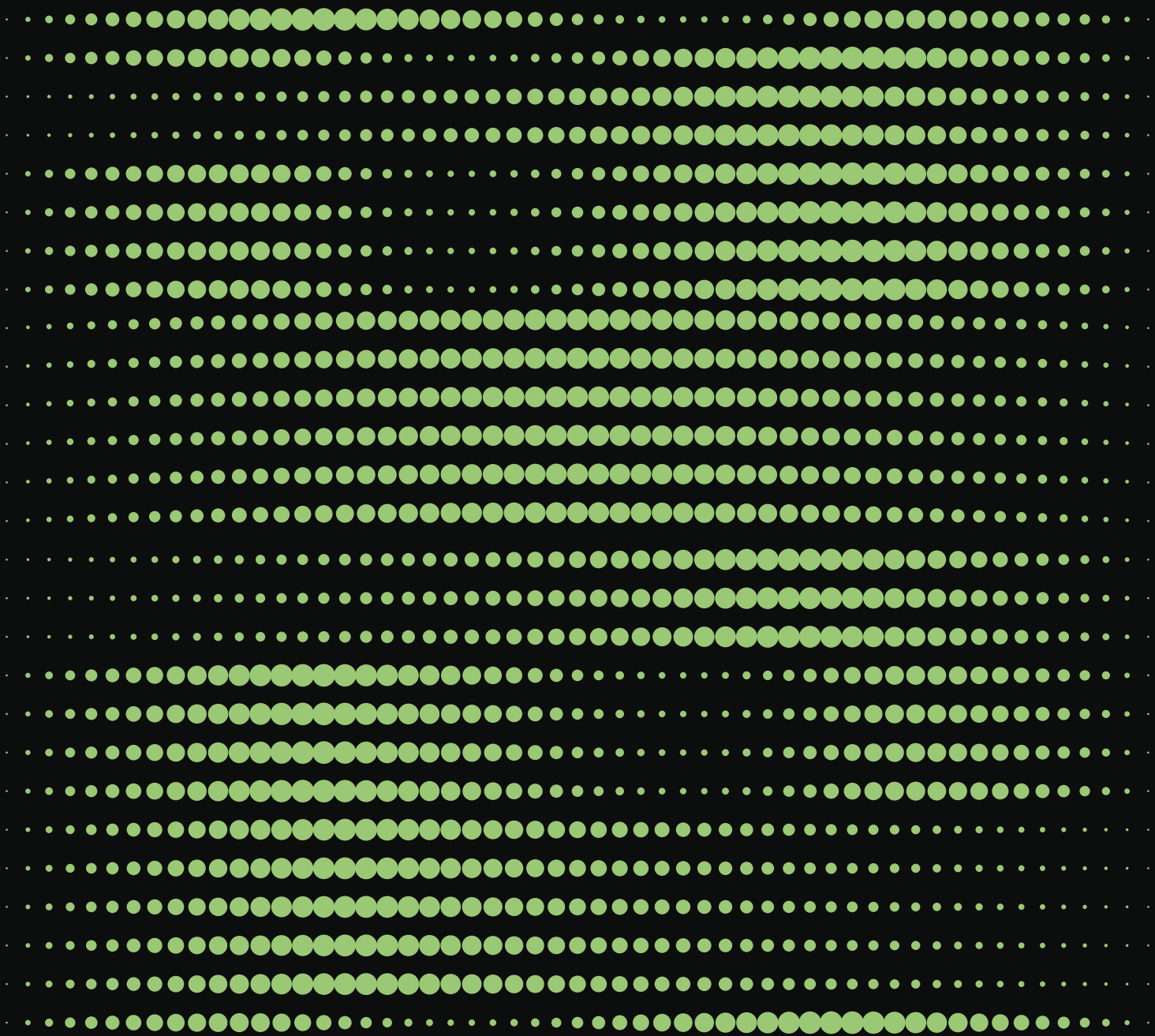
RIVISTA DELLO STATO DIGITALE

02



2025

RIVISTA DELLO **STATO DIGITALE**

02

Pubblicazione scientifica in formato digitale
su informatica e sfera pubblica
ISSN 3103-3768

Numero 2 – Anno 2025

I contributi di questa Rivista sono sottoposti alla valutazione di un revisore in forma anonima (*double blind peer review*), con la sola eccezione della rubrica "Lo Scaffale".

La Rivista si conforma alle linee guida stabilite dalla *Committee on Publication Ethics* (COPE), nel rispetto del Codice etico consultabile in: https://www.rivistastatodigitale.eu

Ogni riflessione e ogni suggerimento sono i benvenuti, nello spirito di una comunità scientifica aperta e partecipata. Per ogni informazione in merito all'invio dei contributi è possibile contattare la Rivista all'indirizzo rsd@irpa.eu

Direttore scientifico
Bruno Carotti

Vicedirettori
Paolo Clarizia, Gianluca Sgueo

Comitato scientifico:
Sabino Cassese, Stefano Battini, Enrico Carloni, Lorenzo Casini, Edoardo Chiti, Sveva del Gatto, Stefano Civitarese Matteucci, Fulvio Costantino, Giovanni Gallone, Barbara Marchetti, Marco Macchia, Bernardo Giorgio Mattarella, Enrico Nardelli, Luigi Previti, Giorgio Resta, Stefano Rossa, Aldo Sandulli, Luisa Torchia, Riccardo Ursi, Giulio Vesperini.

