GRUPPO di PISA

Dibattito aperto sul Diritto
e la Giustizia Costituzionale

La Rivista / Quaderno n° 5

Fascicolo speciale monografico

A cura di

Daniele CASANOVA, Alessandro DE NICOLA,
Maria Chiara GIRARDI, Pietro VILLASCHI

«Le fonti della crisi: prospettive di diritto comparato»

in memoria di
PAOLO CARROZZA

GRUPPO di PISA
Dibattito aperto sul Diritto e la Giustizia Costituzionale

La Rivista / Quaderno n° 5
Fascicolo speciale monografico

A cura di

Daniele CASANOVA - Alessandro DE NICOLA - Maria Chiara GIRARDI - Pietro VILLASCHI

Le fonti della crisi: prospettive di diritto comparato

Atti del Seminario di diritto comparato – 25 marzo 2022

in memoria di
Paolo Carrozza

Contributi di:

N. Abate, A.K. Abou Koïni, A. Apostoli, E. Aureli, M. Aurino, M. Barone, L. Bartolucci, S. Bissaro, V. Brigante, D. Bruno, S. Cafiero, D. Camoni, V. Cavanna, G. Costa, M. D'Amico, N. D'Anza, M.F. De Tullio, L. Del Corona, C. Della Giustina, V. Desantis, V. Di Capua, C. Doubovetzky, T. Esposito, N. Fiano, V. Fogliame, A. Formisano, P. Gambatesa, T. Giorgio, L. Giurato, A. Iannotti Della Valle, E. La Fauci, L. Leo, J. Levi Mello do Amaral Jr., A. Lo Calzo, I. M. Lo Presti, X. Magnon, C. Malinverno, A.V. Mamfouana, M. Marazzini, L. Mariantoni, G. Martinico, A. Mazzola, G. Naglieri, R. Neri, L. Pace, M. Pittari, B.J. Queiroz Ceretta, I. Rivera, C. Sagone, G. Scoppetta, Giu. Serges, F. Serini, M.A. Sevilla Duro, C. Siccardi, L. Sottile, R. Tarchi, V. Valenti, G. Verrigno, P. Villaschi.

Quaderno monografico abbinato al fascicolo 2022/3 de «La Rivista Gruppo di Pisa»

Atti del Seminario di diritto comparato dell'Associazione "Gruppo di Pisa" del 25 marzo 2022 su "Le fonti della crisi: prospettive di diritto comparato" – Università degli Studi di Brescia

Tutti i contributi sono stati sottoposti a referaggio ai sensi dell'art. 5 del Regolamento della Rivista

Finito di comporre nel mese di dicembre 2022

La Rivista **Gruppo di Pisa. Dibattito aperto sul Diritto e la Giustizia Costituzionale** è inclusa tra le riviste scientifiche dell'Area 12 - Scienze giuridiche. Codice **ISSN: 2039-8026**.

GRUPPO di PISA
Dibattito aperto sul Diritto e la Giustizia Costituzionale

RIVISTA DEL GRUPPO DI PISA - INDICE DEL QUADERNO N° 5

SECONDA SESSIONE

PARTE I

I LIVELLI DELLA PRODUZIONE NORMATIVA DELLA CRISI: LA DIMENSIONE SOVRANAZIONALE

Introduzione ai lavori del I Atelier

Contributi dei partecipanti

PARTE II

I LIVELLI DELLA PRODUZIONE NORMATIVA DELLA CRISI: LA DIMENSIONE NAZIONALE

Introduzione ai lavori del II Atelier

Contributi dei partecipanti

Contributi dei partecipanti

GRUPPO di PISA
Dibattito aperto sul Diritto e la Giustizia Costituzionale

TERZA EDIZIONE DEL SEMINARIO INTERNAZIONALE DI DIRITTO COMPARATO
«LE FONTI DELLA CRISI: PROSPETTIVE DI DIRITTO COMPARATO»
IN MEMORIA DEL PROF. PAOLO CARROZZA

L'USO DELLA NORMATIVA TECNICA TRA ESIGENZE DI MERCATO E DI SICUREZZA DELLE RETI E DELLE RISORSE INFORMATICHE

FEDERICO SERINI

SOMMARIO: 1. Il rischio informatico come rischio globale. – 2. Lo "sconfinamento" della normativa tecnica verso gli interessi pubblici. – 2.1. Segue. Il Regolamento 1025/2012 – 3. La sicurezza delle reti e delle risorse informatiche come sicurezza del mercato unico europeo. – 4. Dalla cybersicurezza del mercato unico alla cybersicurezza nazionale italiana. – 5. Conclusioni.

