *deskilling* dei professionisti della salute, fino all'inclusività e completezza dei dati e al pericolo di riprodurre e perpetrare su larga scala discriminazioni esistenti, così come le potenziali disparità dovute al *digital divide,* l'affidabilità delle decisioni algoritmiche e il problema della *black box*[3]. Questi sono soltanto alcuni dei profili conflittuali delle nuove tecnologie rispetto ai principi cardine che governano l'etica biomedica – quali il principio di beneficenza, di non maleficenza, di autonomia e di giustizia – e a beni di assoluta rilevanza costituzionale quali l'eguaglianza, la dignità umana, la protezione dei dati personali e della riservatezza, la salute e l'autodeterminazione terapeutica.

Le enormi potenzialità offerte dalle tecnologie digitali emergenti nel campo della salute soprattutto in termini di maggior efficienza e accessibilità dell'assistenza sanitaria, nonché del miglioramento del processo di cura dei pazienti, scontano però un ulteriore prezzo importante, quello della propria intrinseca fragilità alle minacce informatiche, ovvero la possibilità che possano venire volontariamente compromesse sfruttando le falle o comunque aggirando le misure di cibersicurezza in atto. Questo si può riverberare negativamente non solo sul singolo strumento o servizio interessato dall'attacco informatico, ma anche sull'intera infrastruttura colpita – che si tratti di un ospedale, di una clinica privata, di un istituto di ricerca oppure di un'azienda farmaceutica o produttrice di dispositivi medici –, con conseguenze dannose non solo rispetto alla protezione e tutela dei dati personali ma anche sulla salute dei pazienti, causando lesioni (più o meno dirette) alla loro integrità fisica o addirittura mettendone a

svantaggiati, comprese le persone con disabilità, e in zone rurali e remote, offrendo servizi e strumenti inclusivi, efficienti, interoperabili e personalizzati con standard elevati in materia di sicurezza e privacy» (art. 3, lett. g). Per un approfondimento sulle politiche europee in materia di salute digitale si rimanda a EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *eHealth – Technology for health*, marzo 2015; C. BOTRUGNO, *Information and Communication Technologies in Healthcare: A New Geography of Right to Health,* in *Rivista di filosofia del diritto,* 1, 2021, 164 ss.; G. DI FEDERICO, S. NEGRI, *Unione europea e salute. Principi, azioni, diritti e sicurezza,* Milano, 2019, 215 ss.

[3] Per una panoramica dei rischi correlati all'utilizzo di tecnologie digitali – e in particolare dell'Intelligenza Artificiale – in medicina e delle conseguenti implicazioni sul piano etico e giuridico si vedano, *ex multis,* EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *eHealth – Technology for health*, marzo 2015, 5-6; COMITATO NAZIONALE PER LA BIOETICA, COMITATO NAZIONALE PER LA BIOSICUREZZA E LE BIOTECNOLOGIE E LE SCIENZE DELLA VITA, *Intelligenza artificiale e medicina: aspetti etici,* 29 maggio 2020; S. GERKE, T. MINSSEN, G. COHEN, *Ethical and legal challenges of artificial intelligence-driven healthcare,* in A. BOHR, K. MEMARZADEH (a cura di), *Artificial Intelligence in Healthcare,* Cambridge (MA), 2020; D. CHIAPPINI, *Legal and ethics state-of-the-art of artificial intelligence in medicine,* in *Diritto e Processo,* 2020, 120 ss.; WORLD HEALTH ORGANIZATION, *Ethics and Governance of Artificial Intelligence for Health: WHO guidance,* 2021, 31 ss.; EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *The rise of digital health technologies during the pandemic,* aprile 2021, 8-9; EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Artificial intelligence in healthcare. Applications, risks and ethical and societal impacts,* giugno 2022, 15 ss.; GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale,* settembre 2023.

repentaglio la vita[4]; nonché più in generale sulla fiducia dei cittadini nei confronti dell'utilizzo di tecnologie digitali, così come verso l'intero sistema sanitario e le istituzioni[5].

Purtroppo, non si tratta di ipotesi "di scuola" dal momento che la sanità rientra tra i settori maggiormente colpiti da *cyberattacks* e continua a registrare, anno dopo anno, un considerevole incremento delle incursioni da parte di *hacker*[6]. Tale fenomeno è dovuto a una molteplicità di fattori concorrenti.

[4] Nell'incipit di un recente Report della ENISA – l'Agenzia dell'Unione europea per la cibersicurezza – viene detto chiaramente che «[a]n attack directed at a critical infrastructure, such as a hospital, can lead to physical damages and put the lives of patients at risk» (così EUROPEAN UNION AGENCY FOR CYBERSECURITY, *CSIRT capabilities in healthcare sector. Status and Development,* novembre 2021, 3). La medesima preoccupazione è condivisa anche dalla *U.S. Food and Drug Administration,* secondo cui «cybersecurity threats to the healthcare sector have become more frequent and more severe, carrying increased potential for clinical impact. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the U.S. and globally. Such cyber attacks and exploits may lead to patient harm as a result of clinical hazards, such as delay in diagnoses and/or treatment» (U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, FOOD AND DRUG ADMINISTRATION, CENTER FOR DEVICES AND RADIOLOGICAL HEALTH, CENTER FOR BIOLOGICS EVALUATION AND RESEARCH, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. Guidance for Industry and Food and Drug Administration Staff*, 27 settembre 2023, https://www.fda.gov/media/119933/download, 1). Un simile scenario si è peraltro già presentato nella realtà. Infatti, a seguito di un *ransomware* ai danni di un ospedale di Düsseldorf, avvenuto nel settembre del 2020, e al ritardato accesso alle cure per una paziente e al suo decesso, vi è stato il tentativo (non riuscito) di incriminare gli *hacker* per omicidio e di stabilire il nesso causale tra la morte della paziente e l'attacco informatico. Come evidenziato in EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Artificial intelligence in healthcare,* cit., 25, «[a]lthough it was later argued that it could not be proven that the death was directly caused by the cyberattack, because the patient was already suffering a life-threatening condition, this case brought to the forefront the real physical harms that cyberattacks can cause in the healthcare sphere». La vicenda è stato oggetto di attenzione da parte di diversi siti d'informazione: M. KIENER, '*You may be hacked' and other things doctors should tell you,* in *The Conversation,* 3 November 2020, https://theconversation.com/you-may-be-hacked-and-other-things-doctors-should-tell-you-148946; *Prosecutors open homicide case after cyber-attack on German hospital,* in *The Guardian,* 18 settembre 2020, https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital; M. EDDY, N. PERLROTH, *Cyber Attack Suspected in German Woman's Death,* in *The New York Times,* 18 settembre 2020, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html; W. RALSTON, *The untold story of a cyberattack, a hospital and a dying woman,* in *Wired,* 11 novembre 2020, https://www.wired.co.uk/article/ransomware-hospital-death-germany.

[5] Così E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* in *arXiv,* 6 marzo 2023, https://arxiv.org/abs/2303.03140v1, 1; E. BIASIN, B. YAŞAR, E. KAMENJAŠEVIĆ, *New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act,* in *Law, Technology and Humans,* 5, 2, 2023, 43; K.R. LUDVIGSEN, *The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions,* in *Law, Technology and Humans,* 5, 2, 2023, 59-61. Per maggiori dettagli sulla portata e sulle tipologie di incidenti, sui soggetti maggiormente colpiti all'interno del settore sanitario e sull'impatto sulle persone coinvolte si vedano i dati raccolti ed elaborati dal *Cyber Peace Institute,* consultabili al seguente indirizzo: https://cit.cyberpeaceinstitute.org/explore.

[6] Come evidenziato da un recente studio, nel corso del 2022 «[a]ttacks on the healthcare sector registered the highest surge, 74% more attacks than last year, placing it as the third most targeted industry in this index. From hospitals and clinics to research facilities, attackers have been focusing on the healthcare industry since the beginning of the COVID-19 pandemic, seeking financial gain. 89% of healthcare organizations reported cyberattacks within the last year with an average total cost reaching $4.4M» (CHECK POINT RESEARCH, *2023 Cyber Security Report,* consultabile al seguente indirizzo: https://resources.checkpoint.com/report/2023-check-point-cyber-security-report, 48 ss.; così anche EUROPEAN UNION AGENCY FOR CYBERSECURITY, *CSIRT capabilities in healthcare sector. Status and Development,* cit., 6; e più diffusamente sul tema EUROPEAN UNION AGENCY FOR CYBERSECURITY, *ENISA Threat Landscape: Health Sector,* giugno 2023, https://www.enisa.europa.eu/publications/health-threat-landscape).

Da un lato, infatti, soprattutto a partire dalla pandemia da Covid-19 la rivoluzione digitale ha travolto l'intero comparto sanitario che sempre più si affida a soluzioni tecnologiche *smart* e connesse nello svolgimento delle proprie attività, da quelle strettamente cliniche o di ricerca fino a quelle amministrative e organizzative, con la conseguenza di esporsi al rischio di incursioni esterne e ostili[7]. Dall'altro lato, la digitalizzazione della sanità ha come immediato effetto la creazione di esponenziali quantità di dati, considerati particolarmente preziosi e di valore per la criminalità informatica perché permettono di ricavare informazioni relative alla salute dei pazienti (come il gruppo sanguigno, gli esiti di accertamenti diagnostici, le operazioni chirurgiche svolte, le informazioni genetiche, …), così come altri dati di carattere personale[8]. A muovere gli *hacker* sono prevalentemente motivazioni economiche dal momento che i dati illegalmente ottenuti possono essere venduti nel *dark web* con ingenti ricavi oppure essere oggetto di azioni estorsive (*ransomware*), ma anche altre ragioni come il furto d'identità o il loro utilizzo per effettuare frodi assicurative[9]. A ciò si aggiunge che la qualità delle infrastrutture IT

[7] Per usare le parole del considerando 3 del Regolamento sulla cibersicurezza (*Regolmento (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, e che abroga il regolamento (UE) n. 526/2013*): «[l]'incremento della digitalizzazione e della connettività comporta maggiori rischi connessi alla cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori». Sullo stretto rapporto tra salute digitale e aumento dei rischi per la cibersicurezza si vedano, *ex multis,* E. Frumento, *Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution,* in G. Andreoni, P. Perego, E. Frumento (a cura di), *m_Helath Current and Future Applications,* Cham, 2019, 35 ss.; S. Gerke, T. Minssen, G. Cohen, *Ethical and legal challenges of artificial intelligence-driven healthcare,* cit., 323 ss.; European Parliamentary Research Service, *The rise of digital health technologies during the pandemic,* cit., in particolare 8-9; European Union Agency for Cybersecurity, *CSIRT capabilities in healthcare sector. Status and Development,* cit., 3; World Health Organization, *Ethics and Governance of Artificial Intelligence for Health*, cit., 58; E. Biasin, E. Kamenjašević, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals*, in *International Cybersecurity Law Review*, 3, 2022, 164; U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Center for Biologics Evaluation and Research, *Cybersecurity in Medical Devices,* cit., 1; E. Biasin, E. Kamenjašević, K.R. Ludvigsen, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 2-3; A.J. Cartwright, *The elephant in the room: cybersecurity in healthcare,* in *Journal of Clinical Monitoring and Computing,* 37, 2023, 1123 ss.

[8] Secondo quanto riportato da una ricerca condotta dalla International Data Corporation (IDC), si stima che «the Global Datasphere will grow from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025» e, tra i settori considerati, si prevede che quello sanitario registrerà la crescita maggiore con un incremento del 36% entro il 2025, di 6 punti percentuali superiore al settore manifatturiero, di 10 rispetto a quello finanziario e di 11 a quello dei media e dell'intrattenimento (vedi D. Reinsel, J. Gantz, J. Rydning, *The Digitization of the World. From Edge to Core,* novembre 2018, consultabile al seguente indirizzo: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf, rispettivamente 3 e 22).

[9] In S.T. Argaw, J.R. Troncoso-Pastoriza, D. Lacey *et al., Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks,* in *BMC Medical Informatics and Decision Making,* 20, 146, 2020, 2, si sottolinea come la «[c]ybersecurity in the health field is unique due to the type of information at risk and the consequences for patient safety. When a credit card number is stolen, the bank cancels the card, issues a new one, and reimburses the client. However, when a patient's PHI [Protected health information] is stolen, the patient cannot change, for example, their birthdate, blood type, and health and genetic information. Once stolen, health information is widely applicable and valuable for a range of crimes, from identity theft to medical fraud. An individual's health information is valued significantly more on the dark web than their social security number or credit card number; it can sell for 10 to 20 times more than this type of data». Vedi anche R. Luna, E. Rhine, M.

maggiormente colpite, cioè gli ospedali, è spesso carente per la scarsità delle risorse economiche disponibili, soprattutto laddove il sistema sanitario nazionale – come nel caso italiano – sia finanziato con soldi (per lo più) pubblici[10]. Questo aspetto limita fortemente gli investimenti sulla sicurezza informatica che riguardano aspetti diversi, tra cui la sostituzione delle attrezzature obsolete, il costante aggiornamento dei sistemi operativi, il corretto *backup* dei dati, così come l'assunzione di personale specializzato e l'adeguata formazione dei professionisti della salute[11].

In un contesto sanitario sempre più digitalizzato e connesso le minacce informatiche si moltiplicano, sia con riferimento alla portata e al volume delle incursioni esterne ma anche al loro – o meglio ai loro – *target*. Innanzitutto, il bersaglio principale è rappresentato dai dati e in particolare dall'accesso non autorizzato alla moltitudine di informazioni relative ai pazienti, soprattutto per motivi di lucro. Un esempio di attacco mirato esclusivamente ai dati si è verificato in Norvegia, dove nel gennaio del 2018 le misure di sicurezza della *South-Eastern Norway Regional Health Authority* – l'autorità regionale che gestisce gli ospedali specializzati e i servizi sanitari nell'area di riferimento – sono state violate, mettendo potenzialmente nelle mani dei cibercriminali coinvolti le informazioni contenute nelle cartelle sanitarie di più di metà della popolazione[12].

Accanto al rischio di violazione della *privacy,* non si devono però trascurare i pericoli che possono derivare alla sicurezza e alla salute del paziente anche a causa della temporanea indisponibilità dei dati oppure della loro distruzione o manomissione. Questo può avvenire qualora ad essere attaccata sia direttamente una struttura ospedaliera con l'effetto di determinare un rallentamento o, nello scenario

---

MYHRA *et al., Cyber threats to health information systems: A systematic review,* in *Technology and Health Care,* 24, 2016, 6; EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Artificial intelligence in healthcare,* cit., 23 ss.

[10] Come sottolineato da A. CANNAVACCIUOLO, *Il finanziamento del Servizio Sanitario Nazionale,* in *Spesa sanitaria,* 1, 2023, 22, «[i]l fabbisogno sanitario nazionale è finanziato da entrate proprie del SSN, da fiscalità regionale (IRAP, IRPEF) e dal bilancio dello Stato (compartecipazione all'accisa sulla benzina e la compartecipazione regionale all'IVA), a cui va aggiunta la quota finanziata dal FSN "vincolata" al perseguimento di determinati obiettivi sanitari».

[11] Vedi S.T. ARGAW, J.R. TRONCOSO-PASTORIZA, D. LACEY *et al., Cybersecurity of Hospitals,* cit., 4. Come sottolinea A.J. CARTWRIGHT, *The elephant in the room: cybersecurity in healthcare,* cit., 1126, «[h]istorically, it is clearly established that IT, and more specifically cybersecurity, has been grossly underfunded within the healthcare sector globally. This has led to the continued use of older equipment, a deliberate abandonment of support and patching services, reduced IT and cybersecurity staff employment and caregiver training which has created an environment which is ripe for the cybercriminal. This is the perfect storm to increase the frequency of attacks on a perceived soft target and an increasing threat surface as healthcare adopts the inevitable digital transition into EMRs [Electronic Medical Records] and the IoMT. The monetization of healthcare records has also made the healthcare sector a rewarding target and this focus is not going to abate soon».