Primo redattore - Coordinamento editoriale
Gianluca Buttarelli

Comitato di redazione
Alessia Madeddu, Alessandra Mattoscio, Agostino Sola, Giulia Taraborrelli

IRPA | ISTITUTO DI RICERCHE SULLA PUBBLICA AMMINISTRAZIONE
Piazza Venezia, 11 - Roma

Roma, febbraio 2026

Pubblicata con licenza Creative Commons CC BY 4.0., che richiede l'attribuzione dell'opera. Per conoscere I termini d'uso, si può vistare il sito: https://creativecommons.org/licenses/by/4.0/

Progetto grafico: **Nuvola Studio**

Sommario

Spunti in tema di cybersicurezza ed ecosistemi digitali: il caso della telemedicina

Stefano Rossa*

Abstract

L'elaborato indaga la relazione che intercorre fra cybersicurezza ed ecosistemi digitali, analizzando in particolare l'ambito della telemedicina. Dopo averne sommariamente ricostruito la disciplina giuridica, l'articolo si sofferma sulla bassa percezione degli effetti reali causati dalle azioni virtuali poste in essere nel cyberspazio, in grado di colpire e danneggiare gli ecosistemi digitali, interrogandosi se ciò sia la conseguenza della condizione di a-territorialità fisica, immateriale, insita nello stesso concetto di *cyberspace*. Nella parte conclusiva lo scritto, evidenziando gli sforzi delle Istituzioni pubbliche nazionali nel 'territorializzare' il cyberspazio, sottolinea l'esigenza di adottare pratiche di educazione alla cybersicurezza, basate sull'approccio collaborativo, che pongano l'accento sulla dimensione fisico-territoriale delle azioni virtuali, onde poter aumentare il livello di protezione cibernetica degli ecosistemi digitali.

Sommario

1. Introduzione. Rischio cyber ed ecosistemi digitali

Risale a fine settembre 2025 la notizia relativa all'arresto di un presunto *hacker*, accusato dalla polizia britannica di aver effettuato attacchi *ransomware*[1] ai danni della rete digitale della Collins Aerospace, società statunitense che gestisce le procedure di *check-in* in molti aeroporti mondiali, causando malfunzionamenti e disagi in tutta l'Unione europea[2].
Lo scorso anno, invece, è circolata la notizia

* Ricercatore a t.d. in Tenure Track di Diritto amministrativo e Pubblico nell'Università degli Studi del Piemonte Orientale (stefano.rossa@uniupo.it). Il presente contributo è realizzato nell'ambito del progetto "Cybersecurity Risk Governance in Public Administration – CybeR-GoPA" (ID: 1083758, CUP: C15F21001720001), finanziato dal Bando Ricerca UPO 2022 a valere su risorse Next Generation EU e Compagnia di San Paolo.

1 Per un inquadramento tecnico di questa tipologia di *malware* si rimanda a ACN-CSIRT, *Ransomware. Caratteristiche, preparazione e risposta agli attacchi ransomware*, Roma, 19 dicembre 2024, p. 6-7. Per una ricostruzione di questo lemma e di altri termini tecnici, in chiave giuridica, si rimanda a *Breviario giuridico della cybersicurezza*, a cura di A. Simoncini, M. Pietrangelo, CNR Edizioni, Roma, 2025.

2 Si v. *Attacco hacker agli aeroporti europei, arrestato a Londra un 40enne*, in *Rainews.it*, 24 settembre 2025 (in https://s.uniupo.it/12ue0).

dell'arresto di Julius Kivimäki, *hacker* finlandese conosciuto con il soprannome di Zeekill e accusato di aver rubato *terabyte* di dati clinici (per lo più di sedute psicoterapiche) di circa trentamila persone, che ha ricattato chiedendo loro denaro in cambio della non diffusione di tali dati del *deepweb*[3]. Molte di queste persone, non potendo pagare e temendo la divulgazione di tali dati, si sono suicidate.

Indipendentemente dai numerosi e differenti motivi che spingono gli *hacker* ad agire – ragioni criminali (es. a scopo estorsivo), politiche (es. delegittimazione dell'avversario), militari (es. guerra ibrida) – questi due esempi consentono di constatare un fatto: all'avanzare del processo di digitalizzazione aumenta proporzionalmente il potere di quei soggetti dotati delle più alte competenze tecnico-informatiche, le quali consentono loro di 'surfare' l'onda tecnologica. Se questo processo ha caratterizzato ogni era tecnologica[4], esso però risulta assai più marcato nella società digitale.

Di contro, questa circostanza interessa altresì quei soggetti che non possiedono tali capacità tecniche e che, anziché 'surfare' l'onda tecnologica, vengono da essa travolti. Questi soggetti – fra cui spiccano quelli pubblici – sono però giocoforza obbligati ad affrontare l'onda e, trovandosene travolti, fanno di tutto per non 'affogare'. Essi, infatti, devono ottemperare alle numerose norme settoriali in materia – riservatezza, trasparenza, accesso, digitalizzazione – adattando la propria organizzazione e la propria azione a dinamiche ed esigenze in continua accelerazione e spesso avendo a disposizione poche figure tecniche esperte[5].

In tale contesto, le istituzioni pubbliche devono affrontare e gestire il cd. 'rischio da ignoto tecnologico'[6] dando ai cittadini risposte concrete ed effettive. E nel far ciò devono tenere in considerazione la circostanza per cui al concetto di società (inteso in senso ampio) oggi tende ad affiancarsi (e parzialmente sovrapporsi a) quello di ecosistema digitale, intendendosi con tale perifrasi quella «comunità di soggetti che collaborano e si sviluppano grazie ad interazioni digitali»[7]. Interazioni che sorgono e si sviluppano in un contesto virtuale connotato da assenza di una dimensione territoriale e fisica. Un elemento che, come ivi si cercherà di mettere in evidenza, condiziona in modo significativo le risposte che le istituzioni sono chiamate a intraprendere per fronteggiare le sfide che sorgono negli ecosistemi digitali.

Richiamando la figura retorica precedentemente impiegata, il divario fra 'chi surfa' e 'chi cade dalla tavola' si traduce in alcune circostanze, fra cui nel fatto che i primi riescono con facilità ad accedere e a esfiltrare enormi moli di dati riservati che i secondi producono o gestiscono.

---

3 Si v. J. Tidy, *From teenage cyber-thug to Europe's most wanted*, in *BBC.com*, 5 maggio 2024 (in https://s.uniupo.it/p8cwx).

4 Per una storia dello sviluppo tecnologico si veda C. Singer, E.J. Holmyard, A. R. Hall, T. I. Williams, *A History of Technology*, I-VIII, Oxford, Clarendon Press, 1954.