1. *Il rischio informatico come rischio globale*

Nel celebre "La società del rischio" Ulrich Beck scriveva che «[n]ella modernità avanzata la produzione sociale di ricchezza va sistematicamente di pari passo con la produzione sociale dei rischi. In essa emergono problemi e conflitti che scaturiscono dalla produzione, definizione e distribuzione di rischi prodotti dalla scienza e dalla tecnica»[1].

L'assunto è particolarmente significativo e utile per approcciare l'analisi sull'uso della normativa tecnica nel particolare settore della sicurezza delle reti e delle risorse informatiche poiché ci consente da subito di individuare il nodo della questione, rappresentato dalla relazione produzione-diffusione dei rischi-esigenza di sicurezza.

Da sempre il progresso e l'espansione verso confini inesplorati hanno imposto all'uomo di fare i conti eventi futuri imprevedibili portandolo così a tenere in debita considerazione il "fattore rischio"[2].

[1] U. BECK, *La società del rischio. Verso una seconda modernità*, Roma, 2000, p. 25.

[2] Sul punto v. A. GIDDENS, *Il mondo che cambia. Come la globalizzazione ridisegna la nostra vita*, Bologna, 2000, p. 36 ss., ove l'A. scrive che «l'idea di rischio emerge nei secoli XVI e XVII, coniata per

Simili valutazioni hanno condizionato la storia umana sia nelle scelte individuali, sia in quelle collettive, col l'obiettivo di preservare la propria vita e i propri interessi di fronte all'incertezza dell'ignoto.

È curioso constatare come il processo di creazione del *cyberspace,* quale frutto della globalizzazione, non sia stato accompagnato da tali considerazioni in merito ai possibili pericoli che ne sarebbero potuti derivare. Questo nuovo dominio è infatti caratterizzato da debolezze tecniche e strutturali intrinseche che lo rendono particolarmente vulnerabile nei confronti di azioni malevole che possono incidere fortemente sui diritti e le libertà dei singoli; tanto che alcuni Studiosi hanno ipotizzato, di qualificare la "cybersicurezza" come bene pubblico[3].

Le reti e le risorse informatiche oggi non rappresentano solo i mezzi che consentono agli individui di esprimere liberamente la propria personalità attraverso nuove forme e modi[4], ma, a livello tecnico, sono anche i parametri di configurazione e funzionamento di molte infrastrutture essenziali per l'economia e per la società: si pensi agli apparati informatici in uso presso operatori attivi nei settori energetico, dei trasporti, delle comunicazioni ecc.

Si comprende quindi come il rischio tecnologico, o meglio in questo caso informatico, porti all'esigenza di elaborare un quadro normativo idoneo a far fronte a questa categoria di rischio caratterizzata almeno da due elementi.

Il primo attiene alla vulnerabilità intrinseca poc'anzi accennata. Il *cyberspace* è un fenomeno privato, la cui progettazione e gestione è avvenuta fuori dal controllo e dall'iniziativa degli Stati[5]. Probabilmente i diversi attori che parteciparono al progetto *ArpaNet,* e ai suoi successivi sviluppi che portarono alla creazione della "rete delle reti", l'*Internet*, non immaginavano che di lì a pochi anni le società moderne avrebbero affidato all'informatica importanti servizi e funzioni, facendole acquisire rilevanza pubblica. In particolare, l'intento di creare una "rete globale" caratterizzata dalle prerogative di libero accesso e interoperabilità portò alla creazione di un sistema non concepito per obbedire a criteri di sicurezza, quanto piuttosto a quelli di libero accesso e scambio delle

la prima volta dagli esploratori occidentali che si avventuravano per il mondo: la parola "rischio" sembra infatti derivare dallo spagnolo o dal portoghese, lingue nell'ambito delle quali era impiegata per indicare la navigazione in acque ignote, non segnate sulle carte».