[12] Uno degli aspetti più significativi della vicenda, che fortunatamente non ebbe ripercussione sulla salute dei pazienti o sul funzionamento dell'autorità sanitaria o delle aziende ospedaliere collegate, è la violazione dell'obbligo posto dal *Regolamento generale sulla protezione dei dati* (Reg. (UE) 2016/679) a capo del titolare del trattamento di notificare la violazione dei dati personali all'autorità di controllo competente non più tardi di 72 ore dopo esserne venuto a conoscenza (ex art. 33). Per maggiori dettagli sulla vicenda si veda S.T. ARGAW, J.R. TRONCOSO-PASTORIZA, D. LACEY *et al., Cybersecurity of Hospitals,* cit., 15; e anche O. HUGHES, *Norway healthcare cyber-attack 'could be biggest of its kind',* in *digitalhealth,* 24 gennaio 2028, https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/; W. ASHFORD, *Norwegian healthcare breach alert failed GDPR requirements,* in *ComputerWeekly.com,* 22 gennaio 2018, https://www.computerweekly.com/news/252433538/Norwegian-healthcare-breach-alert-failed-GDPR-requirements.

peggiore, un vero e proprio ostacolo all'erogazione delle prestazioni sanitarie[13]. Emblematico è il caso del noto *ransomware WannaCry* che nella primavera del 2017 colpì il sistema sanitario britannico, rendendo inutilizzabile qualsiasi strumento digitale presente negli ospedali coinvolti – dai computer, alle cartelle sanitarie elettroniche, fino ai dispositivi medici – e limitando l'accesso ai dati fino al pagamento del riscatto[14]. A causa di ciò, decine di ospedali in tutta la nazione si videro costretti a tornare all'analogico e così ad annotare le informazioni dei pazienti a mano e a usare il fax per scambiarsi i referti, ad annullare numerosi consulti e interventi chirurgici programmati, a posticipare gli accertamenti diagnostici che necessitavano di dispositivi o apparecchiature mediche (come risonanze magnetiche, esami del sangue, ...), se non addirittura a dirottare i pazienti verso altre strutture[15].

[13] Cfr. S.T. ARGAW, J.R. TRONCOSO-PASTORIZA, D. LACEY *et al., Cybersecurity of Hospitals,* cit., 1 ss.; E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of Medical Devices. Regulatory Challenges in the European Union,* in I.G. COHEN, T. MINSSEN, W.N. PRICE II, C. ROBERTSON, C. SHACHAR (a cura di), *The future of medical device regulation. Innovation and protection,* Cambridge, 2022, 51.

[14] Non si tratta, peraltro, di un caso isolato. Infatti, analoghi attacchi *ransomware* si erano già verificati in precedenza e sono continuati anche dopo, mettendo in pericolo – seppur con una portata e intensità diversa – numerosi ospedali in diverse parti del mondo, come in Germania nel 2016 (tra i vari bersagli c'era anche il *Lukas Krankenhaus* a Neuss, come riportato da S.T. ARGAW, J.R. TRONCOSO-PASTORIZA, D. LACEY *et al., Cybersecurity of Hospitals,* cit., 3; vedi anche S. STEFFEN, *Cyber attack on hospitals*, in *Deutsche Welle,* 25 febbraio 2016, https://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030) oppure in Nuova Zelanda (S. RYAN, *Hackers attack hospital system,* in *Whanganui Chronicle,* 23 febbraio 2016, https://www.nzherald.co.nz/whanganui-chronicle/news/hackers-attack-hospital-system/TODIJWDVBFLY-VRI5QYMP3L3V5U/?c_id=1503426&objectid=11594628). Tra i paesi maggiormente colpiti vi sono gli Stati Uniti che nel corso degli anni hanno subito ripetuti attacchi, tra i casi più celebri si ricordano l'*Hollywood Presbyterian Medical Center* – soprattutto per la decisione di pagare il riscatto al fine di decriptare il sistema –, l'*Erie County Medical Center* a Buffalo (cfr. W.B. MILLARD, *Where Bits and Bytes Meet Flesh and Blood. Hospital Responses to Malware Attack*, in *Annals of Emergency Medicine,* 70, 3, 2017), l'*Hancock Regional Hospital* (S.T. ARGAW, J.R. TRONCOSO-PASTORIZA, D. LACEY *et al., Cybersecurity of Hospitals,* cit., 3-4) o il recente attacco alla *Prospects Medical Holdings,* un'azienda che gestisce decine di ospedali, cliniche e ambulatori in diversi Stati americani (R. CARBALLO, *Ransomware Attack Disrupts Health Care Services in at Least Three States,* in *The New York Times,* 5 agosto 2023, https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html). Episodi simili non hanno (purtroppo) risparmiato il nostro Paese che, negli ultimi anni, si è spesso trovato a dover fronteggiare incursioni di *hacker* nelle aziende sanitarie a scopi estorsivi. Questo è quanto avvenuto sul finire del 2021 nella ULSS 6 di Padova, dove alcuni cibercriminali si sono infiltrati nei sistemi informatici bloccando alcuni servizi (come la prescrizione di farmaci e specialistica) e minacciando di diffondere i dati dei pazienti, come in parte avvenuto, se non fosse stato pagato il riscatto (per maggiori dettagli: https://www.aulss6.veneto.it/Attacco-hacker-in-Ulss-6-Euganea). La medesima dinamica si è verificata nell'ottobre del 2023 contro l'Azienda Ospedaliera Universitaria di Verona e, a un mese di distanza, ai danni di tre Aziende sanitarie modenesi, provocando – in entrambi i casi – alcuni importanti disservizi e mettendo in pericolo la sicurezza delle informazioni dei pazienti (cfr. D. FADDA, *Attacco all'Azienda Ospedaliera di Verona: dati in vendita, ma quelli sanitari sono una minima parte,* in *Cybersecurity360,* 20 novembre 2023, https://www.cybersecurity360.it/news/in-ospedale-solo-per-urgenze-laoui-di-verona-sotto-attacco-hacker-per-ora-nessuna-rivendicazione/; e ID., *Ransomware colpisce tre Asl di Modena: c'è la rivendicazione del gruppo Hunters, primi dati rubati online,* in *Cybersecurity360,* 13 dicembre 2023, https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-colpisce-tre-asl-di-modena-emergenza-e-rallentamenti-nei-servizi-medici/).

[15] Una dettagliata ricostruzione della portata e della gestione dell'attacco è riportata in NATIONAL AUDIT OFFICE, *Investigation: WannaCry cyber attack and the NHS*, 25 aprile 2018, https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ e W. SMART, *Lessons learned review of the WannaCry Ransomware Cyber Attack*, 1 febbraio 2018, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf. Per maggiori informazioni si vedano anche D. GAYLE, A.

Infine, l'azione dei cibercriminali può essere rivolta alla compromissione dei dispositivi medici in quanto tali oppure come espediente per "entrare" nei sistemi informatici dell'infrastruttura ospedaliera, sfruttando l'interconnessione esistente tra la singola apparecchiatura e l'ambiente digitale circostante[16]. Anche in questo caso, il pericolo per la salute e l'incolumità dei pazienti non deve essere sottovaluto. Attraverso un virus o un *malware* gli *hacker* possono, infatti, prendere il controllo dello strumento in questione e manometterlo cosicché la pompa di insulina[17] o il dispositivo per l'anestesia rilascino un dosaggio errato (se non addirittura letale), il *pacemaker* invii (o meno) un impulso elettrico al cuore al di fuori dei casi previsti[18] oppure per spegnere il respiratore che tiene in vita il paziente[19]. A complicare ulteriormente la situazione, vi è poi il fatto che il numero di dispositivi medici *AI-based* – ovvero dotati o abilitati dall'Intelligenza Artificiale – sta crescendo, portando con sé «una propria – e nuova – superficie di attacco»[20]. Il riferimento è, in particolare, ai c.d. *adversarial attacks* che, per

---

TOPPING, I. SAMPLE *et al., NHS seeks to recover from global cyber-attack as security concerns resurface,* 13 maggio 2017, https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack?CMP=share_btn_tw; C. GRAHAM, *Everything you need to know about 'biggest ransomware' offensive in history,* in *The Telegraph,* 20 maggio 2017, https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

[16] Vedi S. GERKE, T. MINSSEN, G. COHEN, *Ethical and legal challenges of artificial intelligence-driven healthcare*, cit., 323-324; E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,* cit., 164; E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of Medical Devices. Regulatory Challenges in the European Union*, cit., 51; E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 1; K.R. LUDVIGSEN, *The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions,* cit., 67 ss.

[17] Nel 2016 la multinazionale farmaceutica *Johnson & Johnson* informò i pazienti e i medici della presenza in una pompa di insulina di sua produzione – la *OneTouch Ping* – di una falla nelle misure di sicurezza, che laddove debitamente sfruttata avrebbe potuto consentire il controllo da remoto del dispositivo e finanche il rilascio di una dose letale (così J. FINKLE, *J&J warns diabetic patients: Insulin pump vulnerable to hacking,* in *Reuters,* 4 ottobre 2016, https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L/). Un caso simile ha coinvolto anche l'azienda *Medtronic,* come riportato da L.H. NEWMAN, *These Hackers Made an App That Kills to Prove a Point,* in *Wired*, 16 luglio 2019, https://www.wired.com/story/medtronic-insulin-pump-hack-app/.

[18] Questa possibilità è stata testata e confermata da un gruppo di ricercatori. Per maggiori dettagli sulla vicenda si rimanda a L.H. NEWMAN, *A New Pacemaker Hack Puts Malware Directly on the Device,* in *Wired,* 9 agosto 2018, https://www.wired.com/story/pacemaker-hack-malware-black-hat/; A. HERN, *Hackable implanted medical devices could cause deaths, researchers say,* in *The Guardian,* 10 agosto 2018, https://www.theguardian.com/technology/2018/aug/09/implanted-medical-devices-hacking-risks-medtronic.

[19] Per ulteriori esempi di possibili attacchi informatici a danno di dispositivi medici si rimanda all'*Annex II* del MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices – MDCG 2019-16 Rev. 1,* July 2020 (rev. 1), https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf.

[20] Così S. KRASSER, *Attacchi di Adversarial Machine Learning: come riconoscerli e contrastarli*, in *Cybersecurity360,* 24 febbraio 2023, https://www.cybersecurity360.it/nuove-minacce/attacchi-di-adversarial-machine-learning-come-riconoscerli-e-contrastarli/; vedi anche WORLD HEALTH ORGANIZATION, *Ethics and Governance of Artificial Intelligence for Health,* cit., 58; EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Artificial intelligence in healthcare,* cit., 25. Come evidenziato da E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 4: «[w]hat makes AI as or in medical devices unique is the kind of *risks* they pose, as the models and methods used to create and control them are not unique or novel. Examples of these physical risks could be physical harm to the patient through injuries, wrong or dangerous recommended medication, and inadequate choice of surgery. These failures in cybersecurity, make the usage of such medical devices more dangerous than if they possessed no hardware or software, and AI as medical devices go further than this. Instead

esempio, attraverso l'introduzione nel sistema di dati ingannevoli consentono di alternare il corretto funzionamento degli algoritmi di apprendimento automatico causando così errori nella classificazione e, dunque, negli *outputs* prodotti[21].

Le vulnerabilità emergenti nel settore sanitario e le loro potenziali ripercussioni sui diritti fondamentali dei pazienti hanno reso sempre più evidente la necessità di intervenire e di investire sulla cibersicurezza, intesa come l'insieme di misure e attività volte a preservare e garantire al contempo la *security* dei sistemi informativi e delle reti di comunicazione (compresi i dispositivi digitali e i dati) e la *safety* delle persone coinvolte[22]. In questo frangente, anche sulla spinta dei ripetuti attacchi informatici verificatisi negli ultimi decenni, lo sforzo messo in campo dalle istituzioni europee per rafforzare la resilienza informatica e proteggere, così, i cittadini e l'economia dell'Unione è stato notevole, con diversi interventi di portata generale che si inseriscono nella *EU Cybersecurity Strategy*[23].

---

of just attacking a local network or device, the attacker can cause damage to the model, or the AI service used by or as the medical devices, causing damage at scale instead of locally».

[21] Simili attacchi sono stati testati con specifico riferimento al settore medico da un gruppo di ricercatori, che hanno dimostrato come l'immissione di «adversarial noise» in un modello di *machine learning* volto alla classificazione di immagini mediche possa portare a identificare un neo come maligno al 100%, quando prima della "perturbazione" era stato correttamente etichettato come benigno (con un grado di certezza >99%). Come affermato da S.G. FINLAYSON, J.D. BOWERS, J. ITO *et al., Adversarial attacks on medical machine learning. Emerging vulnerabilities demand new conversations*, in *Science,* 363, 6433, 2019, 1287-1288, «such adversarial examples reflect not that machine-learning models are inaccurate or unreliable per se but rather that even otherwise-effective models are susceptible to manipulation by inputs explicitly designed to fool them». Sul possibile impatto degli *adversarial attacks* in medicina si vedano anche gli ulteriori esempi riportati da E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 5 ss.

[22] Nel Regolamento (UE) 2019/881 (o *Cybersecurity Act*), il termine "cibersicurezza" è definito 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» (art. 2, par. 1). Sull'ampiezza e i contenuti del concetto di cibersicurezza si veda EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Definition of Cybersecurity – Gaps and overlaps in standardisation,* dicembre 2015, 10 ss.

[23] Per maggiori dettagli sulle *Cybersecurity policies* dell'Unione europea si rimanda al seguente indirizzo: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq7bt98. In aggiunta ai documenti considerati *infra,* è bene ricordare che sono attualmente in corso di approvazione altre due proposte, quali parti integranti della strategia europea in materia di cibersicurezza. Il riferimento è, innanzitutto, al *Cyber Resilience Act* (*Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 - COM/2022/454 final*), una proposta di regolamento che mira a rafforzare i requisiti di cibersicurezza per i prodotti con elementi digitali, al fine di garantire prodotti *harware* e *software* più sicuri e resilienti alle vulnerabilità informatiche (per maggiori dettagli si veda: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act; EUROPEAN PARLIAMENT RESEARCH SERVICE, *EU cyber-resilience act,* novembre 2023). A questa si affianca, poi, il *Cyber Solidarity Act* (*Proposal for a Regulation of the European Parliament and of the Council Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents - COM (2023) 209 final*), promosso dalla Commissione europea nell'aprile del 2023 con l'obiettivo di potenziare la capacità dell'Unione di identificare, mitigare e rispondere alle minacce e agli incidenti di cibersicurezza anche attraverso l'implementazione di uno scudo europeo per la cibersicurezza e di un meccanismo per affrontare le emergenze informatiche (ulteriori informazioni sono disponibili al seguente indirizzo: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity; EUROPEAN PARLIAMENT RESEARCH SERVICE, *Cyber solidarity act,* novembre 2023). Per maggiori dettagli sugli emendamenti introdotti alla proposta legislativa da parte Consiglio in data 20 dicembre 2023 si rimanda al seguente indirizzo: https://bit.ly/3vbeCW7.

Tra le politiche di sicurezza informatica rientra, innanzitutto, il regolamento sulla cibersicurezza (c.d. *Cybersecurity Act*)[24] il cui scopo è di «garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione»[25]. Come stabilito dall'articolo 1 co. 1, il raggiungimento di tale obiettivo è collegato, da un lato, al rafforzamento del ruolo attribuito all'ENISA (*European Union Agency for Cybersecurity*) e, dall'altro, alla creazione di «un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC»[26]. Di recente, è stata poi adottata la Direttiva NIS2[27] – che sostituirà la precedente Direttiva NIS1[28] a partire dal 18 ottobre 2024[29] – con il dichiarato intento di porre fine alla frammentazione giuridica esistente circa le misure per garantire la ciberresilienza nei settori e servizi, sia pubblici che privati, ritenuti chiave per la società e l'economia europea[30]. Nell'ambito di applicazione della Direttiva NIS2

[24] *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, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).*

[25] Cfr. art. 1 co. 1, Reg. (UE) 2019/881.