5 Sul punto si pensi alle responsabilità in capo al referente per la *cybersicurezza* nella pubblica amministrazione (*recte*: in alcune pubbliche amministrazioni), figura istituita dalla legge n. 90 del 2024 a finanza invariata. Sul punto si rimanda a L. Previti, *La nuova legge sulla cybersicurezza, un passo avanti e due indietro*, in *Giornale di dir*itto amministrativo, 2025, p. 60.

6 Sia consentito il riferimento a S. Rossa, *La necessità dell'indagine scientifica nel contesto del "rischio da ignoto tecnologico": il caso della* cybersecurity*, fra multidisciplinarietà e approcci sinergici. Prefazione*, in *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, fascicolo I, a cura di G. Bombelli, S. Rossa, in *Teoria e Critica della Regolazione Sociale,* 2024, n. 2, Milano, Mimesis, 2025, p. 7 ss.

7 A. Fuggetta, *Ecosistemi digitali e imprese: come coltivare la cultura dell'innovazione*, in *Agenda Digitale*, 25 marzo 2024.

E questo avviene in particolare nel settore sanitario, come ha esplicitamente evidenziato il recente report dell'Agenzia per la Cybersicurezza Nazionale intitolato *La minaccia cibernetica al settore sanitario*[8]. Secondo questo documento «[s]ul territorio nazionale, a partire da gennaio 2023 si sono verificati mediamente 4,3 eventi cyber malevoli al mese ai danni di strutture sanitarie, dei quali la metà circa ha dato luogo a "incidenti", ovvero ha avuto un impatto effettivo sui servizi sanitari erogati»[9]. Eventi cyber malevoli la cui causa è principalmente riconducibile alla cattiva implementazione di pratiche di sicurezza (anche elementari), alla «scarsa attenzione agli aspetti di sicurezza connessi alla gestione di sistemi digitali, o [alla] carente formazione specifica sulla cybersicurezza del personale impiegato in ospedali, centri medici, cliniche e altre strutture sanitarie»[10]. Una situazione che emerge con chiarezza da due dati lapalissiani: la maggior parte degli attacchi subiti hanno natura di *ransomware* (46% nel 2023 e 17% nel 2024)[11] e una significativa parte degli incidenti cyber è stata il frutto di diffusione di *malware* tramite e-mail (11%)[12].

In un contesto come quello attuale, post pandemico, proprio la telemedicina[13] rappresenta un esempio emblematico di ecosistema digitale *in fieri*: il diritto alla salute –nella sua dimensione di diritto individuale quanto in quella di diritto sociale[14] – è sempre più condizionato da ciò che accade nel cyberspazio. Sia, come pare intuitivo, in relazione ai profili più operativi di cybersicurezza[15], che impongono la protezione delle pratiche di teleme-

8 ACN, *La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni – gennaio 2023-settembre 2025*, 31 ottobre 2025 (in https://s.uniupo.it/gs6b9).

9 ACN, *La minaccia cibernetica al settore sanitario*, *cit.*, p. 5.

10 *Ibidem*.

11 ACN, *La minaccia cibernetica al settore sanitario*, *cit.*, p. 11.

12 *Ibidem*.

13 Fra i numerosi contributi su questo argomento, *ex multis* si vedano F. Cimbali, *La governance della sanità digitale*, Milano, Wolters Kluwer, 2023; S. Samo, *La telemedicina alla luce dell'avvento della robotica e dell'Intelligenza Artificiale*, in *Federalismi.it*, 2025, n. 20, p. 227 ss.; M. Matassa, *Colmare i divari. Come le nuove tecnologie promettono di rivoluzionare la sanità italiana*, in *Federalismi.it*, 2025, n. 12, p. 162 ss.; C. Nicolosi, *Telemedicina, PNRR e Piani di rientro sanitari: uniformità versus autonomia dell'organizzazione sanitaria?*, in *Amministrativamente*, 2024, p. 1042 ss.; V. Molaschi, *Telemedicine: Impact and Perspectives in Healthcare Delivery and Organization of the Italian National Health Service*, in *European Review of Digital Administration & Law - Erdal*, 2023, n. 1, p. 153 ss.; F. Aperio Bella, *The Role of Law in Preventing "Remote" Defensive Medicine: Challenges and Perspectives in the Use of Telemedicine*, in *Federalismi.it*, 2023, n. 1, p. 305 ss.; A. Mazza Laboccetta, *Telemedicina: sfide, problemi, opportunità*, in *Federalismi.it*, 2023, n. 22, p. 135 ss.; M. D'Arienzo, *La trasformazione digitale della sanità tra problemi organizzativi e profili di responsabilità professionale*, in *Dir. econ.*, 2022, n. 1, p. 135 ss.; E. Catelani, *Nuove tecnologie e tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain*, in *Federalismi.it*, 2021, n. 4, p. 212 ss.; N. Posteraro, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza*), in *Federalismi.it*, 2021, n. 26, p. 189 ss.; M. Campagna, *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid*, in *Corti supreme e salute*, 2020, n. 3, p. 599 ss.; C. Botrugno, *Telemedicina ed emergenza sanitaria: un grande rimpianto per il nostro Paese*, in *Rivista di Biodiritto*, 2020, n. 1S, p. 691 ss.

14 *Ex multis* R. Balduzzi, *Salute (diritto alla)*, in *Dizionario di diritto pubblico*, a cura di S. Cassese, VI, Milano, Giuffrè, 2006, p. 5394 ss.