[3] M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds & Machines*, n. 29, Springer, 2019, p. 354

[4] V. FROSINI, *La democrazia nel XXI secolo* (1997), Macerata, 2010, pp. 40-41.

[5] G. DELLA MORTE, *Big data e protezione internazionale dei diritti umani, regole e conflitti*, Napoli, 2018, p. 27. v. anche M. O'MARA, *The Code: Silicon Valley and the Remaking of America*, New York, 2019, p. 17. L'A. osserva che la rivoluzione delle "high-tech" negli Stati Uniti sia stata il frutto tanto dell'iniziativa dei privati quanto anche dei governi; specificamente tale rivoluzione «it is neither a big-government story nor a free-market one: it's both».

informazioni[6]. Principi questi che si scontrano oggi con le possibilità di *dual use*[7] della rete e dei servizi informatici.

Il secondo elemento riguarda la capillare diffusione delle tecnologie informatiche presso il pubblico che ha aperto alla possibilità di veicolare minacce da una parte all'altra del mondo per mezzo della rete.

Tali peculiarità hanno reso evidente l'obiettiva difficoltà dei pubblici poteri locali di far fronte a questo fenomeno di natura globale[8], che richiederebbe una risposta regolatoria allo stesso modo diffusa e uniforme da parte di tutti gli Stati[9].

La riflessione sull'uso della normativa tecnica per fini di sicurezza delle reti e delle risorse informatiche si inserisce nelle pieghe di questo dibattito, in quanto tali elementi costituiscono beni posti al centro di diverse regolazioni. Da una parte quelle di diritto pubblico (nazionale, europeo e intenzionale), volte a proteggere le informazioni e le infrastrutture di rilevanza strategica per il mercato e per la società, dall'altra, quelle del "diritto dei privati"[10], in quanto beni tecnologici rimessi al rispetto di determinati standard di funzionamento, qualità e sicurezza nella loro costruzione e implementazione (vedi ad esempio il requisito dell'interoperabilità)[11].

L'elevato *expertise* richiesto nella regolazione della materia e la mutabilità della tecnica hanno mostrato come sempre più spesso i legislatori abbiano delegato la competenza regolatoria di materie fortemente caratterizzate da elementi attinenti il mondo della tecnica e della scienza agli enti di normalizzazione responsabili della produzione di tali standard[12]. In particolare, tra questi, quelli sulla sicurezza delle risorse informatiche

---

[6] G. CORASANITI, *Esperienza giuridica e sicurezza informatica*, Milano, 2003, p. 332. Nello specifico, la vulnerabilità (debolezza) delle reti e dei sistemi informatici è una caratteristica propria di tali strumenti, la cui esistenza può essere attribuita all'idea che portò alla creazione del primo archetipo di rete, l'*ArpaNet*, concepita e sviluppata come uno spazio privo di regole - se non quelle tecniche che ne regolavano il suo funzionamento – il cui scopo era unicamente fornire un servizio "aperto" per la comunità, primo fra tutti quello di agevolare le comunicazioni tra soggetti che intendevano collaborare tra loro. Per questo motivo l'*ArpaNet*, così come oggi l'*Internet*, ossia l'insieme delle reti autonome e interconnesse, costituiscono dei sistemi privi di misure di sicurezza intrinseche. Sul punto v. anche C. GIUSTOZZI, *Cos'è il "rischio cyber" e perché ce ne dobbiamo preoccupare*, in F. RUGGE, S. DOMINIONI (a cura di), *La gestione dei rischi nello spazio cibernetico*, Dossier ISPI, 2019, p. 3.

[7] I prodotti *dual use* sono i prodotti, inclusi *software* e le tecnologie informatiche, che possono avere un utilizzo sia civile sia militare. Tali beni sono disciplinati dal regolamento (UE) 2021/821, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso.