[26] Cfr. art. 46 co. 1. Sulla portata del *Cybersecurity Act* in relazione ai dispositivi medici si rimanda a E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 9 e, in particolare, a E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of Medical Devices. Regulatory Challenges in the European Union*, cit., 57-59, che hanno sottolineano le possibili sovrapposizioni tra i sistemi di certificazione e i requisiti relativi alla cibersicurezza contenuti nel *Cybersecurity Act* e nel Regolamento (UE) 2017/745 sui dispositivi medici (c.d. *Medical Devices Regulation*).

[27] *Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)*.

[28] *Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*. Infatti, pur avendo senz'altro contribuito ad innalzare il complessivo livello di ciberresilienza dell'Unione e alla diffusione di una cultura della cibersicurezza negli Stati Membri attraverso l'implementazione di strategie e normative nazionali a protezione dei settori chiave individuati, l'ampia discrezionalità lasciata agli Stati Membri dalla Direttiva NIS1 ha portato a considerevoli divergenze nella sua attuazione, minando così il suo stesso obiettivo che, come emerge a chiare lettere dalla base giuridica (art. 114 TFUE), consisteva «[nel]l'instaurazione e [ne]l funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali» (cons. 4 della Direttiva NIS2). Sulle criticità della Direttiva NIS1 si vedano anche le considerazioni di E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,* cit., 165.

[29] Cfr. Art. 41 co. 1 della Direttiva NIS2.

[30] Come specificato nel considerando 5 della Direttiva NIS2, «la presente direttiva mira a eliminare tali ampie divergenze tra gli Stati membri [cfr. considerando 4], 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». Maggiori informazioni sulle principali novità introdotte dalla Direttiva NIS2 sono contenute in E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,* cit., 165-166, dove sono anche evidenziati – in prospettiva critica – gli elementi di affinità e divergenza tra la procedura di segnalazione di incidenti stabilita nella Direttiva (cfr. art. 23) e la tutela offerta dal *Medical Devices Regulation* (*ivi,* 168 ss.). Sul punto vedi anche E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 14-15.

rientra anche il settore sanitario e anzi la nuova direttiva estende il catalogo di entità ad esso riferibili[31]. Nel rispetto dei criteri stabiliti dall'articolo 2[32], accanto ai prestatori di assistenza sanitaria, rientrano tra i «settori ad alta criticità» (Allegato I) anche i laboratori di riferimento dell'UE[33], i fabbricanti di dispositivi medici critici durante un'emergenza di sanità pubblica e di alcuni prodotti o preparati farmaceutici, nonché i soggetti che svolgono attività di ricerca e sviluppo di medicinali; mentre, negli «altri settori critici» (Allegato II) sono compresi anche coloro che fabbricano dispositivi medici e dispositivi medico-diagnostici *in vitro*[34].

[31] In base alla Direttiva NIS1, soltanto i prestatori di assistenza sanitaria identificati dagli Stati Membri come «operatori di servizi essenziali» (art. 5) rientrano nel suo campo di applicazione e, dunque, sono soggetti agli obblighi di sicurezza e di notifica degli incidenti, ovvero sono tenuti: ad adottare «misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni» così da assicurare «un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente» (art. 14 co. 1); a implementare «misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi» (art. 14 co. 2); e a notificare «senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati» (art. 14 co. 3). Tali misure di sicurezza, nonché l'identificazione degli incidenti che devono essere notificati e le relative modalità di comunicazione sono definite da ciascuno Stato membro all'interno delle strategie nazionali in materia di sicurezza della rete e dei sistemi informativi (ex art. 1 co. 2). Analoghi obblighi a carico degli Stati membri sono contenuti anche nella Direttiva NIS2, all'interno del Capo IV dedicato alle *Misure di gestione del rischio di cibersicurezza e obblighi di segnalazione.* Per maggiori dettagli sulla Direttiva NIS1 si vedano D. MARKOPOULOU, V. PAPAKONSTANTINOU, P. DE HERT, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation,* in *Computer Law & Security Review,* 35, 6, 2019; E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 9-10.

[32] Oltre all'aggiunta di nuovi settori, sottosettori ed entità (Allegato I e II), la Direttiva NIS2 prevede – con maggior chiarezza rispetto alla precedente – un criterio uniforme per identificare i soggetti che rientrano nel suo ambito di applicazione. Per questo motivo, viene stabilita una soglia di dimensione in base alla quale tutte le medie e grandi imprese nei settori elencati che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione sono tenute al rispetto degli obblighi previsti dalla Direttiva (art. 2 co. 1). Nel caso di entità più piccole viene, invece, lasciata agli Stati Membri una certa discrezionalità nell'individuazione di quelle che, alla luce di criteri relativi al loro ruolo nella società e nell'economia o ai particolari settori o servizi forniti (art. 2 co. 2-4), devono essere ricomprese nella NIS2. Le entità così individuate sono poi classificate come "soggetti essenziali" o "soggetti importanti" a seconda della loro dimensione e dell'importanza per il settore o del tipo di servizio fornito, come stabilito dall'art. 3. Si tratta di una distinzione rilevante dal momento che, accanto alle misure di gestione del rischio di cibersicurezza e agli obblighi di segnalazione previsti al Capo IV per tutte le entità soggette alla NIS2, la Direttiva stabilisce differenti regimi di esecuzione e di vigilanza per le due categorie individuate. Le entità qualificate come "importanti" sono, infatti, sottoposte a un regime di vigilanza *ex post* più leggero per quanto riguarda la conformità ai requisiti stabiliti nella NIS2; mentre per le entità "essenziali" sono previste sia misure di vigilanza *ex ante* basate sull'attività prevista, sia *ex post* circa la conformità alla Direttiva. Al fine di delimitare con chiarezza l'ambito di applicazione della NIS2, come previsto dall'art. 3 co. 3, gli Stati membri devono definire entro il 17 aprile 2025 «un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio» e ogni due anni saranno poi chiamati a riesaminare e aggiornare tale elenco.

[33] Ovvero quelli che secondo il *Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio del 23 novembre 2022 relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE* sono responsabili per la promozione di buone pratiche e per il coordinamento della rete di laboratori nazionali di riferimento (ex art. 15).

[34] Mentre per le entità precedentemente elencate il settore di appartenenza è quello sanitario, in questo caso si tratta del settore «fabbricazione» e del settosettore «fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro» (vedi Allegato II, punto 5).

Al Regolamento sulla cibersicurezza e alla Direttiva NIS2 si affiancano poi ulteriori strumenti normativi che affrontano il tema della cibersicurezza in relazione a profili più circoscritti riguardanti, per esempio, i dati, l'intelligenza artificiale e i dispositivi medici. In riferimento ai dati bisogna, innanzitutto, considerare la protezione offerta dal *General Data Protection Regulation* (GDPR)[35], che – come è noto – disciplina il trattamento e la circolazione dei dati personali. In esso sono, infatti, sono stabiliti – seppure limitatamente ai dati personali e, in alcuni casi, ai dati particolari (compresi quelli relativi alla salute)[36] – specifici obblighi in capo al titolare e al responsabile del trattamento per tutelarne l'integrità, la disponibilità e la riservatezza. In estrema sintesi, questi riguardano, da un lato, la messa in atto di «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio»[37], e,

[35] *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*

[36] In base all'art. 9 del GDPR, il trattamento di categorie particolari di dati personali – i c.d. dati sensibili, ovvero «dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (cfr. art. 9 co. 1) – è in principio vietato, tranne nel caso in cui si verifichi una delle condizioni previste dal secondo comma tra cui rientra anche il consenso esplicito dell'interessato per una o più finalità specifiche (lett. a), oppure nel caso in cui il trattamento risulti necessario «per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali» (lett. h), per «motivi di interesse pubblico nel settore della sanità pubblica (lett. i) o ancora «a fini […] di ricerca scientifica» (lett. j). Inoltre, come riportato all'art. 4 par. 14, i *dati relativi alla salute* sono tutti quei «dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute». E, come precisato dal cons. 35, «[n]ei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro».

[37] L'art. 32 co. 1 del GDPR stabilisce, infatti, che «[t]enendo 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». Inoltre, come evidenziato dall'art. 25, le misure tecniche e organizzative volte alla protezione dei dati devono essere incorporate e integrate nel prodotto o servizio in questione fin dalla sua progettazione e pianificazione in accordo al principio della *privacy by design.* Il principio della protezione dei dati fin dalla progettazione – la cui attuazione ricade sul titolare del trattamento – costituisce, infatti, un elemento indispensabile per garantire all'utente la conformità alle disposizioni del GDPR del trattamento dei suoi dati personali. Per maggiori dettagli sul concetto e sulle concrete modalità di attuazione del principio di *privacy by design* si rimanda alle *Linee guida 4/2019*

dall'altro lato, la notifica all'autorità di controllo delle violazioni dei dati personali[38]. Benché il tema non possa essere qui oggetto di esaustiva trattazione, è bene sottolineare che l'attenzione alla questione della protezione dei dati sotto al profilo della cibersicurezza ha trovato conferma nella più recente legislazione di settore in materia di *data sharing*, ovvero in particolar modo in due proposte ancora in corso di approvazione quali lo *European Health Data Space* e il *Data Act*[39].

sull'articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita adottate il 20 ottobre 2020 (versione 2.0) dallo European Data Protection Board.

[38] Cfr. art. 33 GDPR. Come specificato all'articolo 4 par. 12 del GDPR, per *violazione dei dati personali* si intende qualsiasi «violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati». In merito alle interazioni tra GDPR, NIS1, e *Medical Devices Regulation* (Regolamento (UE) 2017/745, vedi *infra*) circa la notifica di incidenti alla sicurezza dei dispositivi medici si rimanda alle considerazioni svolte da E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of Medical Devices. Regulatory Challenges in the European Union*, cit., 60-61.

[39] Assieme al *Data Governance Act* (già entrato in vigore e pienamente applicabile dal settembre del 2023), tali proposte si inseriscono nella strategia europea per i dati (COM(2020)66), promossa dalla Commissione europea allo scopo di promuovere la disponibilità e la condivisione dei dati tra cittadini, soggetti pubblici e privati (come imprese di piccole o grandi dimensioni e *start-up*) nell'ambito dell'Unione europea, garantendo al contempo lo sviluppo dell'innovazione tecnologica e la difesa dei valori e dei diritti europei. In estrema sintesi, per raggiungere tali obiettivi il *Data Governance Act* mira a facilitare la condivisione di dati tra settori pubblici e soggetti privati, prevedendo la possibilità – entro determinate condizioni – di riutilizzare determinate categorie di dati detenute da enti pubblici all'interno dell'Unione, attraverso servizi di intermediazione oppure organizzazioni per l'altruismo dei dati. Il *Data Act* si focalizza maggiormente sulle aziende private e sugli utenti/consumatori dei prodotti digitali, stabilendo precise condizioni relative all'accesso e all'uso dei dati generati dai dispositivi IoT, oltre a prevedere meccanismi per consentire agli enti pubblici di avere accesso e utilizzare i dati detenuti dal settore privato in caso di necessità eccezionali (es. emergenze sanitarie, emergente dovute a calamità naturali, ..). Lo *European Health Data Space* (EHDS) ha, invece, uno scopo più specifico ovvero la creazione di uno spazio comune europeo dei dati sanitari che permetta alle persone di avere maggior controllo sui propri dati sanitari, e di sfruttarne così appieno le potenzialità. Pertanto, le misure contenute nella Proposta sono volte a rafforzare il diritto della persona di disporre e gestire i propri dati sanitari elettronici; a regolare l'immissione sul mercato europeo, la messa a disposizione o la messa in servizio di sistemi di cartelle cliniche elettroniche (anche introducendo requisiti di sicurezza e cibersicurezza per tali prodotti); a predisporre norme e meccanismi circa l'uso secondario dei dati sanitari elettronici; a creare infrastrutture transfrontaliere responsabili dell'uso primario e secondario dei dati sanitari elettronici (cfr. art. 1, co. 2 dello EHDS). Per un approfondimento sulle implicazioni in materia di cibersicurezza dei dispositivi medici si rimanda a E. BIASIN, B. YAŞAR, E. KAMENJAŠEVIĆ, *New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act,* cit., 46-47 e 51 ss.

Per quanto riguarda, invece, il secondo ambito tematico – ovvero l'intelligenza artificiale –, il regolamento europeo in materia (c.d. *Artificial Intelligence Act* o *AI Act*)[40] non è certamente una «cybersecurity-specific law»[41], ma al contempo prescrive una serie di requisiti di cibersicurezza per i sistemi di IA ad alto rischio[42], ampia categoria che – come vedremo – comprende la stragrande maggioranza dei dispositivi medici. E così anche la disciplina europea sui dispositivi medici[43] dove – pur non menzionando espressamente il termine *cybersecurity* – viene dedicato ampio spazio alla protezione dei prodotti medicali da vulnerabilità informatiche che potrebbero intaccarne il funzionamento a danno della salute e della sicurezza dei pazienti[44].

Da questa essenziale panoramica, si evince come in un quadro così composito (e spesso ridondante) possa risultare spesso arduo per l'interprete trovare la bussola e capire quali sono le norme, di volta in volta, applicabili. Ed è proprio in questa direzione che si intende muovere il presente contributo, delimitando però il campo d'indagine ad uno specifico frangente, quello della cibersicurezza dei dispositivi medici, che – come già evidenziato – si interseca e inserisce a pieno titolo nel più ampio tema della resilienza informatica del settore sanitario alla luce della stretta interdipendenza e connessione tra i singoli *devices* e l'ambiente fisico e digitale circostante.

---

[40] Come è ben noto, il Regolamento europeo sull'intelligenza artificiale, presentato dalla Commissione europea nell'aprile del 2021 (*Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione - COM/2021/206 final,* per brevità *AI Act Proposal*), è oramai in via di definitiva adozione a seguito della recente approvazione da parte del Parlamento europeo. Il testo votato lo scorso 13 marzo è frutto dell'accordo provvisorio raggiunto l'8 dicembre 2023 dal Consiglio e dal Parlamento, con cui sono state introdotte alcune modifiche rispetto alla versione originaria, poi confermate – il 2 febbraio 2024 – con voto unanime da parte del Comitato dei Rappresentanti Permanenti (il testo presentato ai rappresentanti degli Stati membri dalla presidenza belga del Consiglio dei ministri, d'ora in poi *AI Act Draft,* è consultabile al seguente indirizzo: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf). Per completare la procedura, si attende la verifica dei giuristi-linguisti e il voto finale del Parlamento e del Consiglio, a cui seguirà poi la pubblicazione in Gazzetta ufficiale dell'UE e la successiva entrata in vigore (dopo 20 giorni). Per maggiori dettagli si rimanda al comunicato stampa pubblicato al seguente indirizzo: https://www.europarl.europa.eu/news/it/press-room/20240308IPR19015/il-parlamento-europeo-approva-la-legge-sull-intelligenza-artificiale. In attesa della definitiva adozione del regolamento, si segnala che le considerazioni svolte nel presente lavoro sono aggiornate all'ultimo testo approvato dal Parlamento, il c.d. *AI Act* (reperibile al seguente indirizzo: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_IT.pdf).

[41] Così E. Biasin, B. Yaşar, E. Kamenjašević, *New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act,* cit., 48.

[42] Vedi H. Junklewitz, R. Hamon, A. André, T. Evas, J. Soler Garrido, J.I. Sanchez Martin, *Cybersecurity of Artificial Intelligence in the AI Act*, Luxembourg, 2023, in particolare 7 ss.