15 In argomento, a titolo non esaustivo, si vedano *La sicurezza nel cyberspazio*, a cura di R. Ursi, Milano, Franco Angeli, 2023; E. Buoso, *Potere amministrativo e sicurezza nazionale cibernetica*, Torino, Giappichelli, 2023; M. Macchia, G. Sferrazzo, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, in *Dir. amm.*, 2025, p. 109 ss.; T.F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quad. cost.*, 2024, n. 2, p. 277 ss.; A. Contaldo, *La funzione di "public cybersecuirty" come preminente funzione pubblica digitale alla luce della direttiva NIS2*, in *Medialaws*, 2024, n. 3, p. 184 ss.; E. Longo, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in *Rass. parlam.*, 2024, n. 2 p. 313 ss.; L. Previti, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *federalismi.it*, 2022, n. 25, p. 65 ss.; B. Carotti, *Sicurezza cibernetica e Stato-nazione*, in *Giornale di diritto amministrativo*, 2020, n. 5, p. 629 ss. Più recentemente M. Matassa, *La sicurezza cibernetica come funzione pubblica*, Milano, Franco Angeli, 2025. Sia consentito il richiamo a S. Rossa, *Cybersicurezza e pubblica am-*

dicina da cyber attacchi e incidenti[16]; sia agli aspetti maggiormente teorici legati alle caratteristiche intrinseche dello stesso *cyberspace* – fra cui, appunto, l'assenza di una dimensione territoriale e fisica – in grado di condizionare il comportamento dei vari attori che ivi agiscono.

2. Cybersicurezza e telemedicina, quale esempio di ecosistema digitale

Senza l'intenzione di ricostruirne la disciplina giuridica, rimandando sul punto agli studi della dottrina[17], appare tuttavia evidente che la telemedicina abbia acquisito fondamentale centralità nell'ordinamento, come testimonia la Missione 6 del Piano Nazionale di Ripresa e Resilienza[18]. Circostanza che comporta la conseguente necessità di adozione di misure di cybersicurezza a sua protezione.

Tale considerazione viene in rilievo altresì a fronte dei concreti vantaggi pratici che questo processo di digitalizzazione apporta al contesto sanitario e che hanno condotto a una sua rapida adozione.

Si pensi, ad esempio, alla maggior facilità con cui è possibile predisporre misure di medicina personalizzata, in cui il rapporto medico-paziente è incentrato sullo specifico individuo, visto come persona prima ancora che come paziente (come previsto anche dal Patto per la Salute 2019-2021)[19]. In tal senso, i servizi tecnologici sanitari possono costituire strumenti concreti per rendere tale relazione di cura più efficace, in quanto sartoriale, proprio grazie alle ICT. E, conseguentemente, contribuire a ridurre comportamenti ascrivibili alla cd. medicina difensiva[20].

Oppure si pensi, altresì, all'azione di rafforzamento della sanità territoriale[21] che la telemedicina è in grado di realizzare. Il Decreto del Ministero della Salute del 23 maggio 2022, n. 77[22], noto come DM 71, nel dettare standard attuativi dei LEA definisce espressamente i servizi di telemedicina[23] «un'opportunità e un fattore abilitante la strutturazione di modelli di gestione integrata dell'assistenza sanitaria e socio-sanitaria a rilevanza sanitaria, in grado di rispondere [...] alle necessità

ministrazione, Napoli, Editoriale Scientifica, 2023.

16 Su questo argomento sia consentito il rimando a S. Rossa, *Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario*, in *Vergentis. Revista de Investigación de la Cátedra Internacional conjunta Inocencio III*, 2023, n. 17, p. 161 ss.

17 Si rimanda alla nota n. 13.

18 Si v. *Piano nazionale di ripresa e resilienza*, Missione 6 Componente 1 («Reti di prossimità, strutture intermedie e telemedicina per l'assistenza sanitaria territoriale») e Missione 6 Componente 2 («Innovazione, ricerca e digitalizzazione del servizio sanitario nazionale»), 2021, p. 225 ss.

19 *Patto per la Salute 2019-2021*, approvato il 18 dicembre 2019 in sede di Conferenza Permanente per i rapporti fra Stato, Regioni e Province Autonome di Trento e Bolzano.

20 In argomento si veda l'analisi di R. Balduzzi, *La medicina difensiva come ostacolo alla difesa della salute*, in *Diritto e medicina. Un'ipotesi di dialogo fra le scienze*, a cura di R. Lombardi, F. Santini, Torino, Giappichelli, 2021, p. 49 ss. Per alcune riflessioni circa la medicina difensiva quale espressione di burocrazia difensiva si rimanda a F. Aperio Bella, *Defensive Medicine and Defensive Bureaucracy*, in *Rivista trimestrale di scienza dell'amministrazione*, 2023, n. 3, p. 2 ss.

21 In argomento si veda R. Ferrara, *L'ordinamento della sanità*, Torino, Giappichelli, 2025, p. 121 ss.

22 Decreto del Ministero della Salute del 23 maggio 2022, n. 77, rubricato *Regolamento recante la definizione di modelli e standard per lo sviluppo dell'assistenza territoriale nel Servizio sanitario nazionale*.

23 Fra cui, a titolo non esaustivo, l'All. 1 punto 15 del Decreto del Ministero della Salute del 23 maggio 2022, n. 77 elenca la televisita specialistica, la teleassistenza, il telemonitoraggio, la teleriabilitazione, il teleconsulto medico, la teleconsulenza medico sanitaria e la telerefertazione.

dei sistemi sanitari»[24]. Più nel dettaglio, il DM 71 prevede, da un lato, che l'Unità di Continuità Assistenziale agisca sul territorio di riferimento ricorrendo altresì a strumenti digitali di telemedicina (si pensi alla televisita o al teleconsulto, in grado di costituire un ausilio a distanza di specialisti operanti in differenti strutture ospedaliero-sanitarie)[25]. Dall'altro lato, il Decreto stabilisce che all'interno degli Ospedali di Comunità il monitoraggio dei pazienti possa avvenire altresì tramite servizi di telemedicina[26].

Ed è proprio il DM 71 a descrivere la telemedicina come un fattore «abilitante per l'attuazione della riorganizzazione dell'assistenza territoriale»[27]. Questo poiché la telemedicina riduce la distanza temporale e spaziale dell'azione medica 'classica' (analogica), nell'ottica del buon andamento *ex* art. 97 Cost. e dei suoi corollari di efficienza, efficacia ed economicità. Essa, infatti, non soltanto consente potenzialmente di eliminare la distanza fisica che si pone fra l'operatore sanitario e il paziente: emblematica è la possibilità che la tecnologia offre ai chirurghi di effettuare interventi da remoto, operando pazienti a chilometri di distanza[28]. Ma la telemedicina permette altresì di anticipare sul piano cronologico le cure, come nell'ipotesi di visite effettuate digitalmente dall'équipe ospedaliera sul mezzo di trasporto d'emergenza diretto all'ospedale[29].