[8] M. BETZU, *Poteri pubblici e private nel mondo digitale*, in *La Rivista Gruppo di Pisa*, fasc. 2, 2021. V. anche D.R. JOHNSON, D.G. POST, *Law and Borders – The Rise of Law in Cyberspace*, in *Stanford Law Review*, n. 48, 1996, pp. 1367 ss., secondo cui «Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the *power* of local governments to assert control over online behavior; (2) the *effects* of online behavior on individuals or things; (3) the *legitimacy* of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give *notice* of which sets of rules apply».

[9] A. ODDENINO, *Digital standardization, cybersecurity issues and international trade law*, in *Questions of international law*, 2018, pp. 31 -51.

[10] W. CESARINI SFORZA, *Il diritto dei privati*, Milano, 1963.

[11] M.C. GAMITO, *Europeanization through Standardization: ICT and Telecommunications*, in *Yearbook of European Law*, vol. 37, n. 1, 2018, pp. 395–423.

[12] v. C. JOERGES, H. SCHEPEL, E. VOS, *The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the "New Approach"*, in EUI Working Paper law, n. 9, 1999.

e delle informazioni hanno acquisito sempre maggiore rilevanza alla luce della stretta correlazione tra rischio informatico e rischio sociale[13], Difatti, in tale condizione, la sicurezza di tali beni, garantita per mezzo degli standard di produzione, rappresenta allo stesso tempo una forma indiretta di sicurezza pubblica[14].

Così. tra i fallimenti della cooperazione internazionale[15], e il tentativo a livello europeo di istituire un quadro di regole in materia di cybersicurezza volte a garantire la garanzia dei diritti anche in rete (vedi la direttiva NIS di cui nel proseguo), il frequente ricorso alla standardizzazione mostra come nella società globalizzata concorrano alla regolazione delle esperienze umane non solo i poteri pubblici, la cui sovranità è ormai limitata, ma anche soggetti privati; soprattutto quando la fattispecie che esige di essere regolata necessita di conoscenze che rinviano al mondo della scienza e della tecnica[16].

Il presente contributo intende pertanto svolgere alcune riflessioni sullo "sconfinamento" di questo strumento la cui funzione originaria non è la regolazione degli interessi pubblici ma il buon funzionamento e la qualità della produzione industriale.

2. *Lo "sconfinamento" della normativa tecnica verso gli interessi pubblici*

Possiamo definire brevemente gli standard come le norme tecniche indicanti le caratteristiche che un determinato prodotto, materiale, tecnologia o procedura deve avere per raggiungere un certo livello di qualità, sicurezza e affidabilità. Nello specifico, si tratta di "norme" non aventi natura giuridica, e quindi prive di cogenza, in quanto la loro formazione non avviene per mezzo di un processo giuridico-politico, ma attraverso una alternativa forma di aggregazione di interessi che coinvolge organismi indipendenti non statuali, ossia gli enti di normazione.

Le "norme tecniche" devono tuttavia essere distinte dalle "regole tecniche", qualificate invece come cogenti, in quanto prodotte autoritativamente da organi o enti pubblici, statali o regionali, sulla base di cognizioni fornite o da una scienza specialistica, o dalla conoscenza di una tecnica per la produzione di un bene o di un servizio non ricollegali alla scienza.

Da ultimo si aggiungono le "norme armonizzate", nozione con il quale si indicano le norme tecniche europee prodotte su mandato della Commissione europea ai fini

[13] M.G. LOSANO, *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. FORNI - T. VETTOR (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Torino, 2017, p. 22, ove l'A. scrive: «[l]a nostra società è retta ormai dall'informatica, che è anche lo strumento principale della globalizzazione: di conseguenza, ogni società è oggi tanto vulnerabile quanto è vulnerabile l'informatica di cui fa uso; quindi, più le società sono avanzate, più sono vulnerabili. La tendenza delle odierne città a trasformarsi in megalopoli informatizzate aumenta rischi di interventi militari nelle reti e nei cloud collegati a servizi essenziali».

[14] Sulla sicurezza pubblica v. R. URSI, *La sicurezza pubblica*, Bologna, 2022.