[43] Il riferimento è, in particolare, al *Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio* (c.d. *Medical Devices Regulation* o MDR); anche se – come specificato *infra* – l'attuale disciplina europea in materia è comprensiva del *Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione* (c.d. *In Vitro Diagnostic Medical Devices Regulation* o IVDR), che riguarda i dispositivi medico-diagnostici *in vitro.*

[44] Per una disamina delle misure di cibersicurezza dei dispositivi medici (*AI-based* e non) stabilite dal Regolamento (UE) 2017/745 e dall'*AI Act* si veda il par. 2.2.

Per affrontare tale questione, verrà innanzitutto analizzato il Regolamento (UE) 2017/745 sui dispositivi medici, concentrandosi, *in primis,* sugli aspetti definitori e in particolare sul significato del termine *software* che consente di estendere il campo di applicazione anche ai prodotti *AI-based*. Chiarire i contorni della definizione di dispositivo medico (oltre che la relativa classificazione) costituisce un tassello imprescindibile della presente analisi. Infatti, è proprio da questi elementi che dipende l'applicabilità o meno allo specifico *device* in questione dei requisiti stabiliti a livello europeo non solo dal *Medical Devices Regulation* ma anche – come si vedrà – dall'*Artificial Intelligence Act*. Infine, il contributo si soffermerà sulle misure a garanzia della cibersicurezza dei dispositivi medici, partendo da quelle stabilite nella legislazione di settore – grazie, soprattutto, alla chiave di lettura offerta dal *Medical Device Coordination Group*[45] – fino ad esaminare quali novità verranno introdotte a seguito dell'entrata in vigore e della conseguente applicazione dell'*AI Act.*

2. I dispositivi medici: aspetti definitori e misure per garantirne la cibersicurezza

A partire dagli anni '90, l'Unione Europea ha progressivamente adottato norme relative alla sicurezza e al corretto funzionamento dei dispositivi medici nell'ambito della legislazione sulla sicurezza dei prodotti. Inizialmente, il quadro normativo era composto da tre direttive riguardanti i dispositivi medici impiantabili attivi[46], i dispositivi medici[47] e i dispositivi medico-diagnostici *in vitro*[48]. Tuttavia, l'avanzamento delle conoscenze scientifiche e tecniche registrato nel settore sanitario nei decenni successivi alla loro adozione, unito alle considerevoli divergenze applicative e interpretative e ad alcuni scandali riguardanti prodotti difettosi a danno della salute pubblica[49] resero evidente la necessità di un'approfondita revisione e modernizzazione della normativa vigente.
Per soddisfare tali esigenze, nel 2012 la Commissione europea presentò due proposte legislative volte a rivedere e aggiornare la disciplina dei dispositivi medici. Dopo ampie consultazioni di esperti, le precedenti direttive vennero abrogate e sostituite da due regolamenti, entrambi entrati in vigore nel maggio 2017[50] allo scopo di migliorare la sicurezza e la qualità dei dispositivi medici – e conseguentemente di offrire ai pazienti prodotti più sicuri e innovativi – attraverso il rafforzamento e l'armonizzazione dei

[45] L'ultima versione della *Guidance on Cybersecurity for medical devices,* pubblicata nel gennaio del 2020, offre infatti un'accurata panoramica delle disposizioni e dei requisiti minimi relativi alla cibersicurezza contenute nel Regolamento (UE) 2017/745. Pur non essendo legalmente vincolante, tale guida costituisce un indispensabile e prezioso strumento per i fabbricanti di dispositivi medici, soprattutto per l'autorevolezza dell'organismo che l'ha prodotto, ovvero il *Medical Device Coordination Group,* in cui siede un rappresentante designato da ciascun Stato membro (*ex* art. 103 MDR).
[46] *Direttiva 90/385/CEE del Consiglio, del 20 giugno 1990, per il ravvicinamento delle legislazioni degli Stati Membri relative ai dispositivi medici impiantabili attivi.*
[47] *Direttiva 93/42/CEE del Consiglio, del 14 giugno 1993, concernente i dispositivi medici*.
[48] *Direttiva 98/79/CE del Parlamento europeo e del Consiglio del 27 ottobre 1998 relativa ai dispositivi medico-diagnostici in vitro*.
[49] Così S. KIERKEGAARD, P. KIERKEGAARD, *Danger to public health: Medical devices, toxicity, virus and fraud,* in *Computer law and security review,* 29, 1, 2013, in particolare 17 ss.
[50] Maggiori dettagli sul pacchetto proposto dalla Commissione e sul procedimento di adozione dei due regolamenti sono reperibili al seguente indirizzo: https://ec.europa.eu/commission/presscorner/detail/it/IP_17_847.

requisiti per l'immissione sul mercato e l'impiego dei dispositivi medici[51] e, allo stesso tempo, di promuovere l'innovazione e aumentare la competitività del settore biomedicale.

L'attuale normativa in materia si compone, dunque, del Regolamento (UE) 2017/745 sui dispositivi medici–che a seguito di una proroga di un anno è diventato applicabile dal 26 maggio 2021[52], e del Regolamento (UE) 2017/746 relativo ai dispositivi medico-diagnostici *in vitro* che ha trovato applicazione a decorrere dal 26 maggio 2022[53]. I nuovi regolamenti integrano le precedenti direttive, aggiungendo ulteriori requisiti alle procedure già previste per l'immissione nel mercato o la messa in servizio

[51] I due regolamenti si allineano alle disposizioni di riferimento contenute nella Decisione 768/2008/CE, che ha istituito un quadro comune per la commercializzazione di vari prodotti come parte di un più ampio pacchetto di misure di armonizzazione, noto come *New Legislative Framework* (NLF). Il NLF è stato adottato nel 2008 con l'intento di rafforzare le condizioni per l'immissione nel mercato unico di un'ampia gamma di prodotti, oltre che la sorveglianza del mercato e l'efficacia delle valutazioni di conformità. Per maggiori dettagli vedi https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en.

[52] In base al *Regolamento (UE) 2020/561 del Parlamento europeo e del Consiglio del 23 aprile 2020 che modifica il regolamento (UE) 2017/745 relativo ai dispositivi medici, per quanto riguarda le date di applicazione di alcune delle sue disposizioni*, l'applicabilità del Regolamento (UE) 2017/745 è stata posticipata di un anno a causa della pandemia da Covid-19, soprattutto per la necessità di non ostacolare la fornitura di dispositivi medici essenziali, quali guanti medicali, mascherine chirurgiche, attrezzature per la terapia intensive, … (considerando 2-3). In particolare, nel considerando 3 si sottolinea che «[d]ata l'entità senza precedenti delle sfide attuali, e tenendo conto della complessità del regolamento (UE) 2017/745, è molto probabile che gli Stati membri, le istituzioni sanitarie, gli operatori economici e gli altri soggetti pertinenti non saranno in grado di garantirne l'attuazione e l'applicazione corrette a decorrere dal 26 maggio 2020, come ivi previsto». È importante, però, sottolineare che la completa applicazione del regolamento, in tutte le sue parti, si avrà soltanto allo scadere del periodo transitorio previsto. Infatti, in considerazione della complessità dei nuovi requisiti introdotti e per garantire la loro corretta applicazione, il Regolamento aveva stabilito un periodo transitorio, che inizialmente doveva concludersi il 26 maggio 2024, durante il quale alcuni dispositivi conformi alla Direttiva 90/385/CEE o alla Direttiva 93/42/CEE avrebbero potuto egualmente entrare nel mercato europeo. Tuttavia, a causa della limitata capacità degli organismi notificati di portare a termine le procedure di valutazione della conformità ancora pendenti e delle difficoltà incontrate dai fabbricanti nel soddisfare i requisiti del regolamento e nell'ottenere le certificazioni necessarie, si è resa necessaria l'estensione della durata del periodo transitorio per scongiurare il pericolo di carenza di dispositivi medici oppure crisi della salute pubblica all'interno dell'UE. Per questi motivi, il Regolamento (UE) 2017/745 è stato recentemente modificato dal Regolamento (UE) 2023/607 (*Regolamento (UE) 2023/607 del Parlamento europeo e del Consiglio del 15 marzo 2023 che modifica i regolamenti (UE) 2017/745 e (UE) 2017/746 per quanto riguarda le disposizioni transitorie per determinati dispositivi medici e dispositivi medico-diagnostici in* vitro) per introdurre una proroga scaglionata delle disposizioni transitorie – fino al 31 dicembre 2027 o al 31 dicembre 2028 –, soggetta a determinate condizioni e alla classe di rischio dei dispositivi. Inoltre, è stato rimosso – anche con riferimento ai dispositivi medico-diagnostici *in vitro* – il limite temporale oltre il quale era vietata l'ulteriore messa a disposizione sul mercato o la messa in servizio di dispositivi immessi sul mercato entro la fine del periodo di transizione applicabile e che si trovavano ancora nella catena di fornitura un anno dopo la fine di tale periodo di transizione (c.d. *"sell-off" date*). Per maggiori dettagli si rimanda a https://health.ec.europa.eu/medical-devices-sector/new-regulations_en; https://ec.europa.eu/commission/presscorner/detail/it/qanda_23_24.

[53] Nonostante ciò, il *Regolamento (UE) 2022/112 del Parlamento europeo e del Consiglio del 25 gennaio 2022 che modifica il regolamento (UE) 2017/746 per quanto riguarda le disposizioni transitorie per determinati dispositivi medico-diagnostici in vitro e l'applicazione differita delle condizioni concernenti i dispositivi fabbricati internamente* ha previsto la graduale applicazione del nuovo regolamento sui dispositivi medico-diagnostici *in vitro,* attraverso l'estensione dei limiti temporali contenuti nelle disposizioni transitorie. Infatti, a causa della pandemia, un gran numero di risorse è stato reindirizzato per affrontare tale crisi, ostacolando così la possibilità di dare

di dispositivi medici[54], così da incrementare il livello di protezione della salute dei pazienti e degli utilizzatori, colmare le lacune esistenti e assicurare la sicurezza dei dispositivi medici lungo tutto il loro

piena attuazione alle modifiche normative entro i tempi previsti. A ciò si devono poi aggiungere le carenze organizzative degli organismi notificati che impediscono ai fabbricanti di espletare le necessarie procedure di valutazione della conformità. La necessità di evitare interruzioni significative nella catena di fornitura dei dispositivi medico-diagnostici *in vitro* critici, anche alla luce dei possibili rischi per la salute dei pazienti, ha portato il Parlamento europeo e il Consiglio a modificare le disposizione transitorie del Regolamento UE 2017/746 in base alla classe di rischio dei dispositivi, estendendo così i periodo transitori dei dispositivi ad alto rischio fino al 26 maggio 2025 o 2026 (rispettivamente per la Classe D e la Classe C) e fino al 26 maggio 2027 per quelli a rischio più basso. L'applicazione differita del nuovo regolamento riguarda, però, soltanto i dispostivi medico-diagnostici *in vitro* per cui è richiesto l'intervento di un organismo notificato o i dispositivi "nuovi", ossia quelli che non rientrano nel campo d'applicazione della Direttiva 98/79/CE. Inoltre, la conformità alla maggior parte delle condizioni previste per i dispositivi *in house* è stata rinviata al 26 maggio 2028. Per maggiori dettagli si rimanda alla consultazione del seguente indirizzo: https://ec.europa.eu/commission/presscorner/detail/it/ip_21_5209. Il 23 gennaio 2024 la Commissione europea ha proposto una ulteriore dilazione all'applicazione del Regolamento UE 2017/746 così da concedere più tempo alle imprese per adeguarsi alle nuove disposizioni nel rispetto di determinate condizioni, ed evitare interruzioni nella fornitura di dispositivi medico-diagnostici essenziali per la cura dei pazienti (vedi *Proposal for a Regulation of the European Parliament and the Council amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards a gradual roll-out of Eudamed, information obligation in case of interruption of supply and the transitional provisions for certain in vitro diagnostic medical devices*). Nella Proposta di regolamento si prevede, dunque, di estendere il periodo di transizione fino al dicembre 2027 per i dispositivi a elevato rischio individuale e per la salute pubblica (Classe D), fino al dicembre 2028 per i dispositivi a rischio individuale elevato e/o moderato per la salute pubblica (Classe C) e fino al dicembre 2029 per i dispositivi a basso rischio. Ulteriori informazioni sono reperibili al seguente indirizzo: https://ec.europa.eu/commission/presscorner/detail/it/ip_24_346.

[54] Sui contenuti e i limiti della disciplina precedente si vedano https://www.consilium.europa.eu/it/policies/new-rules-medical-in-vitro-diagnostic-devices/; S. KIERKEGAARD, P. KIERKEGAARD, *Danger to public health: Medical devices, toxicity, virus and fraud,* cit., 14 ss. In sintesi, a differenza di quanto avviene per i prodotti farmaceutici, la commercializzazione di un dispositivo medico non è subordinata ad autorizzazione preventiva da parte di un'autorità apposita, ma piuttosto a una valutazione della conformità allo scopo di accertare il rispetto dei requisiti di sicurezza e di salute stabiliti nella normativa. A seconda del rischio posto dal dispositivo – e, dunque, della relativa classe di rischio –, la valutazione prevede oneri procedurali differenti, tra cui il coinvolgimento di entità terze e indipendenti – note come organismi notificati –, designate e monitorate dagli Stati membri. Se le condizioni previste sono soddisfatte e, di conseguenza, il fabbricante appone la marcatura CE, il dispositivo può essere immesso nel mercato e utilizzato secondo la propria destinazione d'uso. Accanto alle disposizioni che riguardano la fase *pre-market,* per mantenere un elevato standard di qualità e sicurezza dei dispositivi sono stabilite anche regole *post*-commercializzazione che riguardano la gestione di incidenti e la sorveglianza dei dispositivi sul mercato. Per assicurare un adeguato livello di qualità, affidabilità e sicurezza dei dispositivi sul mercato, un ruolo decisivo spetta agli standard ovvero quell'insieme di norme e specifiche tecniche definite da appositi organismi di diritto privato, sia a livello europeo che internazionale. L'adesione agli standard da parte dei fabbricanti non è obbligatoria ma rimane su base volontaria e, tuttavia, come specificato dal considerando 22 e dall'articolo 8 del Regolamento (UE) 2017/745, il rispetto delle norme armonizzate (c.d. *harmonised standards*), ovvero quell'insieme di particolari specifiche tecniche elaborate su richiesta della Commissione europea dal Comitato europeo di normazione (CEN) e dal Comitato europeo di normazione elettrotecnica (CENELEC) – talvolta assieme ad organizzazioni internazionali per la standardizzazione come la *International Standardization Organization* (ISO) – e pubblicate nella Gazzetta Ufficiale dell'Unione Europea, comporta una presunzione di conformità ai requisiti previsti dal regolamento stesso (sul valore e la natura giuridica degli standard tecnici armonizzati si rimanda a C-613/14 - *James Elliott Construction Limited c. Irish Asphalt Limited*, parr. 37-42 e T-474/15 - *Global Garden Products Italy SpA (GGP Italy) c. Commissione europea*, par. 60). L'elenco aggiornato delle norme armonizzate relative ai dispositivi medici è contenuto nella *Decisione di esecuzione (UE) 2021/1182 della Commissione del 16 luglio 2021 re-*

"ciclo di vita", dalla progettazione e fabbricazione, fino allo loro commercializzazione e al loro concreto utilizzo[55]. Le principali novità introdotte riguardano, pertanto, la previsione di regole più stringenti sull'efficacia e sicurezza dei dispositivi prima della loro entrata in commercio[56], il rafforzamento delle misure rivolte ai fabbricanti per la sorveglianza *post-market*[57], nonché una maggior trasparenza, tracciabilità dei dispositivi e accessibilità alle informazioni a beneficio dei pazienti[58].

2.1. La definizione di dispositivo medico secondo il Regolamento (UE) 2017/745: quale spazio per i dispositivi medici *AI-based?*

Il Regolamento (UE) 2017/745 si applica ad un'ampia gamma di dispositivi medici per uso umano, che vengono definitivi come: «qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: — diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie, — diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità, — studio,

lativa alle norme armonizzate per i dispositivi medici redatte a sostegno del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio (per maggiori dettagli si veda: https://health.ec.europa.eu/medical-devices-topics-interest/harmonised-standards_en; e più in generale https://europa.eu/youreurope/business/product-requirements/standards/standards-in-europe/index_it.htm#inline-nav-2).