La telemedicina pone, dunque, un importante tema di (ri)organizzazione amministrativa – con significativi impatti in materia di cybersicurezza. Tanto in relazione al rafforzamento della medicina territoriale e al suo rapporto con la centralizzazione delle prestazioni, quanto, e soprattutto, in riferimento alle azioni che le organizzazioni sanitarie devono predisporre per adattare la propria struttura interna (e i propri macro-processi) alle sfide che il processo di digitalizzazione pone ai poteri pubblici[30] – come del resto già messo in luce da Giannini negli anni '80[31]. Dato che i sistemi di telemedicina 'traslano' sul digitale l'attività sanitaria analogica (o buona parte di essa), risulta allora intuitivo come la digitalizzazione ponga *in primis* la necessità di adeguare l'organizzazione affinché essa risulti essere cyber-resiliente e cyber-sicura. Necessità di cui le Istituzioni sono consapevoli.

L'attenzione ai profili di cybersicurezza nella telemedicina, infatti, prima ancora che nella disciplina specifica di settore, emerge dalle *Indicazioni nazionali per l'erogazione di prestazioni in telemedicina*[32] del 2020, in base alle quali le prestazioni e i servizi di telemedicina sono assimilati a qualunque altra prestazione e servizi diagnostici, terapeutici ed assistenziali; per tale motivo i diritti e gli obblighi

24 Decreto del Ministero della Salute del 23 maggio 2022, n. 77, Allegato 1, punto 15.

25 Si v. Decreto del Ministero della Salute del 23 maggio 2022, n. 77, All. 1, punto 7.

26 Si v. Decreto del Ministero della Salute del 23 maggio 2022, n. 77, All. 1, punto 11.

27 Decreto del Ministero della Salute del 23 maggio 2022, n. 77, All. 1, punto 15.

28 Si v. G. Di Bisceglie, *Bari, Il paziente è a Bari, il medico a Dubai: al Policlinico la prima operazione di telechirurgia intercontinentale grazie al 5G*, in *Corriere della Sera – Corriere del Mezzogiorno, Bari*, 20 aprile 2024 (in https://s.uniupo.it/31vy8).

29 Sul punto si veda la notizia *Dall'ambulanza del futuro all'Intelligenza artificiale: le tecnologie per la sanità a Welfair 2024. IA, telemedicina e domotica: l'hi-tech invade la sanità*, in *Rai News.it*, 4 novembre 2024 (in https://s.uniupo.it/n8ev5).

30 Sul tema *ex multis* R. Cavallo Perin, D.-U. Galetta, *Il Diritto dell'Amministrazione Pubblica digitale*, Torino, Giappichelli, 2025; L. Torchia, *Lo Stato digitale. Una introduzione*, Bologna, Il Mulino, 2025.

31 Si v. M.S. Giannini, *Rapporto sui principali problemi dell'amministrazione dello Stato*, in *Foro Amm.*, 1979, p. 2667 ss.; nonché Id., *Il pubblico potere. Stati e amministrazioni pubbliche*, Bologna, Il Mulino, 1986, p. 140.

32 *Indicazioni nazionali per l'erogazione di prestazioni in telemedicina*, approvate in Conferenza Stato-Regioni il 17 dicembre 2020.

derivanti da un 'atto sanitario digitale' devono essere i medesimi di un 'atto sanitario analogico'; va da sé, dunque, che le caratteristiche di protezione, confidenzialità e riservatezza dei dati sanitari, tipiche del rapporto che si instaura fra medico e paziente, devono essere assolutamente garantite a prescindere dal tipo di mezzo impiegato[33]. Circostanza che, d'altra parte, risulta ancora più necessaria a seguito delle previsioni stabilite dalla recente legge italiana sull'intelligenza artificiale (legge n. 132 del 2025), la quale ha disciplinato l'impiego di questi sistemi automatizzati nell'ambito sanitario, i quali, in tal modo, potranno rafforzare significativamente le pratiche di telemedicina[34].

Senza intenzione di analizzare la disciplina normativa in materia, basti ivi menzionare che il *corpus* principale di riferimento della cybersicurezza è rappresentato dalla Direttiva (UE) 2022/2555[35] (cd. Direttiva NIS 2) che – pare utile anticipare – si applica anche al settore sanitario. Questa direttiva mira a realizzare un elevato livello europeo comune di resilienza e risposta agli attacchi cyber, prevedendo in capo ai soggetti destinatari ultimi un intricato sistema di valutazione e gestione del rischio cyber, anche a livello di catena di fornitura, l'imposizione di requisiti di cybersicurezza e la segnalazione di cyber-incidenti al CSIRT Italia/ACN.

Come noto, la Direttiva NIS 2 ha abrogato la Direttiva NIS (1)[36] e ha fatto venire meno la precedente distinzione fra «operatori di servizi essenziali»[37] e «fornitori di servizi digitali»[38]: la Direttiva NIS 2 ha infatti previsto che i destinatari dei menzionati obblighi siano tutti i soggetti rientranti in due ampie categorie[39]: i «soggetti essenziali», i quali operano nei settori ad alta criticità[40], e i «soggetti importanti», i quali invece operano negli altri settori critici[41]. Classificazione che ben evidenzia come nell'ambito della cybersicurezza, prima ancora che la natura (pubblica o privata) dei soggetti potenziali bersaglio, rilevi la centralità dell'attività che verrebbe compromessa, interrotta o impedita dall'attacco in relazione al corretto funzionamento del sistema democratico[42]. E fra i settori ad alta criticità è infatti ricompreso quello sanitario[43], con la conseguenza che gli obblighi previsti dalla Direttiva NIS 2 si pongono anche in capo alle strutture sanitarie.