[15] Il riferimento è al tentativo di adottare una Convenzione globale sulla criminalità informatica, avvenuto con la proposta presentata al XII Congresso delle Nazioni Unite, tenutosi dal 12 al 19 aprile 2010, poi fallito a causa del disaccordo tra gli Stati. Per

[16] G. M. MARENGHI, *Standard e regolazione condivisa*, Torino, 2018.

dell'applicazione della legislazione dell'Unione sull'armonizzazione[17]. Si tratta di norme qualificate come volontarie, in quanto comunque prodotte fuori dal circuito degli enti di normazione statali.

La normazione tecnica nasce nel contesto industriale dapprima dall'esigenza delle singole aziende di definire le caratteristiche costruttive e dimensionali dei propri prodotti, generando di conseguenza effetti di c.d. *lock-in* che obbligavano i clienti a rivolgersi sempre allo stesso fabbricante. Solo a seguito della rivoluzione industriale e al progressivo sviluppo del tessuto produttivo, la produzione normativa tecnica si spostò presto dalle singole aziende agli enti di normazione, perlopiù di natura statale, con il fine di uniformare la produzione industriale a standard comuni[18]. Come rilevato dalla dottrina, in questo periodo, con il passaggio dallo Stato di polizia allo Stato liberale, l'intervento dei pubblici poteri a garanzia della sicurezza interna dello Stato continuava a manifestarsi anche attraverso l'ingente attività di produzione normativa tecnica[19].

Il dato non è di secondario rilievo, poiché mette in luce come già in origine la normalizzazione fosse stata utilizzata con il fine di perseguire fini sociali come quello della sicurezza pubblica.

Questo tratto sembra inoltre avere continuità anche nel secondo dopoguerra, ove la progressiva erosione della sovranità statale, dovuta all'istituzione delle grandi organizzazioni internazionali, all'obiettivo di superare le barriere economiche tra gli Stati, e al passaggio della produzione normativa tecnica dalle mani pubbliche a quelle dei privati, porta a credere che il perseguimento di tali interessi pubblici, venga oggi perseguito indirettamente attraverso lo strumento della normazione tecnica il cui obiettivo primario rimane comunque legato ad esigenze di produzione industriale e di mercato, rischiando così di capovolgere il processo instaurativo di un ordine internazionale a tutela dei diritti[20].

Proprio per questo motivo l'esperienza dell'Unione europea in questo settore sembra acquisire particolare interesse ai fini del presente studio, dato che l'Unione ha fatto ricorso allo strumento della standardizzazione per facilitare il processo di integrazione del mercato unico, ed allo stesso tempo garantire fini sociali come la tutela dell'ambiente e la sicurezza individuale e collettiva[21].

In particolare, si distinguono due momenti che hanno caratterizzato la standardizzazione europea. Fino alla metà degli anni '80 del Secolo scorso, l'intervento della allora Comunità aveva come unico obiettivo quello di smantellare gli ostacoli tecnici

---

[17] Art. 2 del Regolamento (UE) 1025/2012 sulla normazione europea che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio.

[18] P. ANDEINI, *La normativa tecnica tra sfera pubblica e sfera privata*, in P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO, *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, Bologna, 1995, pp. 45 ss.

[19] F. SALMONI, *Le norme tecniche*, 2001, p. 147.

[20] A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Napoli, 2018, pp. 71-72.

[21] E. CHITI, *La normalizzazione*, in S. CASSESE (a cura di), *Trattato di diritto amministrativo*, vol. IV, 2003, p. 4027.

che si frapponevano al libero scambio intracomunitario, tentando di addivenire ad un'armonizzazione degli standard tecnici nazionali per il tramite di direttive. Questo modello risultò tuttavia fallimentare stante la difficoltà di codificare le specifiche tecniche, nonché le diverse opposizioni dei rappresentanti delle amministrazioni nazionali nelle votazioni all'unanimità in seno al Consiglio che ebbero l'effetto di allungare oltremodo i tempi di adozione rendendone ormai obsoleto il contenuto tecnico[22].