[55] Così F.C. LA VATTIATA, *AI-based medical devices: the applicable law in the European Union,* in *BioLaw Journal – Rivista di BioDiritto,* 4, 2022, 415-416. Per una panoramica delle novità introdotte si vedano https://health.ec.europa.eu/medical-devices-new-regulations/overview_it; EUROPEAN COMMISSION, *New EU Rules to Ensure Safety of Medical Devices,* https://health.ec.europa.eu/system/files/2020-07/md_generic_fs_en_0.pdf.

[56] Per questo motivo vengono previsti: a) controlli addizionali per i dispositivi ad alto rischio prima della loro immissione sul mercato attraverso il coinvolgimento di gruppi di esperti, chiamati a formulare pareri e a fornire consulenze scientifiche, tecniche e cliniche agli organismi notificati (art. 106 MDR e art. 48 IVDR); b) criteri più rigorosi per la designazione, la gestione delle attività e la supervisione degli organismi notificati (Capo IV), anche alla luce del loro maggior coinvolgimento nelle procedure di valutazione della conformità e di certificazione; c) estensione dell'ambito di applicazione a dispositivi con finalità estetica o altra finalità non medica (come, ad esempio, lenti a contatto colorate) con caratteristiche e rischi analoghi a dispositivi medici (cons. 12 del MDR), così come a dispositivi monouso ricondizionati e a dispositivi medico-diagnostici *in vitro* volti ad accertare la predisposizione a una condizione clinica o a una malattia (art. 2, co. 1 n. 2, lett. c, IVDR); d) regole più rigorose in merito alla valutazione e/o indagine clinica dei dispositivi medici, alle evidenze cliniche e alla valutazione delle prestazioni e studi delle prestazioni dei dispositivi medici *in vitro* (Capo VI), compresa una procedura di valutazione coordinata per indagini cliniche o per studi delle prestazioni pluricentrici (art. 78 MDR e art. 74 IVDR); e) un nuovo sistema di classificazione dei rischi per i dispositivi medico-diagnostici *in vitro* in linea con gli orientamenti internazionali (art. 47 e Allegato VIII del IVDR). Per un approfondimento circa le indagini e valutazioni cliniche dei dispositivi medici si rimanda a C. CHILLIN, *Le indagini e le valutazioni cliniche dei dispositivi medici al tempo del* Medical Device Regulation *e del GDPR,* in V. SALVATORE (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea,* Torino, 2023, 81 ss.

[57] Vedi il Capo VII di entrambi i regolamenti.

[58] In risposta alle preesistenti difficoltà, la nuova disciplina mira ad aumentare la trasparenza attraverso diverse misure: a) la creazione di una banca dati europea sui dispositivi medici (EUDAMED), alla quale gli Stati membri, gli operatori economici, i pazienti, gli operatori sanitari e il pubblico possono accedere per ottenere tutte le informazioni pertinenti sui dispositivi medici disponibili sul mercato dell'UE (art. 33 e 34 MDR e art. 30 IVDR); b) l'implementazione di un sistema di identificazione e tracciabilità dei dispositivi, il c.d. sistema UDI (art. 27 MDR e art. 24 IVDR); c) l'onere in capo ai fabbricanti di fornire una "tessera per il portatore di impianto" rivolta ai pazienti e contenente tutte le informazioni pertinenti i dispositivi medici impiantabili (art. 18 MDR).

sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico, — fornire informazioni attraverso l'esame *in vitro* di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi»[59].

Come indicato all'articolo 51, tutti i dispositivi medici sono suddivisi in quattro classi (Classe I, IIa, IIb e III) a seconda della destinazione d'uso prevista e del grado di rischio, a partire da quelli non invasivi fino a dispositivi che presentano un rischio elevato[60]. La classificazione dei dispositivi sulla base del *risk-based approach* incide sensibilmente sul procedimento necessario per l'immissione sul mercato o messa in servizio, dal momento che dalla classe del prodotto dipende la procedura di valutazione della conformità[61].

[59] Cfr. art. 2, par. 1. Nella definizione sono poi ricompresi anche i «dispositivi per il controllo o il supporto al concepimento» e i «prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi di cui all'articolo 1, paragrafo 4, e di quelli di cui al primo comma del presente punto» (*ivi*). Inoltre, il Regolamento si applica anche a prodotti che non hanno uno scopo medico, come alcuni dispositivi estetici (cfr. Allegato XVI) che presentano però caratteristiche simili, in termini di funzionamento e di rischio, a quelle di dispositivi medici che rientrano nel suo campo di applicazione, come, ad esempio, le lenti a contatto colorate.

[60] In base alle regole di classificazione stabilite nell'Allegato VIII, appartengono alla Classe I dispositivi a basso rischio (compresi i prodotti più semplici e non invasivi, come stetoscopi, bende o occhiali); alla Classe IIa dispositivi a medio rischio; mentre nella Classe IIb e III rientrano i dispositivi ad alto rischio. Una completa panoramica sulla classificazione dei dispositivi medici è contenuta nelle linee guida stilate dal Gruppo di coordinamento per i dispositivi medici (vedi MEDICAL DEVICE COORDINATION GROUP, *Guidance on classification of medical devices – MDCG 2021-24,* ottobre 2021, https://health.ec.europa.eu/system/files/2021-10/mdcg_2021-24_en_0.pdf; EUROPEAN COMMISSION, *Factsheet for Class I Medical Devices. What You Need to Know About Regulation (EU) 2017/45*, 2021, consultabile al seguente indirizzo: https://health.ec.europa.eu/system/files/2021-07/md_mdcg_2021_factsheet-cl1_en_0.pdf).

[61] Le diverse procedure di valutazione della conformità sono illustrate negli Allegati IX-XI. In sintesi, come specificato dall'articolo 52, i fabbricanti hanno l'obbligo di intraprendere una procedura di valutazione della conformità per dimostrare che i dispositivi soddisfano le condizioni prescritte dal regolamento (art. 10) prima di procedere alla loro commercializzazione. Mentre i dispositivi della classe I richiedono che il fabbricante rediga, previa predisposizione della documentazione tecnica richiesta, una dichiarazione di conformità UE per attestare l'aderenza del dispositivo al regolamento; per i dispositivi a medio e alto rischio è previsto un maggiore e sempre più incisivo coinvolgimento degli organismi notificati nella procedura di valutazione della conformità del dispositivo (cfr. cons. 60), a cui il fabbricante deve presentare una domanda di certificazione. In termini generali, i requisiti generali di sicurezza e prestazione (Allegato I), tra cui rientrano anche la valutazione clinica del dispositivo e la documentazione tecnica, compresa quella sulla sorveglianza post-commercializzazione (Allegato II, III), si applicano a tutti i prodotti indipendentemente dalla classe. A questi si aggiungono poi le ulteriori condizioni stabilite nelle procedure di valutazione della conformità (cfr. Allegati IX-XI) a seconda del tipo di dispositivo. Inoltre, per alcuni dispositivi ad alto rischio è richiesta la partecipazione di gruppi di esperti indipendenti nella fase di controllo *pre-market*, che hanno il compito di fornire agli organismi notificati la propria consulenza scientifica sul prodotto. Una volta superata la procedura di valutazione della conformità, si deve apporre al prodotto la marcatura CE di conformità, un elemento necessario per la commercializzazione dei dispositivi medici nel mercato europeo che attesta l'aderenza ai requisiti del regolamento. Per maggiori dettagli si veda MEDICAL DEVICE COORDINATION GROUP, *Guidance on classification of medical devices,* cit., 4 ss.; e la pagina *Procedure di valutazione della conformità,* curata dal Ministero della Salute, e consultabile al seguente indirizzo: https://www.salute.gov.it/portale/dispositiviMedici/dettaglioContenutiDispositiviMedici.jsp?lingua=italiano&id=5923&area=dispositivi-medici&menu=organisminotificati.

Uno degli aspetti più lungimiranti del Regolamento (UE) 2017/745 – e, in realtà, già in parte presente nella precedente direttiva – riguarda proprio il suo campo di applicazione e, più nello specifico, la definizione di dispositivo medico. Essa, infatti, sembra tenere in particolare considerazione i *trend* evolutivi del settore, includendo al suo interno anche i dispositivi medici *AI-based* che – come detto in precedenza – rientrano a pieno titolo tra le nuove frontiere della salute[62].

Tornando a quanto stabilito dall'art. 2, anche un *software* destinato dal fabbricante ad essere impiegato sull'uomo per almeno una delle finalità mediche specificate viene considerato un dispositivo medico, sia nel caso in cui venga utilizzato da solo (*stand-alone software* o *medical device software*)[63] oppure come componente di un altro dispositivo, cioè quale suo accessorio[64]. Come ha avuto modo di chiarire la Corte di Giustizia nel caso *Snitem,* la qualificazione di un *software* come dispositivo medico dipende, infatti, da «due condizioni cumulative che ogni dispositivo di tal genere deve presentare, attinenti, rispettivamente, alla finalità perseguita e all'azione prodotta»[65]. In altri termini, questo significa che «un software è di per sé un dispositivo medico quando è specificamente destinato dal fabbricante ad essere impiegato per una o più delle finalità mediche stabilite nella definizione di dispositivo medico»[66], indipendentemente dal fatto che agisca o meno direttamente nel o sul corpo umano[67].

È importante, inoltre, sottolineare che non tutti i *software* adoperati in ambito medico sono automaticamente dei dispositivi medici e devono, pertanto, soddisfare i requisiti stabiliti dal Regolamento (UE)

[62] Così U. RUFFOLO, *L'Intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento",* in *Responsabilità medica,* in *Giurisprudenza italiana,* febbraio 2021, 506. Tuttavia, in EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Artificial intelligence in healthcare,* cit., 30, viene sottolineato come, dal momento che l'elaborazione del regolamento risale ad un periodo in cui l'intelligenza artificiale era nella sua fase iniziale di sviluppo, «many aspects specific to AI are not considered, such as continuous learning of the AI models or the identification of algorithmic biases. In particular, the fact that AI is a highly adaptive technology that continues to learn and adjust over time – as more data becomes available – calls for new approaches to monitor the risks of the AI software». In questo senso, l'imminente adozione Regolamento europeo sull'intelligenza artificiale (il c.d. *Artificial Intelligence Act*) potrebbe giocare un ruolo fondamentale, andando a colmare le lacune esistenti.

[63] In questo caso, come specificato dall'art. 2 par. 4, il *software* è considerato un *dispositivo attivo,* termine con cui si definisce «qualsiasi dispositivo il cui funzionamento dipende da una fonte di energia diversa da quella generata dal corpo umano per tale scopo o dalla gravità e che agisce modificando la densità di tale energia o convertendola. I dispositivi destinati a trasmettere, senza modifiche di rilievo, l'energia, le sostanze o altri elementi tra un dispositivo attivo e il paziente non sono considerati dispositivi attivi».

[64] Cfr. cons. 19 e art. 2 par. 2.

[65] Corte di Giustizia UE, C-329/16 - *caso Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v. Premier ministre and Ministre des Affaires sociales et de la Santé,* 7 dicembre 2017, par. 22.

[66] *Ivi,* par. 24

[67] Questo era, infatti, uno dei due punti centrali del caso *Snitem* che si riferiva alla condizione dell'azione prodotto (cfr. par. 27 ss.). Quanto, invece, alla questione della finalità, la Corte di Giustizia chiarisce che «un software che procede al controllo incrociato dei dati personali del paziente con i medicinali che il medico intende prescrivere e che è quindi in grado di fornire allo stesso automaticamente un'analisi finalizzata a identificare, segnatamente, le eventuali controindicazioni, interazioni tra medicinali e posologie eccessive, è utilizzato a fini di prevenzione, di controllo, di terapia o di attenuazione di una malattia e persegue, di conseguenza, uno scopo specificamente medico, circostanza che lo rende un dispositivo medico ai sensi dell'articolo 1, paragrafo 2, lettera a), della direttiva 93/42» (par. 25). L'interpretazione della Corte di Giustizia circa la definizione di *software* contenuta nella direttiva – ora sostituita dal regolamento – è stata avvallata dal *Medical Device Coordination Group* anche con riferimento alla nuova disciplina (vedi *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR – MDCG 2019-11*, ottobre 2019, https://ec.europa.eu/docsroom/documents/37581, 6 ss.).

2017/745. Il considerando 19 stabilisce, infatti, che «il software destinato a finalità generali, anche se utilizzato in un contesto sanitario, o il software per fini associati allo stile di vita e al benessere non è un dispositivo medico»[68]. Per esempio, il fascicolo sanitario elettronico che contiene documenti e dati relativi ad un paziente non costituisce di per sé un dispositivo medico, se non limitatamente ad alcune funzionalità relative alla prescrizione di farmaci oppure alla visualizzazione di immagini a fini diagnostici; lo stesso vale anche per i sistemi di comunicazione utilizzati nelle aziende ospedaliere che si basano su *software* con finalità generali. Tuttavia, sono da qualificare come dispositivi medici quei moduli che, basandosi sul monitoraggio e l'analisi dei parametri fisiologici del paziente, generano avvisi o allarmi[69].

[68] Su questo punto già la Corte di Giustizia escludeva dalla definizione di dispositivo medico «un software che, pur destinato a essere utilizzato in un contesto medico, ha tuttavia l'unico scopo di archiviare, memorizzare e trasmettere dati, come un software che memorizza i dati sanitari del paziente, un software la cui funzione si limita a indicare al medico curante il nome del medicinale generico associato a quello che intende prescrivere o ancora un software destinato a segnalare le controindicazioni menzionate dal fabbricante di tale medicinale nelle istruzioni per l'uso» (Corte di Giustizia UE, C-329/16, caso *Snitem*, par. 26). Come specificato dalla *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR*: «[s]oftware can directly control a (hardware) medical device (e.g. radiotherapy treatment software), can provide immediate decision-triggering information (e.g. blood glucose meter software), or can provide support for healthcare professionals (e.g. ECG interpretation software). It is important to clarify that not all software used within healthcare is qualified as a medical device. For example, "Simple search", which refers to the retrieval of records by matching record metadata against record search criteria or to the retrieval of information does not qualify as medical device software (e.g. library functions). However, software which is intended to process, analyse, create or modify medical information may be qualified as a medical device software if the creation or modification of that information is governed by a medical intended purpose. For example, the software which alters the representation of data for a medical purpose would qualify as a medical device software (e.g. "searching image for findings that support a clinical hypothesis as to the diagnosis or evolution of therapy" or "software which locally amplifies the contrast of the finding on an image display so that it serves as a decision support or suggests an action to be taken by the user"). However, altering the representation of data for embellishment/cosmetic or compatibility purposes does not readily qualify the software as medical device software. Software intended for non-medical purposes (excluding MDR Annex XVI devices), such as invoicing or staff planning, does not qualify as a medical device software. These software do not fall under the Medical Devices Regulations. A task such as e-mailing, web or voice messaging, data parsing, word processing, and back-up is by itself not considered as having a medical purpose» (*ivi,* 6-7). Per quanto riguarda la definizione di *software* e la relativa classificazione secondo le classi di rischio stabilite nel Regolamento (UE) 2017/745 (cfr. Regola 11, Allegato VIII), si vedano, *ex multis,* K. LUDVIGSEN, S. NAGARAJA, A. DALY, *When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law,* in *European Journal of Risk Regulation,* 13, 2022; F.C. LA VATTIATA, *AI-based medical devices: the applicable law in the European Union,* cit., 416 ss.; D. CHIAPPINI, *Legal and ethics state-of-the-art of artificial intelligence in medicine,* cit., 135-137; S. GERKE, T. MINSSEN, G. COHEN, *Ethical and legal challenges of artificial intelligence-driven healthcare*, cit., 311-312; G. BINCOLETTO, mHealth app *per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali,* in *BioLaw Journal – Rivista di BioDiritto,* 4, 2021, 397 ss.