Gli sforzi imposti dalla menzionata direttiva si sostanziano (principalmente, ma non solo) in misure di natura organizzativa, come del resto suggerisce l'etimologia stessa del lemma 'cybersicurezza'[44]. Sotto questo profilo, le sfide

33 Per approfondimenti legati al tema della gestione dei dati, si vedano B. Ponti, *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, Milano, Franco Angeli, 2023; S. Franca, *I dati personali nell'amministrazione pubblica*, Napoli, Editoriale Scientifica, 2023.

34 Si veda in particolare art. 7, legge n. 132 del 2025.

35 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14/12/2022.

36 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 06/07/2016.

37 Si v. Direttiva (UE) 2016/1148, Capo IV.

38 Si v. Direttiva (UE) 2016/1148, Capo V.

39 Si v. art. 3 Direttiva (UE) 2022/2555.

40 Si v. All. 1 Direttiva (UE) 2022/2555.

41 Si v. All. 2 Direttiva (UE) 2022/2555.

42 Rilevando, come si ha avuto già modo di sottolineare, «l'interesse pubblico oggetto dell'attacco»: si v. S. Rossa, *Cybersicurezza e Pubblica Amministrazione*, *cit.*, p. 17.

43 Oltre a quelli di energia, trasporti, settore bancario, mercati finanziari, spazio, Pubblica amministrazione, gestione dei servizi TIC, infrastrutture digitali e acque potabili e reflue.

44 In proposito si rimanda alle riflessioni esposte in S. Rossa, *Cybersicurezza e Pubblica Amministrazione*, *cit.*, p. 12-13.

lanciate dalla cybersicurezza al settore sanitario permettono di cogliere – probabilmente più che in altri ambiti – come la funzione d'organizzazione della pubblica amministrazione non sia solo volta a stabilirne il mero «disegno preordinato di uffici, e di relative attribuzioni»[45], ma risulti soprattutto uno strumento concreto per garantire i diritti dei cittadini[46].

3. Telemedicina e bassa percezione del rischio cyber: quale relazione con il concetto di 'cyberspazio'?

L'adeguamento dell'organizzazione sanitaria al rischio cyber si scontra quantomeno con due ordini di problemi: da un lato, quello relativo alle risorse finanziarie necessarie a predisporre tale adeguamento – sul quale non ci si soffermerà; dall'altro, quello attinente alla circostanza per la quale piccole e inconsapevoli azioni dei singoli possono avere a valanga effetti devastanti sull'intera organizzazione.

Proprio questo ultimo elemento è già emerso in precedenza *en passant* allorquando si è fatto riferimento ai dati riportati da ACN in relazione alle cause di attacchi cyber nel settore sanitario legate alla mala implementazione di pratiche di cybersicurezza (anche elementari)[47]. D'altronde, è ormai un caso assai noto l'attacco cyber che ha coinvolto nell'estate 2021 la Regione Lazio, partito dall'azione di un dipendente e che ha portato al blocco dei servizi sanitari regionali – per di più durante le fasi più acute della pandemia da Covid-19[48].

Secondo alcune ricerche sulla comunicazione, il linguaggio e la psicologia, un problema dell'uso degli strumenti digitali è legato al fatto per cui le persone che li utilizzano non sempre hanno piena consapevolezza degli effetti reali delle proprie azioni virtuali. Si pensi alla facilità con cui gli utenti dei *social media* sono portati a scrivere commenti e insulti sulle piattaforme, mentre nella vita reale con difficoltà agirebbero in tal modo[49]. Sotto questo profilo, emerge come il contesto dell'ambiente digitale contribuisca a determinare una deresponsabilizzazione di specifici comportamenti[50]. Ciò anche in virtù, come anticipato, dell'assenza di una dimensione fisico-territoriale in grado di far percepire il nesso di causalità fra l'azione (virtuale) posta in essere e la conseguenza (reale) realizzatasi.

Analogamente, tale situazione si ritrova altresì nel più ampio contesto della cybersicurezza, il cui concetto, come noto, discende da quello di 'cyberspazio'. Il quale è «per definizione un non-luogo»[51] fisicamente inteso,

45 M.S. Giannini, *Gli elementi degli ordinamenti giuridici*, in *Rivista trimestrale di diritto pubblico*, 1958, p. 237.

46 Si v. V. Bachelet, *Profili giuridici della organizzazione amministrativa. Strutture tradizionali e tendenze nuove*, Milano, Giuffrè, 1965, p. 3.

47 Si rimanda alle note 8,9,10.

48 Per una ricostruzione della vicenda, e delle relative sanzioni irrogate successivamente dal Garante della privacy, si rimanda all'articolo *Attacco hacker ai sistemi informatici del Lazio nel 2021. Garante Privacy sanziona LazioCrea, Regione e Asl RM 3*, in *Quotidiano Sanità*, 10/04/2024 (in https://s.uniupo.it/rh2af).

49 Si v. E. Menon, *Dibattere sui social. Come domare i leoni da tastiera*, Università degli Studi di Padova – Tesi di laurea, A.A. 2020/2021 p. 90.

50 Aspetto evidente in relazione ai casi di odio *online*, come sottolineato da L. Bova, *Il conflitto tra l'odio e l'empatia nell'essere umano*, Università degli Studi di Padova – Tesi di laurea, A.A. 2023/2024, p. 11.

51 I. Forgione, *Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzione, fra regolazione europea e interna*, in *Dir. amm.*, 2022, p. 113.

immateriale[52] e privo di confini territoriali[53].
Poiché, come insegna il Vangelo, l'uomo è portato a credere e percepire come reale soltanto quello che può 'toccare con mano'[54], ci si potrebbe interrogare se la condizione di 'a-territorialità fisica', insita nel concetto di cyberspazio, possa contribuire a far percepire come fortemente ridotto – se non, in taluni casi, addirittura assente – il senso del rischio cibernetico. Rischio che, a ben considerare, non solo non è venuto meno, ma al contrario pare essere aumentato proprio in conseguenza della sua sottovalutazione, in particolare in quei contesti, quale la sanità, caratterizzati dal perseguimento di esigenze primarie (nel caso specifico: curare i pazienti) che potrebbero indurre a considerare non strettamente prioritarie l'implementazione di pratiche di cybersicurezza.