Successivamente, nel 1985 venne inaugurato il c.d. "Nuovo approccio" in materia di armonizzazione tecnica e normazione[23]. In questo sistema il legislatore comunitario si limitava a stabilire i requisiti minimi obbligatori di interesse collettivo, solitamente in ambiti come sicurezza, salute, ambiente e protezione dei consumatori, delegando agli enti di normazione l'elaborazione delle specifiche tecniche relative ai diversi settori che venivano poi pubblicate in Gazzetta ufficiale come norme armonizzate.

La Commissione affidava quindi, per mezzo di mandato[24], la produzione delle norme tecniche agli organismi di normazione riconosciuti a livello europeo (ossia il CEN e il CENELEC), i quali dovevano elaborarle entro la cornice dettata dalle stesse istituzioni europee che vigilavano sulla loro conformità. La rinuncia della Commissione ad esercitare in via diretta le attribuzioni di rilevanza tecnica veniva così compensata con l'assolvimento di tre fondamentali compiti, ossia: la determinazione degli obiettivi; il controllo sulla "qualità" dell'attività degli enti di normazione e certificazione; e il controllo eventuale e successivo alla immissione nel mercato[25].

Questa nuova strategia ha avuto l'effetto di coniugare l'esigenza di tutelare le libertà economiche con la protezione dai rischi derivanti dallo svolgimento delle attività industriali, realizzando così «una integrazione stabile e permanente della regolazione sociale nella concorrenza, nella prospettiva di una ridefinizione di quest'ultima alla luce del principio dello sviluppo armonioso, equilibrato e sostenibile»[26].

Ad esempio, sono frutto di questo nuovo approccio sulla normazione armonizzata, le direttive sulla sicurezza dei giocattoli, la n. 378 del 1988[27], a cui ha fatto seguito la direttiva 2009/48/Ce, e la direttiva sulla sicurezza generale dei prodotti, la n.59 del 1992, a cui ha fatto seguito la direttiva 2001/95/Ce. In tutti questi casi il legislatore comunitario è intervenuto con il fine di tutelare i consumatori attraverso un sistema di presunzione di

---

[22] P. ANDREINI, *op. cit*, p. 52

[23] Risoluzione 85/C 136/01, 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione.

[24] Ancor prima dello "sconfinamento" verso ambiti non riservati alla normazione tecnica vi è la questione della "delega delle competenze normative" a soggetti diversi dai pubblici poteri. Sul punto v. C. JOERGES, H. SCHEPEL, E. VOS, *op.cit.*. V. anche M. E. BARTOLONI, *La regolazione privata nel sistema costituzionale dell'unione europea. riflessioni sulla disciplina relativa al settore dell'innovazione*, in *Osservatorio sulle fonti*, n. 3, 2021.

[25] G. VESPERINI, *Il controllo della «sicurezza» e della «qualità» dei prodotti industriali: due modelli e confronto*, in P. ANDREINI, G. CAIA, G. ELIAS, F.A. ROVERSI-MONACO, *op. cit*., p. 146.

[26] E. CHITI, *op. cit.*, p. 4027. Sul passaggio dalla eliminazione delle barriere alla libera circolazione delle merci al perseguimento di interessi sociali, v. anche C. JOERGES, *Scientific expertise in Social Regulation and the European Court of Justice: Legal Frameworks for Denationalized Governance Structures*, in C. JOERGES, K.H. LAUDEUR, E. VOS (a cura di), *Integrating Scintific Expertise into Regulatory Decision-Making. National traditions and European Innovation*, Baden-Baden, 1997, pp. 298-299

[27] Direttiva 88 /378 /CEE, relativa al ravvicinamento delle legislazioni degli Stati membri concernenti la sicurezza dei giocattoli.

sicurezza del prodotto conforme alle specifiche disposizioni comunitarie o, in mancanza, alla pertinente normativa nazionale.

2.1. *Segue. Il Regolamento 1025/2012*

Anche la nuova disciplina dettata dal Regolamento 1025/2012 sembra andare nella stessa direzione avviata con l'approccio dell'85[28].