[69] Ulteriori esempi sono contenuti nell'*Annex I* della *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.*

Al contempo, bisogna considerare che il termine *software* all'interno del Regolamento (UE) 2017/745 è ben più ampio rispetto alla definizione fornita nell'*AI Act*[70], con la conseguenza che un *medical device software* non costituisce necessariamente un dispositivo medico *AI-based.* In altri termini, affinché si possa parlare di dispositivo medico *AI-based* è necessario che il *software* venga riconosciuto come dispositivo medico – indipendente o in combinazione ad un altro dispositivo – e che si tratti di un sistema di intelligenza artificiale, ovvero di un *software AI-powered*[71]. Questo è il caso delle applicazioni che attraverso l'analisi di dati e il riconoscimento di immagini mediante tecniche di apprendimento automatico offrono un utile supporto al medico nella diagnosi e nella decisione terapeutica[72] oppure consentono di predire, con sempre maggior accuratezza, il decorso clinico del paziente[73].
A differenza del Regolamento (UE) 2017/745, l'*AI Act* ha una portata generale avendo come obiettivo di regolare l'intelligenza artificiale nel suo complesso tramite l'introduzione di quadro giuridico di rife-

[70] Anche se nel Regolamento (UE) 2017/745 manca una definizione del termine, il *Medical Device Coordination Group* stabilisce – per i fini delle linee guida – che «"software" is defined as a set of instructions that processes input data and creates output data» (*ivi,* 5).

[71] Nell'ultima versione disponibile dell'*AI Act,* per *sistema di IA* si intende «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali» (art. 3, par. 1). La definizione di *AI system* è stata modificata rispetto al testo della Proposta per allinearsi a quanto previsto dalle organizzazioni internazionali che si occupano di intelligenza artificiale (vedi *AI Act Draft,* 3). Tuttavia, la portata innovativa della revisione deve essere ridimensionata alla luce di quanto riportato nel considerando 12 dell'*AI Act* che recita: «la nozione di "sistema di IA" […] dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico. Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi da input o dati. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi [c.d. *machine learning*] e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere [*logic- and knowledge-based approaches*]. La capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati e consente l'apprendimento, il ragionamento o la modellizzazione».

[72] Vedi, *ex multis,* R. SUTTON, D. PINCOCK, D.C. BAUMGART *et al.*, *An overview of clinical decision support systems: benefits, risks, and strategies for success,* in *Nature Partner Journals – Digital Medicine,* 3, 17, 2020; K.A. TRAN, O. KONDRASHOVA, A. BRADLEY *et al.*, *Deep learning in cancer diagnosis, prognosis and treatment selection*, in *Genome Medicine,* 13, 152, 2021; S. SANCHEZ-MARTINEZ, O. CAMARA, G. PIELLA *et al., Machine Learning for Clinical Decision-Making: Challenges and Opportunities in Cardiovascular Imaging,* in *Frontiers in Cardiovascular Medicine,* 8, gennaio 2022; R. GARGEYA, T. LENG, *Automated Identification of Diabetic Retinopathy Using Deep Learning,* in *Ophthalmology,* 124, 7, giugno 2017.

[73] F. MOHSEN, H.R.H. AL-ABSI, N.A. YOUSRI *et al., A scoping review of artificial intelligence-based methods for diabetes risk prediction,* in *Nature Partner Journals – Digital Medicine,* 3, 197, 2023; D. PLACIDO, B. YUAN, J.X. HJALTELIN *et al., A deep learning algorithm to predict risk of pancreatic cancer from disease trajectories,* in *Nature Medicine,* 29, 2023; T.M. USMAN, Y.K. SAHEED, A. NSANG, *A systematic literature review of machine learning based risk prediction models for diabetic retinopathy progression,* in *Artificial Intelligence in Medicine,* 143, 2023.

rimento che sia in grado di favorire lo sviluppo tecnologico e industriale in questo settore e di preservare, al contempo, i valori e i diritti fondamentali riconosciuti e tutelati dal diritto dell'Unione[74]. Da qui la scelta di un approccio normativo proporzionato basato sul rischio ovvero la previsione di regimi regolatori differenziati a seconda del pericolo concretamente posto dalla singola applicazione di intelligenza artificiale alla salute, alla sicurezza o ad altri diritti fondamentali[75].

Pur non contendo disposizioni che riguardano, nello specifico, l'applicazione dell'IA nel settore sanitario, si ritiene che «many medical AI tools, especially those that are autonomous, will be categorised as high-risk», in base alle regole sulla classificazione del rischio previste nell'*AI Act*[76]. L'art. 6 co. 1 del

[74] Cfr. cons. 8 dell'*AI Act*. Come riportava la Commissione europea nell'*Explanatory Memorandum* all'*AI Act Proposal*, «la […] proposta presenta un approccio normativo orizzontale all'IA equilibrato e proporzionato, che si limita ai requisiti minimi necessari per affrontare i rischi e i problemi ad essa collegati, senza limitare od ostacolare indebitamente lo sviluppo tecnologico o altrimenti aumentare in modo sproporzionato il costo dell'immissione sul mercato di soluzioni di IA» (vedi *Explanatory Memorandum*, 3).

[75] Cfr. cons. 26 dell'*AI Act*. I possibili utilizzi dell'IA vengono differenziati in tre diversi livelli di rischio: a) inaccettabile; b) alto; c) basso o minimo. In sintesi, l'*AI Act* prevede al Capo II un elenco di pratiche vietate – in assoluto o soltanto in principio, ovvero con alcune limitate eccezioni – in quanto l'uso di simili sistemi di IA non può considerarsi accettabile, perché profondamente contrario ai valori dell'Unione (vedi cons. 28). Tra i divieti previsti dall'art. 5 rientrano strumenti di IA volti alla manipolazione del comportamento, allo sfruttamento delle vulnerabilità e al controllo sociale, come per esempio le pratiche di *social scoring,* la categorizzazione biometrica sulla base di caratteristiche sensibili, l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto (con poche eccezioni), la raccolta indiscriminata ("*untargeted scraping*") di immagini facciali allo scopo di creare o ampliare *database* di riconoscimento facciale, l'utilizzo di sistemi di riconoscimento delle emozioni in ambito lavorativo o educativo (eccetto per motivi medici o di sicurezza), oppure le pratiche di polizia predittiva fondate unicamente sulla profilazione o sulla valutazione delle caratteristiche della personalità. Con riferimento ai sistemi classificati come "ad alto rischio" (cfr. art. 6, e Allegati I e III), il regolamento condiziona la loro immissione sul mercato, la messa in servizio e l'uso nell'Unione – previa marcatura CE – al rispetto dei requisiti obbligatori previsti (cfr. art. 8 ss.) e di una valutazione di conformità *ex ante* che, in alcuni casi, prevede il coinvolgimento di soggetti terzi, nonché all'adozione di un sistema di vigilanza *post-market.* In aggiunta a ciò, l'ultima versione dell'*AI Act* ha previsto l'introduzione di una valutazione d'impatto sui diritti fondamentali (c.d. *fundamental rights impact assessment,* art. 27) limitata, però, ad alcuni *deployer* e della possibilità di testare i sistemi ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA, ovvero le c.d. *AI regulatory sandboxes* (vedi artt. 60-61). Inoltre, ai cittadini viene attribuito il diritto di presentare un reclamo ad un'autorità di vigilanza del mercato (art. 85) e di ottenere una spiegazione in merito a decisioni basate su sistemi di IA ad alto rischio che incidono sui propri diritti (art. 86). Per l'ultima categoria – residuale rispetto alle altre – dove rientrano i sistemi a basso o minimo rischio è, invece, previsto un regime regolatorio semplificato, in quanto la loro commercializzazione è libera o – in determinati casi – subordinata al rispetto di obblighi di trasparenza in capo ai fornitori (cfr. art. 50). Al contempo, si incoraggia però l'elaborazione di codici di condotta per agevolare e promuovere l'applicazione volontaria dei requisiti previsti per i sistemi ad altro rischio (art. 95). Con riferimento ai sistemi di IA per finalità generali, l'*AI Act* prescrive in capo ai fornitori una serie di obblighi di trasparenza circa il funzionamento del modello di IA, nonché il necessario delle norme UE sul diritto d'autore (art. 53); mentre, a carico dei fornitori di modelli di IA per finalità generali con rischio sistemico (cfr. regole di classificazione *ex* art. 51) sono previste delle condizioni ulteriori tra cui rientrano la valutazione dei modelli, l'analisi e mitigazione di rischi, e la segnalazione di eventuali incidenti e delle appropriate misure correttive (art. 55).

[76] Così European Parliamentary Research Service, *Artificial intelligence in healthcare,* cit., 31. «This means future medical AI tools should fulfil all the requirements already established by the Medical Device Regulation, but also those listed in Chapter II of the AI regulation (use of high quality and representative data, technical documentation and traceability, transparency requirement, human oversight, quality management system, conformity assessment, etc.)» (*ivi,* 32). Al contempo, come specificato dal considerando 51 dell'*AI Act,* «[l]a classificazione di

Regolamento include, infatti, nella categoria ad alto rischio tutti quei sistemi di IA che sono essi stessi prodotti o componenti di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'Unione in base al *New Legislative Framework* (NFL)[77], la cui immissione sul mercato o messa in servizio è soggetta a una valutazione della conformità da parte di terzi. Questo comporta che la quasi totalità dei *medical devices software* rientranti nell'ambito di applicazione dell'*AI Act* potrebbero essere considerati come sistemi di IA ad alto rischio, dal momento che i regolamenti sui dispositivi medici – il Regolamento (UE) 2017/745 e il Regolamento (UE) 2017/746 – fanno parte del NFL e richiedono una valutazione di conformità da parte di un organismo notificato[78]. Fanno eccezione a quest'ultimo requisito soltanto i dispositivi di classe I, per i quali tale procedura «dovrebbe essere svolta, in linea di massima, sotto la responsabilità esclusiva del fabbricante, dato il basso livello di vulnerabilità associata a tali dispositivi»[79].

2.2. Le misure di cibersicurezza dei dispositivi medici (*AI-based* e non) previste dal Regolamento (UE) 2017/745 e dall'*AI Act*

Come precedentemente evidenziato, lo scopo del Regolamento (UE) 2017/745 è quello di garantire un elevato livello di qualità e sicurezza dei dispositivi medici per uso umano e di assicurare una maggiore protezione della salute dei pazienti e degli utilizzatori, stimolando la produzione e commercializzazione di strumenti innovativi e sicuri. In tale orizzonte si inseriscono anche le misure poste a tutela della cibersicurezza. La consapevolezza delle sfide tecnologiche emergenti legate al pericolo di hackeraggio di apparecchiature medicali sempre più sofisticate e connesse ha, infatti, portato il legislatore europeo

un sistema di IA come ad alto rischio a norma del presente regolamento non dovrebbe necessariamente significare che il prodotto il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia considerato "ad alto rischio" in base ai criteri stabiliti nella pertinente normativa di armonizzazione dell'Unione che si applica al prodotto. Ciò vale in particolare per il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio e per il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, in cui è prevista una valutazione della conformità da parte di terzi per i prodotti a medio rischio e ad alto rischio». Per maggiori dettagli sul rapporto tra l'*AI Act* e il Regolamento (UE) 2017/745 si veda *infra.*

[77] Elencata nell'Allegato I dell'*AI Act.*

[78] Cfr. cons. 50 dell'*AI Act*. Vedi E. BIASIN, B. YAŞAR, E. KAMENJAŠEVIĆ, *New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act,* cit., 48; E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 11-12; E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,* cit., 167; MedTech Europe, *Proposal for an Artificial Intelligence Act (COM/2021/206) - MedTech Europe response to the open public consultation,* 6 agosto 2021, https://www.medtecheurope.org/news-and-events/news/medtech-europe-response-to-the-open-public-consultation-on-the-proposal-for-an-artificial-intelligence-act-com-2021-206/; F.C. LA VATTIATA, *AI-based medical devices: the applicable law in the European Union,* cit., 431.

[79] Cfr. cons. 60 MDR. L'intrinseca complessità e l'invasività dei sistemi di IA utilizzati in medicina rendono però arduo immaginare la loro collocazione all'interno della classe I, che – come noto – riguarda dispositivi più semplici e (per la maggior parte) non invasivi, come stetoscopi, bende o occhiali (così F.C. LA VATTIATA, *AI-based medical devices: the applicable law in the European Union,* cit., 417). A ciò si aggiunga che i dispositivi medici *AI-based* sono solitamente considerati come *medical device software* e che questi, in base alla Regola 11 dell'Allegato VIII del Regolamento (UE) 275/2016, sono classificati come dispositivi a rischio medio o elevato ovvero di classe II o superiore.

a rafforzare la capacità di difesa dei dispositivi medici contro attacchi informatici intenzionali e malevoli, non solo con riferimento alla progettazione ma lungo l'intero ciclo di vita del dispositivo[80].

Pur senza mai menzionare il termine *cybersecurity*, il nuovo Regolamento contiene diverse disposizioni volte a proteggere i dispositivi medici da accessi non autorizzati e a evitare la compromissione o alterazione delle loro funzionalità a discapito della salute e sicurezza dei pazienti, oltre che la violazione della confidenzialità, integrità e disponibilità delle informazioni contenute[81]. A conferma di ciò, è sufficiente consultare la *Guidance on Cybersecurity for medical devices* elaborata dal *Medical Device Coordination Group* per i fabbricanti di dispositivi medici, dove vengono riassunti gli standard minimi riferibili alla cibersicurezza che devono essere soddisfatti per l'immissione sul mercato o la messa in servizio dei propri prodotti e mantenuti anche successivamente la loro commercializzazione[82].

Innanzitutto, tra i requisiti generali di sicurezza e prestazione elencati nell'Allegato I del Regolamento è previsto che i dispositivi medici in normali condizioni d'uso siano «sicuri ed efficaci e non compromett[a]no lo stato clinico o la sicurezza dei pazienti, né la sicurezza e la salute degli utilizzatori ed eventualmente di altre persone». Questo comporta che il loro sviluppo e la produzione siano adeguati allo stato dell'arte delle conoscenze scientifiche e tecnologiche in materia, e che gli eventuali rischi residui associati al loro impiego risultino accettabili alla luce di un bilanciamento rispetto ai benefici ricavabili dai pazienti, nonché «compatibili con un elevato livello di protezione della salute e della sicurezza»[83].

---

[80] Così MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 4.

[81] Per un approfondimento sulle disposizioni relative alla cibersicurezza dei dispostivi medici contenute nel Regolamento (UE) 2017/745 si vedano E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of Medical Devices. Regulatory Challenges in the European Union*, cit., 53 ss.; K.R. LUDVIGSEN, *The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions*, cit., 61 ss.

[82] La guida sugli standard di sicurezza si rivolge, *in primis,* ai fabbricanti di dispositivi medici, in quanto principali responsabili della conformità dei prodotti medicali rispetto ai requisiti stabiliti all'interno del Regolamento (UE) 2017/745; ma prevede anche il coinvolgimento attivo di ulteriori soggetti al fine di raggiungere l'obiettivo finale, ossia un adeguato livello di cibersicurezza a tutela dei pazienti (MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 4 e in particolare 12 ss.). Infatti, come riportato dal *Medical Device Coordination Group*, «it should be noted that for the provision of secured healthcare services, it is important to recognise the roles and expectations of all stakeholders, such as manufacturers, suppliers, healthcare providers, patients, integrators, operators and regulators. All of these actors share responsibilities for ensuring a secured environment for the benefit of patients' safety» (*ivi,* 12). Con riferimento agli utenti finali della catena di approvvigionamento del prodotto, il MDCG sottolinea che i professionisti della salute sono tenuti ad adoperare un dispositivo medico soltanto in conformità all'uso previsto e, nel fare ciò, possono accedere, esaminare e scambiare dati, così come essere chiamati a definire i parametri di utilizzo del dispositivo e ad illustrarne il funzionamento ai pazienti. Per quanto riguarda quest'ultimi, in aggiunta alle informazioni contenute nelle istruzioni d'uso, essi devono essere incoraggiati a mettere in pratica *cyber smart behaviours* o *cyber hygiene practices*, ovvero tutte quelle azioni di base che qualsiasi utente può (e dovrebbe) adottare per contribuire alla protezione dispositivo, oltre che di sé stessi e dei propri dati (es. utilizzo di *password* forti, aggiornamento dei *software*, attenzione ai messaggi sospetti, ..). Nel considerando 8 del *Cybersecurity Act* si sottolinea, infatti, che «[l]a cibersicurezza non costituisce soltanto una questione relativa alla tecnologia, ma anche una in cui il comportamento umano è di pari importanza. Di conseguenza, è opportuno promuovere energicamente l'«igiene informatica», vale a dire semplici misure di routine che, se attuate e svolte regolarmente da cittadini, organizzazioni e imprese, riducono al minimo la loro esposizione a rischi derivanti da minacce informatiche».