4. Riflessioni conclusive. La consapevolezza della dimensione fisico-territoriale del cyberspazio come precondizione di cybersicurezza degli ecosistemi digitali

Ipotizzando una risposta positiva all'interrogativo poc'anzi posto, in conseguenza degli effetti reali di azioni malevoli poste in essere nel *cyberspace*, potrebbe essere allora utile riflettere sulla dimensione intrinsecamente fisica del cyberspazio. Dimensione che emerge dagli esiti concreti di condotte virtuali compiute in questo non-luogo fisico per eccellenza, in grado di arrecare danni a persone e cose, oltre alle reti digitali stesse. Come è stato affermato in dottrina, secondo questa prospettiva il cyberspazio potrebbe essere allora visto come «bene giuridico tutelato dalla sicurezza informatica in via soltanto mediata e indiretta, in quanto il fin ultimo perseguito dall'attività pubblica si ravvisa nella protezione delle persone e dei beni del mondo reale messi in pericolo dalla minaccia cibernetica»[55].
D'altronde, condividendo questa interpretazione, non si può non osservare come molte categorie giuridiche 'classiche' scricchiolino innanzi alle questioni legate alla cybersicurezza[56]. E fra esse quella della territorialità[57] – centrale per il diritto pubblico[58] in quanto elemento concettuale su cui si basa la legittimazione statuale.

52 Così la voce *Cyberspazio*, in *Breviario giuridico della cybersicurezza*, a cura di A. Simoncini, M. Pietrangelo, *cit.*, 76 ss. In tal senso anche F. Serini, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?*, in *MediaLaws*, 2023, n. 3, p. 147, il quale però, richiamando la letteratura straniera, fa come notare la difficoltà di definire in modo univoco il concetto di cyberspazio, potendo in esso intravvedersi anche una dimensione strettamente materiale legata alla componentistica *hardware* alla base delle infrastrutture digitali che ne permettono il funzionamento.

53 Come sottolinea M. Matassa, *La sicurezza cibernetica come funzione pubblica*, *cit.*, p. 53, nota 109, questa impostazione si lega, e discende, dai dibattiti sulla natura di luogo (o meno) di Internet, come già emerso in M. Augé, *Non-lieux. Introduction à une anthropologie de la surmodernité*, Seuille, 1992.

54 Si v. Giovanni 20:25-27.

55 M. Matassa, *La sicurezza cibernetica come funzione pubblica*, *cit.*, p. 54, il quale evidenzia come già L. Denardis, *The Internet in Everything. Freedom and security in a world with no off switch*, New Haven, Yale University Press, 2020, p. 93 ss. avesse coniato a riguardo l'espressione «*cyber-physical security*».

56 In tal senso anche R. Ursi, *Introduzione. La sicurezza cibernetica come funzione pubblica*, in *Cybersecurity e Istituzioni democratiche. Un'indagine interdisciplinare: diritto, informatica e organizzazione aziendale*, fascicolo II, a cura di P. Heritier, S. Rossa, in *Teoria e Critica della Regolazione Sociale,* 2025, n.1, Milano, Mimesis, 2025, p. 10.

57 Così F. Castaldo, F. Serini, *Public-private collaboration in European cybersecurity. Between organizational and regulatory plans*, in, *Cybersecurity e Istituzioni democratiche*, *cit.*, a cura di G. Bombelli, S. Rossa, pp. 177-178. Sul punto anche M. Matassa, *La sicurezza cibernetica come funzione pubblica*, *cit.*, p. 18 ss.

58 Obbligatori i rimandi a G. Jellinek, *Allgemeine Staatslehre*, Berlino-Heidelberg, Springer Verlag, 1921 e a C. Schmitt, *Der Nomos der Erde im Völkerrecht des Jus Publicum Europaeum*, Berlino, Duncker & Humblot, 1950. Più recente-

A tal proposito pare utile richiamare la definizione che Luciano Floridi ha coniato per descrivere l'attuale società: l'*onlife*[59]. In essa, infatti, non vi è più una netta distinzione fra *online* e *offline* poiché queste due dimensioni sono ormai fuse e le azioni in una dimensione si ripercuotono inevitabilmente sull'altra. Questa costruzione teorica, peraltro, trova riscontro in fatti di cronaca ancora una volta legati all'ambito sanitario, come quello accaduto in Germania nel 2020 in cui per la prima volta un attacco cyber diretto a un ospedale ha causato la morte di una paziente[60].

Il paradigma vestfaliano, legato a doppio filo al concetto di sovranità-territorialità (fisica), si scontra con le sfide poste dalla tecnologia, cybersicurezza *in primis*[61]. Un settore, come è stato scritto, «in costante movimento e in cerca della propria identità»[62]. Con la conseguenza che «[d]i questo percorso risentono le istituzioni che lo governano»[63]. A ben riflettere, tuttavia, gli sforzi delle Istituzioni pubbliche – specialmente nazionali – sono indirizzati a recuperare una sorta di «*area di territorializzazione effettuale*»[64] del cyberspazio, che consenta agli Stati di esercitare al meglio la funzione di sicurezza cibernetica proprio grazie al recupero della dimensione nazionale entro cui esercitarla. Aspetto che del resto emerge plasticamente dalla disciplina italiana del Perimetro di sicurezza nazionale cibernetica[65], la quale si pone nel solco della «difesa del "fortino" tecnologico»[66] che protegge gli interessi pubblici da attacchi esterni provenienti dal cyberspazio.