Sebbene il fine della normazione resti quello di promuovere la competitività delle imprese - agevolando la libera circolazione dei beni e dei servizi, l'interoperabilità delle reti, i mezzi di comunicazione, lo sviluppo tecnologico e l'innovazione - dalla lettura dei considerando apprendiamo che tale vantaggio concorrenziale è parte del piano politico dell'Unione di fronteggiare le sfide sociali come «il cambiamento climatico, l'uso sostenibile delle risorse, l'innovazione, l'invecchiamento della popolazione, l'integrazione della persone con disabilità, la protezione dei consumatori, la sicurezza dei lavoratori e le condizioni di lavoro»[29].

In particolare, la realizzazione di detti fini, stabilmente integrati con le esigenze del libero mercato, sembra trovare concreta espressione nelle forme di cooperazione tra la Commissione europea e gli enti di normazione, e nell'enfasi posta sull'ampia partecipazione delle parti interessate[30], quali soggetti che rappresentano la dimensione dell'interesse pubblico nel processo di normazione e aiutano a rendere più accettabili le norme agli utilizzatori[31].

Il Regolamento del 2012 richiama in più occasioni tali forme di "pluralismo" nel processo di formazione degli standard quando prevede che le organizzazioni europee di normazione «incoraggiano e facilitano» la rappresentanza e la partecipazione di tutti i soggetti interessati alle proprie attività di normazione[32], e alle consultazioni per l'adozione del Programma annuale che identifica le priorità strategiche in materia di normazione europea[33].

Emerge pertanto il riconoscimento da parte dell'Unione del valore politico assunto dalla normazione tecnica e il suo impatto sulla società, che rende necessaria la più ampia partecipazione non solo dei soggetti destinatari delle norme tecniche, quali le industrie e i consumatori, ma anche le organizzazioni di rappresentanti di interessi pubblici diffusi[34].

---

[28] Regolamento (UE) 1025/2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio.

[29] Considerando 19 Reg. (UE) 1025/2012.

[30] A. ZEI, *Tecnica e diritto tra pubblico e privato*, Milano, 2008, pp. 372 ss.

[31] Comunicazione della commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo - Integrazione degli aspetti ambientali nella normazione europea, COM(2004)130 def., del 25, febbraio, 2004.

[32] Cfr. artt. 5, 7, 10, 11, 13, 20 Reg. (UE) 1025/2012.

[33] Art. 8 Reg. (UE) 1025/2012, si tratta del c.d. Programma di lavoro annuale dell'Unione per la normazione europea.

[34] v. A. ZEI, *op. cit*., pp. 384 ss. In particolare sul valore politico degli standard, il riferimento è agli Orientamenti generali per la cooperazione tra il CEN, il Cenelec e l'ETSI e la Commissione e

Dal quadro disciplinare appena descritto restano fuori le norme tecniche non armonizzate, ossia quelle norme prodotte da enti di normazione non europei e non elaborate in conformità ai "principi fondatori" unionali[35]. Questi standard, aventi natura volontaria e non cogente, costituiscono la maggior parte delle specifiche tecniche impiegate nel settore delle TIC. Già nel 2009, la Commissione europea, nel libro bianco sull'ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione, evidenziava come fossero divenuti sempre più attivi nell'elaborazione di tali standard forum e consorzi specializzati a livello globale, e come la politica comunitaria in tema di normalizzazione non rispecchiasse tale evoluzione[36].

Il tema interessa in particolare la fissazione dei requisiti tecnici nelle procedure di appalto pubblico per l'acquisto di *hardware*, *software* e servizi di tecnologia dell'informazione.

Il Regolamento 1025/2012 è intervenuto sul punto promuovendo una procedura di identificazione delle specifiche tecniche delle TIC, cui si potrebbe fare riferimento negli appalti pubblici, effettuando un'ampia consultazione di una vasta gamma di soggetti interessati, compresi le organizzazioni europee di normazione, le imprese e le autorità pubbliche.

3. *La sicurezza delle reti e delle risorse informatiche come sicurezza del mercato unico europeo*

Tra i diversi obiettivi sociali perseguiti per mezzo degli standard europei troviamo anche quello della sicurezza, del benessere dei cittadini e dell'efficienza delle reti[37]: elementi questi che rientrano complessivamente nelle politiche di cybersicurezza e protezione dei dati personali promosse a livello unionale[38].