[83] Punto 1, Allegato I, MDR. Come evidenziato al punto successivo, la riduzione per quanto possibile dei rischi derivanti dall'utilizzo del dispositivo – comprensivi dei «security risks», «security risks with safety impact» e «safety related risks» (così MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 10) – deve essere realizzata senza compromettere il rapporto benefici-rischi, ovvero garantendo al contempo le

A tal fine, allo scopo «di limitare al massimo i rischi e prevenire incidenti relativi ai dispositivi»[84] si richiede ai fabbricanti di implementare fin dalla progettazione un sistema di gestione del rischio indirizzato a proteggere il dispositivo da incursioni esterne (c.d. *security issues*), oltre che la salute e sicurezza dei pazienti (c.d. *safety issues*)[85], di cui fanno parte anche la valutazione dei rischi (o *risk assessment*) e la previsione di misure di controllo del rischio[86].

Il Regolamento introduce, poi, ulteriori e specifici requisiti per tutti i dispositivi più avanzati, ovvero quelli contenenti sistemi elettronici programmabili (compresi i *software*) e per i *medical device software.* La loro progettazione e fabbricazione deve, infatti, assicurare la riproducibilità, l'affidabilità e le prestazioni in conformità alla destinazione d'uso prevista e deve includere misure adeguate a eliminare

prestazioni del dispositivo secondo la sua destinazione d'uso e un elevato livello di protezione della salute (punto 2, Allegato I, MDR). A tal proposito, può essere importante l'implementazione da parte dei fabbricanti degli standard elaborati dalle organizzazioni per la standardizzazione. Infatti, anche laddove non si tratti di norme armonizzate (*harmonised standards*), il rispetto degli standard riconosciuti permette di attestare che le decisioni del fabbricante siano conformi allo stato dell'arte e di dimostrare l'adeguatezza delle scelte compiute per affrontare i rischi circa la sicurezza del dispositivo (vedi MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 7).

[84] Cfr. cons. 32 MDR.

[85] Tanto più che, come sottolineato dal MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 9-10, una minaccia alla sicurezza (*security*) del dispositivo può riverberarsi negativamente sulla salute e integrità fisica delle persone e che anche nella predisposizione delle misure per garantire la cibersicurezza del dispositivo bisogna tener conto del loro possibile impatto sulla *safety* del paziente. In altri termini, «the use of too restrictive security measures that provide a high level of protection may have a safety impact, especially if the security functionalities are not well designed. For example, during an emergency, the medical personnel must be able to access an implanted cardiac device without restrictions, but strong security measures need to be in place under normal operating conditions» (*ivi,* 10).

[86] Il sistema di gestione del rischio deve essere introdotto a partire dalla fase di progettazione e poi mantenuto e aggiornato lungo l'intero ciclo di vita del dispositivo, anche grazie alle informazioni provenienti dalla fase di produzione e dal sistema di sorveglianza post-commercializzazione (cfr. punto 3, lett. e-f, Allegato I, MDR). Esso, in particolare, si compone di un piano di gestione del rischio; di una valutazione dei rischi, ovvero di un'analisi dei pericoli noti e prevedibili oltre che dei rischi associati all'utilizzo del dispositivo (compresi quelli associati alla cibersicurezza), tenendo conto non solo dell'uso previsto ma anche dell'«uso scorretto ragionevolmente prevedibile» (cfr. punto 3, lett. a-c, Allegato I, MDR); di misure di controllo del rischio per la fabbricazione e produzione dei dispositivi volte alla eliminazione o riduzione dei rischi, e che devono attenersi a principi di rispetto della sicurezza e tener conto dello stato dell'arte generalmente riconosciuto (cfr. punto 4, Allegato I, MDR). Per dimostrare la conformità ai requisiti previsti dal Regolamento in materia di gestione del rischio i fabbricanti possono fare riferimento alla norma armonizzata *EN ISO 14971:2019 Dispositivi medici - Applicazione della gestione dei rischi ai dispositivi medici,* emendata A11:2021 (vedi MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 16-17). Con riferimento ai dispositivi non su misura, tutti gli aspetti sopra elencati devono essere accuratamente riportati dal fabbricante all'interno della relativa documentazione tecnica, in modo che la sua consultazione permetta di valutare l'aderenza o meno alle prescrizioni del regolamento (cfr. art. 10 co. 4, MDR). Tale documentazione tecnica, che deve essere redatta dal fabbricante e contenere le informazioni indicate nell'Allegato II, costituisce una rilevante misura di tipo organizzativo, indispensabile ai fini della valutazione di conformità del dispositivo e, dunque, per la sua immissione sul mercato o messa in servizio. Inoltre, è compito del fabbricante tenere aggiornata la documentazione tecnica del dispositivo – comprendente anche il piano di sorveglianza post-commercializzazione (cfr. art. 84 e Allegato III) – alla luce dei dati emersi proprio dal sistema di sorveglianza post-commercializzazione (cfr. art. 83), soprattutto in relazione alla gestione e alle azioni correttive per affrontare gli incidenti e le vulnerabilità in materia di cibersicurezza (MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 23-24).

o quantomeno a ridurre al minimo il deterioramento delle prestazioni e i rischi[87], compresi quelli «associati alla possibile interazione negativa tra il software e l'ambiente tecnologico ("ambiente IT") in cui opera e interagisce»[88].

Lo sviluppo dei *software* – autonomi o incorporati in un dispositivo – deve conformarsi allo stato dell'arte, così come tenere presente l'eventuale necessità di interventi di manutenzione o aggiornamenti nel rispetto dei c.d. «principles of development life cycle». Inoltre, considerata la capacità di registrare, trasmettere e memorizzare una molteplicità di dati – anche particolari *ex* art. 9 del GDPR – , specifica attenzione all'interno del processo di gestione del rischio deve essere dedicata alla *sicurezza delle informazioni*, attraverso la predisposizione di presidi tecnici volti a garantire adeguata protezione dal pericolo di furto, cancellazione o manomissione dei dati contenuti[89].

Oltre a ciò, per garantire un sufficiente livello di qualità e sicurezza e, in particolare, per assicurare il corretto funzionamento del *software* risulta indispensabile non solo integrare direttamente nel prodotto misure di sicurezza *by design* calibrate alla sua destinazione d'uso, ma anche considerare l'ambiente operativo in cui potrebbe essere concretamente impiegato[90]. Per questo motivo, il fabbricante è chiamato ad individuare una serie di requisiti minimi con specifico riferimento al contesto applicativo in cui il dispositivo in questione andrà ad operare, che comprendono indicazioni «in materia di hardware, caratteristiche delle reti informatiche e misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato»[91]. Spetta, poi, al fabbricante anche il compito di fornire agli utilizzatori o alle altre persone coinvolte i *minimum IT requirements* identificati, facendo sì che questi vengano

[87] Punto 17.1, Allegato I, MDR.

[88] Cfr. punto 14.2 lett. d, Allegato I, MDR. Infatti, nel processo di progettazione e fabbricazione di apparecchiature medicali non si può trascurare l'interazione con l'ambiente circostante e/o con altri dispositivi o *software* e, di conseguenza, le eventuali ripercussioni che ciò può determinare sulle prestazioni delle stesse. A tal fine, come sottolineato al punto 14.1, «[s]e un dispositivo è destinato a essere utilizzato insieme ad altri dispositivi o attrezzature, l'insieme risultante, compreso il sistema di raccordo, è sicuro e non compromette le prestazioni previste dei singoli dispositivi». Inoltre, al punto 14.5 si stabilisce che «[i] dispositivi destinati a essere utilizzati insieme ad altri dispositivi o prodotti sono progettati e fabbricati in modo tale che l'interoperabilità e la compatibilità siano affidabili e sicure».

[89] Al punto 17.2. è, infatti, stabilito che «[p]er i dispositivi contenenti un software o per i software che costituiscono dispositivi a sé stanti, il software è sviluppato e fabbricato conformemente allo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, compresa la sicurezza delle informazioni, della verifica e della convalida».

[90] In MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 10, si afferma, infatti, che «[a] medical device should be designed in a layered defence in depth approach and therefore should not rely on security controls in the operating environment. Nevertheless, as part of this layered defence in depth approach, there are expectations on the intended operating environment […]. Expectations on the operating environment might include protection and performance characteristics. Often the expectations are common best practice, often called "good security hygiene". Expectations on the intended operating environment should be clearly documented and communicated to the operator».

[91] Cfr. Punto 17.4, Allegato I, MDR. Come specificato dal MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 20, è infatti responsabilità del fabbricante indicare le misure tecniche e organizzative relative al contesto operativo che risultano essenziali per garantire la cibersicurezza del dispositivo e che non possono essere integrate *by design.* Tra queste rientrano presidi di varia natura che vanno dalle garanzie all'integrità del dispositivo (es. controllo degli accessi tramite autenticazione), all'utilizzo di appropriati controlli di sicurezza (es. gestione dell'accesso degli utenti; sistemi di *antivirus* e di protezione da *malware*), fino a misure che riguardano la crittografia dei dati o l'utilizzo di *password* forti (*ivi,* 21-22).

riportati nelle istruzioni d'uso del dispositivo[92], assieme a tutte le ulteriori informazioni rilevanti[93]. La conoscenza di tali misure – comprese le pratiche di *cyber hygine* – e dei possibili rischi residui relativi alla cibersicurezza rappresenta un tassello fondamentale per permettere al professionista della salute e al paziente di avere maggior controllo sulle funzionalità del dispositivo e di contribuire attivamente per preservare la sicurezza informatica dello stesso[94].

In aggiunta alle misure di sicurezza *by design* e a quelle relative all'ambiente IT, è inoltre essenziale adottare efficaci strategie di sorveglianza e vigilanza della cibersicurezza dei dispositivi medici anche con riferimento alla fase successiva alla commercializzazione dei dispositivi. Infatti, in un settore dinamico e particolarmente soggetto ad accelerazioni sotto il profilo scientifico e tecnologico – quale è quello biomedico – le minacce e vulnerabilità informatiche mutano ed evolvono nel tempo, con la conseguenza che le difese inizialmente adottate possono risultare – anche a distanza ravvicinata – obsolete e non più idonee a raggiungere un accettabile livello rischio-beneficio[95]. Per questo motivo, è responsabilità del fabbricante implementare e mantenere aggiornato un sistema di sorveglianza post-commercializzazione che tenga conto anche delle misure di cibersicurezza del dispositivo. Come stabilito dall'art. 83 del Regolamento (UE) 2017/745, esso si basa sulla raccolta e analisi delle pertinenti informazioni circa la qualità, le prestazioni e la sicurezza del dispositivo, ricavate anche grazie al coinvolgimento e all'esperienze maturata da diversi attori – *in primis* dagli utenti e dai distributori, e se del caso dagli importatori e dal rappresentante autorizzato –, al fine di aggiornare e migliorare il sistema di gestione del rischio, così come di individuare e attuare tempestivamente le azioni preventive e correttive più appropriate per eliminare potenziali motivi di difformità del prodotto rispetto agli standard richiesti o altre situazioni indesiderabili in relazione alla natura e ai rischi associati al dispositivo[96].

[92] Cfr. Punto 23.4, lett a *ter),* Allegato I, MDR. In MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 20, viene specificato che «[t]he manufacturer shall provide clear documentation of the device's instructions for use, including IT security features/configurations (if applicable), and clear instructions for the IT security controls related to the operating environment, including product specifications, compatibilities, recommended IT security measures, IT environment configuration (e.g. traffic control), etc.».

[93] Infatti, in relazione all'etichettatura e alle istruzioni d'uso, il punto 23.1 dell'Allegato I del MDR prescrive che «[o]gni dispositivo [sia] corredato delle informazioni necessarie a identificare il dispositivo e il fabbricante e da tutte le informazioni in materia di sicurezza e prestazione pertinenti per gli utilizzatori o per altre persone». Per una panoramica delle indicazioni relative alla cibersicurezza che devono essere fornite nelle istruzioni d'uso e ai prestatori di assistenza sanitaria si veda MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 23 ss.

[94] Con riferimento a ciò, il Regolamento (UE) 2017/745 stabilisce che i dispositivi destinati a utilizzatori profani debbano essere «progettati e fabbricati in modo tale da essere funzionali rispetto alla loro destinazione d'uso, tenuto conto delle capacità e dei mezzi a disposizione di tali utilizzatori profani e degli effetti derivanti da variabilità tecniche e ambientali che si possono ragionevolmente prevedere». Questo comporta che i fabbricanti devono fornire informazioni quanto più comprensibili e appropriate in modo da permettere agli utenti di metterle agevolmente in pratica e di utilizzare il dispositivo in modo sicuro e preciso, riducendo per quanto possibile i rischi all'integrità fisica nonché errori d'uso (cfr. punto 22.1 e 22.2, Allegato I).

[95] Vedi MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 28.

[96] *Ivi,* 28-29. Come precedentemente evidenziato, la documentazione tecnica che deve accompagnare il dispositivo viene aggiornata dal fabbricante sulla base delle informazioni emerse attraverso il sistema di sorveglianza post-commercializzazione (cfr. art. 83 co. 3, MDR).

Infine, tra i compiti di vigilanza del fabbricante rientra la segnalazione di qualsiasi incidente grave[97] relativo a dispositivi già sul mercato – compresa la violazione delle difese del prodotto a causa di attacchi informatici – e delle azioni correttive di sicurezza intraprese o da mettere in atto al fine di prevenire o ridurre il pericolo di danni alla salute e sicurezza del paziente[98], così da poter svolgere le indagini necessarie per risalire alle cause dell'incidente informatico e valutare l'adeguatezza delle soluzioni avanzate anche grazie alla cooperazione delle autorità competenti ed eventualmente dell'organismo notificato[99].

Per avere una visuale quanto più completa sulle misure di cibersicurezza dei dispositivi medici risulta, poi, necessario ampliare lo sguardo e soffermarsi sulle disposizioni rilevanti contenute, in particolar modo, nell'*AI Act*[100]. Infatti, come visto nel precedente paragrafo, la maggior parte degli strumenti di intelligenza artificiale impiegati in ambito sanitario è destinata a rientrare nella categoria degli *high-risk AI systems* sulla base dell'art. 6 co. 1 dell'*AI Act,* con la conseguenza di dover applicare loro i requisiti obbligatori stabiliti nel regolamento per poterli far entrare nel mercato europeo[101]. Tra questi rientrano anche specifiche indicazioni relative alla cibersicurezza che meritano di essere brevemente analizzate in considerazione dell'oggetto della presente trattazione.

---

[97] Con il termine *incidente grave* si intende «qualsiasi incidente che, direttamente o indirettamente, ha causato, può aver causato o può causare una delle seguenti conseguenze: a) il decesso di un paziente, di un utilizzatore o di un'altra persona; b) il grave deterioramento, temporaneo o permanente, delle condizioni di salute del paziente, dell'utilizzatore o di un'altra persona; c) una grave minaccia per la salute pubblica» (art. 2, par. 65, MDR).