Questa impostazione securitaria non basta, da sola, a garantire un'efficace protezione da attacchi e incidenti cyber. Tramite il recupero della dimensione territoriale e fisica, potrebbe venire meno la percezione del cyberspazio come 'terra di nessuno' in cui la giustizia coincide con la forza (tecnologica), risultando invece essere un luogo presidiato dalle Istituzioni pubbliche. Le quali si trovano però ad agire soprattutto per via autoritativa[67], ma non in modo esclusivo. Questa impostazione securitaria-autoritativa, infatti, dovrebbe essere integrata da ap-

mente N. Irti, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, Laterza, 2006; S. Cassese, *Territori e potere. Un nuovo ruolo per gli Stati*, Bologna, Il Mulino, 2016.

59 Si v. L. Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, Springer, 2015.

60 Si v. G. Porro, *Un cyberattacco a un ospedale tedesco ha causato la morte di una donna*, in *Wired*, 18 settembre 2020 (in https://s.uniupo.it/r3p7s).

61 Così G. Bombelli, *Dogmatica, certezza e (in)calcolabilità. Note su profili di "anticipazione cognitiva" in tema di* legal design *e* decision-making, in *Cybersecurity e Istituzioni democratiche*, *cit.*, a cura di P. Heritier, S. Rossa, p. 28.

62 B. Carotti, *Uniformità e autonomia nella sicurezza cibernetica*, in *Cybersecurity e Istituzioni democratiche*, *cit.*, a cura di G. Bombelli, S. Rossa, p. 53

63 *Ibidem.*

64 E ciò «in modo da definire un ambito di tradizionale autorità ed esercizio dei poteri correlati: una funzione di tutela che si lega alla natura nazionale (e quindi direttamente o indirettamente territoriale) degli interessi tutelati», R. Ursi, *Introduzione. La sicurezza cibernetica come funzione pubblica*, in P. Heritier, S. Rossa, *Cybersecurity e Istituzioni democratiche*, *cit.*, a cura di P. Heritier, S. Rossa, p. 12.

65 Il riferimento è al d.l. n. 105 del 2019, conv. l. n. 133 del 2019. In argomento E. Buoso, *Ritorno al futuro: il perimetro di sicurezza nazionale cibernetica*, in *Cybersecurity e Istituzioni democratiche*, *cit.*, a cura di P. Heritier, S. Rossa, p. 33 ss.; Id., *Potere amministrativo e sicurezza nazionale cibernetica*, *cit.*, p. 87 ss.; B. Carotti, *Sicurezza cibernetica e Stato nazione*, *cit*.

66 R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in *La sicurezza nel cyberspazio*, a cura di R. Ursi, *cit.*, p. 14.

67 Sia consentito al riguardo rimandare alle riflessioni contenute in S. Rossa, *Cybersicurezza e pubblica amministrazione*, *cit.*, p. 159 ss.

procci di carattere cooperativo e sinergico che coinvolgano cittadini e imprese[68]. Approcci che devono necessariamente trovare un previo fondamento nell'attività pubblica di educazione e di sensibilizzazione rivolta a soggetti terzi (i cittadini, imprese, ecc.) sui rischi insiti nell'impiego delle tecnologie digitali. Attività di educazione che però, in ultima analisi, appare possibile proprio grazie al recupero della menzionata azione di territorializzazione del cyberspazio.

È in questo solco, con l'espresso intento di aumentare la cd. *cybersecurity awareness*, che si pongono le specifiche iniziative di educazione cyber realizzate da ENISA a livello europeo e da ACN sul piano nazionale[69]. In particolare, tali ultime iniziative paiono, peraltro, giustificate dal contesto sociale italiano emergente dai risultati del DESI 2024, secondo cui solo il 45,8% dei cittadini possiede competenze digitali di base[70].

Solo tramite la diffusione di pratiche di educazione alla *cybersecurity* da parte delle Istituzioni pubbliche può essere veicolata la consapevolezza della dimensione fisico-territoriale, materiale, delle azioni digitali, consentendo ai cittadini di comprendere che, anche se a colpo d'occhio non sembra, le condotte che vengono poste in essere nel cyberspazio possono avere enormi ricadute concrete. Le quali sono in grado di ripercuotersi anche su altri soggetti, potendo comportare significativi danni a organizzazioni complesse – pubbliche o private.

Questa presa di coscienza è fondamentale, rappresentando un presupposto di cybersicurezza che integra una condizione indispensabile per poter governare il rischio tecnologico; e dunque per poter realizzare interventi pubblici funzionali a proteggere le situazioni giuridiche soggettive di tutti coloro i quali operano nei diversi ecosistemi digitali, telemedicina compresa.

68 Sul punto S. Terracciano, *La dimensione collaborativa tra soggetti pubblici e tra soggetti pubblici e privati nel contesto della cybersicurezza*, in *Cybersecurity e Istituzioni democratiche*, *cit.*, a cura di P. Heritier, S. Rossa, p. 181 ss.; L. Previti, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, *cit.* In argomento anche M. Macchia, G. Sferrazzo, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, *cit.*, p. 145.

69 Si v. ad esempio le numerose campagne di consapevolezza della cybersicurezza promosse da ENISA, consultabili sul sito istituzionale dell'Agenzia europea per la cybersicurezza (si v. https://s.uniupo.it/9ubpk) e da ACN (si v. https://s.uniupo.it/v5mv4).

70 Si v. European Commission, *Italy 2024 Digital Decade Country Report*, 22 luglio 2024.

Notes on Cybersecurity and Digital Ecosystems: the Telemedicine Case Study

Abstract

The paper explores the relationship between cybersecurity and digital ecosystems, with a particular focus on telemedicine. After briefly reconstructing the legal framework, the article focuses on the low perception of the real effects caused by virtual actions carried out in cyberspace, which can affect and damage digital ecosystems, questioning whether this is a consequence of the physical and immaterial a-territoriality inherent in the very concept of cyberspace. In the final part, the paper highlights the efforts of national public institutions to 'territorialise' cyberspace and emphasises the need to adopt cybersecurity education practices based on a public-private collaborative approach that emphasises the physical-territorial dimension of virtual actions, to increase the level of cyber protection of digital ecosystems.

Parole chiave: cybersicurezza – cyberspazio – ecosistema digitale – telemedicina

Keywords: *cybersecurity – cyberspace – digital ecosystem – telemedicine*