[98] Cfr. Art. 87 MDR.

[99] Cfr. Art. 89 MDR. Vedi anche MEDICAL DEVICE COORDINATION GROUP, *Guidance on Cybersecurity for medical devices,* cit., 29-30.

[100] Per maggiori dettagli sui requisiti relativi alla cibersicurezza contenuti nell'*AI Act* e sulle possibili divergenze applicative rispetto alla procedura di segnalazione di incidenti prevista nel MDR si vedano E. BIASIN, E. KAMENJAŠEVIĆ, K.R. LUDVIGSEN, *Cybersecurity of AI medical devices: risks, legislation, and challenges,* cit., 11 ss.; E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,* cit., 167-168 e 171 ss; e anche E. BIASIN, B. YAŞAR, E. KAMENJAŠEVIĆ, *New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act,* cit., 47 ss.

[101] Il riferimento è ai requisiti per i sistemi di IA ad alto rischio, previsti agli artt. 8 ss. dell'*AI Act* (Sezione 2, Capo III). In merito al rapporto tra il Regolamento europeo sull'intelligenza artificiale e il Regolamento (UE) 2017/745, è bene evidenziare come già nell'*Explanatory Memorandum* dell'*AI Act Proposal* si sottolineasse la necessità di garantire – in forza della «natura orizzontale della proposta» – un'assoluta coerenza tra le disposizioni contenute nell'*AI Act* e la normativa di armonizzazione dell'Unione volta a regolare la sicurezza di quei prodotti che potrebbero – già ora oppure in un prossimo futuro – incorporare o costituire sistemi di IA (comprendente anche il *Medical Device Regulation*), al fine di ridurre oneri e costi addizionali per gli operatori del settore (*ivi,* 4). Per maggiori dettagli si rimanda alle considerazioni svolte da A. GERYBAITE, S. PALMIERI, F. VIGNA, *Equality in Healthcare AI: Did Anyone Mention Data Quality?*, in *BioLaw Journal – Rivista di BioDiritto,* 4, 2022, 399-400; F.C. LA VATTIATA, *AI-based medical devices: the applicable law in the European Union,* cit., 429; E. BIASIN, E. KAMENJAŠEVIĆ, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals,* cit., 172 ss. In relazione a questo profilo, l'articolo 8 co. 2 del testo consolidato dell'*AI Act* chiarisce che «[s]e un prodotto contiene un sistema di IA cui si applicano i requisiti del presente regolamento e i requisiti della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, [in cui rientra anche il Regolamento (UE) 2017/745] i fornitori sono responsabili di garantire che il loro prodotto sia pienamente conforme a tutti i requisiti applicabili previsti dalla normativa di armonizzazione dell'Unione applicabile». Al contempo, quando si tratta di *high-risk AI systems* risulta indispensabile applicare i requisiti previsti dal nuovo Regolamento (artt. 8 ss.), dal momento che – come specificato nel considerando 64 – la «normativa settoriale non affronta i rischi specifici dei sistemi di IA».

A differenza del Regolamento (UE) 2017/745, la parola *cybersecurity* figura espressamente nell'*AI Act,* in quanto viene menzionata tra le caratteristiche imprescindibili dei sistemi di IA ad alto rischio – assieme all'accuratezza e alla robustezza –, al fine di garantire l'affidabilità dell'IA e di mitigare i pericoli per la salute, la sicurezza e i diritti fondamentali a danno dei pazienti o altri utenti finali del prodotto in questione[102]. Infatti, come recita l'articolo 15 co. 1 dell'*AI Act*, un adeguato livello di accuratezza,

E, pertanto, «al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari processi di prova e di comunicazione nonché le informazioni e la documentazione che forniscono relativamente al loro prodotto nella documentazione e nelle procedure esistenti e richieste in conformità della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A» (art. 8 co. 2). In altri termini, a fronte della flessibilità riconosciuta al fornitore (cfr. considerando 46 e 64), permane l'esigenza di applicare simultaneamente diversi atti legislativi ad un singolo prodotto e di valutarne la conformità. Per questo motivo, in un'ottica di semplificazione, è il Regolamento stesso a stabilire che in tali circostanze il rispetto degli obblighi per i sistemi di IA ad alto rischio possa essere verificato nell'ambito della valutazione della conformità già prevista dalla relativa normativa di settore (cfr. considerando 124). L'articolo 43 co. 3 dell'*AI Act* prescrive, infatti, che «[p]er i sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fornitore segu[a] la pertinente procedura di valutazione della conformità prevista da tali atti giuridici», integrandola con le ulteriori valutazioni richieste dal presente Regolamento per simili sistemi. Nel caso di un dispositivo medico *AI-based,* questo si traduce in procedura per l'immissione in commercio o messa in servizio dove gli organismi notificati competenti in base al MDR saranno chiamati a verificare contemporaneamente anche la conformità del singolo dispositivo alle disposizioni dell'*AI Act,* comprese quelle relative alla cibersicurezza. Se, dunque, l'intenzione (certamente apprezzabile) del legislatore è di evitare eccessivi aggravi a carico dei fabbricanti, a non apparire sufficientemente chiare sono le modalità con cui in concreto dovrebbe realizzarsi questo procedimento semplificato. Alcune incertezze riguardano, per esempio, l'effettiva capacità e competenza degli organismi notificati deputati alla valutazione dei dispositivi medici di farsi carico anche della verifica delle condizioni previste dalla normativa sull'intelligenza artificiale, una volta che questa sarà entrata in vigore e pienamente applicabile. In aggiunta a tali opportuni chiarimenti, sarebbe poi auspicale un intervento del *Medical Device Coordination Group* per definire come i fabbricanti di dispositivi medici *AI-based* si dovranno muovere, dal punto di visto operativo, per realizzare prodotti sicuri e di qualità, rispettando al contempo gli obblighi (talvolta soprapposti) stabiliti a loro carico dalla normativa di settore – il Regolamento (UE) 2017/745 – e dall'*AI Act.* In tale orizzonte, si inserisce un ulteriore elemento utile per assicurare la coerenza tra le diverse normative applicabili, ovvero l'elaborazione di standard armonizzati – e "integrati" – su impulso della Commissione europea riguardanti i requisiti per i sistemi di IA ad alto rischio (Sezione 2, Capo III, dell'*AI Act*). A tal proposito, l'articolo 40 co. 2 dell'*AI Act* specifica infatti che, in questi casi, «le [relative] norme devono essere chiare, coerenti, anche con le norme elaborate nei vari settori per i prodotti disciplinati dalla normativa di armonizzazione dell'Unione vigente elencata nell'allegato I, e volte a garantire che i sistemi di IA o i modelli di IA immessi sul mercato o messi in servizio nell'Unione soddisfino i pertinenti requisiti di cui al presente regolamento».

[102] Infatti, come precisato nel considerando 66, i requisiti obbligatori per i sistemi ad alto rischio – *ivi* compresa la cibersicurezza – «sono necessari per attenuare efficacemente i rischi per la salute, la sicurezza e i diritti fondamentali e, non essendo ragionevolmente disponibili altre misure meno restrittive degli scambi, sono così evitate limitazioni ingiustificate del commercio». Inoltre, il considerando 76 con specifico riferimento alla cibersicurezza afferma che questa «svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza. Gli attacchi informatici contro i sistemi di IA possono far leva sulle risorse specifiche dell'IA, quali i set di dati di addestramento (ad esempio il *data poisoning*, "avvelenamento dei dati") o i modelli addestrati (ad esempio gli *adversarial attacks,* "attacchi antagonisti" o la *membership inference*, "attacchi inferenziali"), o sfruttare le vulnerabilità delle risorse digitali del sistema di IA o dell'infrastruttura TIC sottostante». Pertanto, «[a]l fine di garantire un livello di cibersicurezza adeguato ai rischi, è […] opportuno che i fornitori di sistemi di IA ad alto rischio adottino misure adeguate, come controlli di sicurezza, anche tenendo debitamente conto dell'infrastruttura TIC sottostante».

robustezza e cibersicurezza deve essere integrato e garantito negli *high-risk AI systems* fin dalla progettazione e sviluppo, oltre che preservato durante tutto il loro ciclo di vita[103]. Inoltre, le informazioni circa il grado di precisione, robustezza e cibersicurezza raggiunto dal prodotto a seguito di test e convalida delle sue prestazioni, e ogni circostanza nota o prevedibile capace di determinarne un'alterazione deve essere rivelata agli utenti e contenuta nelle istruzioni d'uso[104].

Sempre in riferimento alla cibersicurezza, l'*AI Act* prevede poi che i sistemi di IA ad alto rischio siano «resilienti ai tentativi di terzi non autorizzati di modificarne l'uso, gli *output* o le prestazioni sfruttando le vulnerabilità del sistema». Per questo motivo, le soluzioni tecniche implementate nel prodotto a garanzia della cibersicurezza devono tenere adeguato conto delle circostanze e dei rischi pertinenti, nonché essere adatte a fronteggiare «le vulnerabilità specifiche dell'IA». Questo significa che – laddove necessario – si debbano prevedere anche «misure volte a prevenire, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare il set di dati di addestramento (*data poisoning*, ossia "avvelenamento dei dati"), gli input progettati in modo da far sì che il modello commetta un errore (*adversarial examples*, ossia "esempi antagonistici", o *model evasion*, ossia "evasione dal modello"), gli attacchi alla riservatezza o i difetti del modello»[105].

3. Conclusioni

La gestione della cibersicurezza in ambito sanitario è una questione complessa in quanto entrano in gioco diverse tipologie di minacce informatiche, oltre che diverse superfici di attacco (o *target*). Come precedentemente illustrato, possono infatti verificarsi – ed in alcuni casi si sono già verificate – incursioni esterne volte a prendere il controllo del sistema informatico di una struttura ospedaliera così da impedire l'ordinario proseguimento delle attività assistenziali e di cura o, ancora, attacchi diretti ad impossessarsi delle informazioni (anche personali) contenute nelle cartelle sanitarie elettroniche oppure a manomettere un'apparecchiatura medicale con potenziali effetti dannosi per l'integrità fisica e la salute del paziente.

[103] Il testo completo prevede quanto segue: «I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita». A tal proposito il considerando 74 afferma che «[l]e prestazioni dei sistemi di IA ad alto rischio dovrebbero essere coerenti durante tutto il loro ciclo di vita e tali sistemi dovrebbero garantire un livello adeguato di accuratezza, robustezza e cibersicurezza, alla luce della loro finalità prevista e conformemente allo stato dell'arte generalmente riconosciuto. […] Il livello atteso delle metriche di prestazione dovrebbe essere dichiarato nelle istruzioni per l'uso che accompagnano il sistema. I fornitori sono invitati a comunicare tali informazioni ai *deployer* in modo chiaro e facilmente comprensibile, senza malintesi o affermazioni fuorvianti».

[104] Cfr. art. 13 co. 3, lett b, ii.

[105] Cfr. art. 15 co. 5 dell'*AI Act.* A norma dell'articolo 42 co. 2 dell'*AI Act,* la conformità ai requisiti di cibersicurezza stabiliti dall'art. 15 può essere presunta nel caso in cui il sistema di IA ad alto rischio sia stato certificato o abbia ottenuto una dichiarazione di conformità ai sensi del *Cybersecuriy Act,* «nella misura in cui tali requisiti siano contemplati nel certificato di cibersicurezza o nella dichiarazione di conformità o in parti di essi». Come specificato dal considerando 122, «ciò lascia [però] impregiudicata la natura volontaria di tale sistema di cibersicurezza».

A fronte di una realtà così eterogenea, la risposta del legislatore (*in primis* europeo) per fronteggiare tale fenomeno sul piano giuridico appare altrettanto frammentata. La strategia messa in atto si compone, infatti, di interventi di portata generale che affrontano il tema della *cybersecurity* con una visuale più ampia (come nel caso del *Cybersecurity Act* o delle Direttive NIS1 e NIS2), e di legislazioni di settore dove invece la cibersicurezza costituisce soltanto uno degli elementi per consentire il raggiungimento dell'obiettivo dell'atto in questione, che esso sia la tutela della riservatezza dei dati personali (*General Data Protection Regulation*), l'affidabilità dei sistemi di IA (*Artificial Intelligence Act*) oppure la sicurezza del dispositivo medico (*Medical Devices Regulation*). Ad emergere con chiarezza da un quadro giuridico così frammentato – o meglio stratificato – è però la direzione intrapresa dall'Unione europea fondata, da un lato, sull'idea che per costruire un sistema sanitario ciberresiliente sia necessario agire su più livelli – da quello individuale (operatori sanitari, pazienti, …), a quello industriale-manifatturiero (fabbricanti di apparecchiature medicali, …), fino all'infrastruttura operativa (ospedale, clinica privata, …) –; e, dall'altro, sulla convinzione che la tutela dei diritti fondamentali non possa prescindere da un'adeguata considerazione della cibersicurezza, dal momento che una falla alla sicurezza di un sistema IT o di un prodotto può avere conseguenze deleterie per la vita, la salute e la riservatezza dei suoi cittadini.
Ed è questo il motivo per cui anche con riferimento a un settore più circoscritto, quale quello biomedicale dei dispositivi medici, l'attenzione ai profili della *cybersecurity* è in crescita, soprattutto per l'avvertita esigenza di stare al passo con il progresso scientifico. Infatti, lo sviluppo di dispositivi sempre più avanzati dal punto di vista tecnologico e maggiormente connessi all'ambiente informatico e digitale circostante rende necessario rafforzare le difese integrate all'interno del dispositivo ma anche ad esso esterne, ovvero relative all'infrastruttura IT di applicazione e agli operatori del singolo *device*. Lo sforzo in questo senso è evidente se si prendono in considerazione le norme stabilite nel Regolamento (UE) 2017/745, dove accanto a requisiti di sicurezza e prestazione per i dispositivi medici tradizionali sono stabilite condizioni aggiuntive per la commercializzazione o la messa in servizio di apparecchiature medicali sofisticate, ovvero quei dispositivi che contengono sistemi elettronici programmabili (compresi i *software*) e per gli *stand-alone software.* In particolare, alla luce delle peculiarità di tali *devices,* sono previste apposite disposizioni che riguardano la sicurezza delle informazioni in essi contenute così come requisiti minimi relativi al contesto operativo in cui il dispositivo è destinato ad essere impiegato, tenendo conto anche del grado di competenza degli utenti finali del prodotto.
Oltre a ciò, il crescente utilizzo dell'intelligenza artificiale nel settore biomedico impone di spostare lo sguardo verso le norme elaborate a livello europeo per regolare tale fenomeno. Infatti, anche se l'*Artificial Intelligence Act* – data la natura orizzontale della proposta – non si occupa in modo specifico delle applicazioni di intelligenza artificiale nell'ambito della salute, si ritiene che molti dispositivi medici di ultima generazione non solo rientreranno nel suo campo di applicazione ma saranno anche classificati come *high-risk AI system*[106].
Questo significa che a seguito della definitiva adozione dell'*AI Act* e della sua entrata in vigore, la disciplina dei dispositivi medici dovrà necessariamente essere integrata con le regole europee in materia di intelligenza artificiale ed in particolare con quelle previste per i sistemi di IA ad alto rischio, comprese le disposizioni – analizzate *supra* – relative alla cibersicurezza. In modo (forse) ancor più chiaro all'in-

[106] Questo aspetto è stato approfondito *infra* (in particolare al paragrafo 2.1).

terno dell'*AI Act* la cibersicurezza si riconferma, dunque, quale caratteristica indispensabile dei prodotti digitali a partire dalle prime fasi di sviluppo e progettazione, in quanto elemento essenziale per garantire adeguata tutela alla salute, alla sicurezza (intesa come *safety*) e ai diritti fondamentali[107].

[107] Quello che resta, invece, da chiarare sono le modalità con cui tale integrazione opererà in concreto (alcune considerazioni sul tema sono accennate al paragrafo precedente).