Da tempo l'accesso alle reti informatiche, il controllo dei contenuti dell'informazione digitale e la comunicazione elettronica sono temi che interessano la politica dell'Unione europea. Tuttavia, solo in un secondo momento l'Unione ha focalizzato l'attenzione sul problema delle vulnerabilità informatiche ed in particolare sulle conseguenze che errori o attacchi informatici avrebbero potuto avere sul funzionamento del mercato.

Nel 2004, in una Comunicazione sulla protezione delle infrastrutture critiche, la Commissione faceva riferimento alla necessità di fornire protezione a tali soggetti anche

l'Associazione europea di libero scambio, del 28 marzo 2003, Gazzetta ufficiale n. C 091 del 16/04/2003, in cui si riconosce che «le norme [tecniche] occupano uno spazio sempre maggiore in nuovi settori politici, quali la sicurezza sul luogo di lavoro, la protezione dei consumatori e dell'ambiente, il trasferimento al mercato dei risultati della ricerca o l'attuazione di reti transeuropee».

[35] Considerando 31 Reg. (UE) 1025/2012.

[36] Comunicazione della Commissione delle comunità europee, Libro bianco - Ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione nell'UE – Prospettive, COM(2009) 324 definitivo.

[37] Considerando 22 Reg. (UE) 1025/2012.

[38] Si faccia riferimento alla Comunicazione congiunta al Parlamento europeo e al Consiglio - La strategia dell'UE in materia di cybersicurezza per il decennio digitale, COM(2020) 18 final, del 16 dicembre 2020.

da eventuali "attentati informatici" che avrebbero potuto produrre effetti negativi sul loro funzionamento[39]. Nello stesso anno, con il regolamento Ce n. 460/2004 veniva istituita l'Agenzia amministrativa responsabile per la sicurezza delle reti e dell'informazione (l'ENISA), la cui principale funzione, oltre a quella di assicurare un alto ed efficace livello di sicurezza in tali settori, era anche di «sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico dell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno»[40].

Tuttavia, prima di arrivare ad avere una disciplina specifica sulla sicurezza delle reti informatiche infrastrutturali si dovrà attendere il 2016, quando l'Unione è intervenuta in materia di cybersicurezza con la direttiva UE 2016/1148, anche nota come direttiva NIS (ossia "*Network and Information Security*"), poi recepita in Italia con il decreto legislativo 18 maggio 2018, n. 65.

La direttiva stabilisce una serie di misure volte a innalzare il livello di sicurezza delle reti e dei sistemi informativi in Europa al fine di evitare che le attività economiche e sociali europee, nonché il funzionamento del mercato interno, possano essere impattati dagli effetti negativi degli attacchi informatici. Nello specifico si tratta di uno strumento di armonizzazione minima volto a istituire un omogeneo livello di protezione attraverso l'imposizione di una serie di obblighi per gli Stati membri, e soprattutto per le infrastrutture rientranti nel campo d'applicazione della stessa[41], ossia gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD)[42].

In virtù dei relativi atti di recepimento della disciplina nei diversi Stati membri, tali infrastrutture sono tenute ad adottare misure adeguate e proporzionate alla gestione dei rischi per la sicurezza delle reti e dei sistemi informativi perlopiù consistenti: da una parte

[39] Comunicazione della Commissione al Consiglio e al Parlamento europeo per la protezione delle infrastrutture critiche nella lotta contro il terrorismo, COM(2004) 702 final.

[40] Art. 1 Reg. CE n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione. L'Agenzia è stata inizialmente dotata di un mandato temporaneo, via via esteso con i Regolamenti (UE) n. 1007/2008, e n. 580/2011. Tuttavia, solo con il successivo Regolamento (UE) 2019/881 (c.d. *Cybersecurity Act*), è stato conferito all'ENISA un mandato permanente, rafforzandone il ruolo, i compiti, le responsabilità, e predisponendo maggiori risorse al fine di contribuire al supporto degli Stati membri nel prevenire e rispondere efficacemente agli attacchi informatici.

[41] Tali oneri possono essere brevemente sintetizzati nell'obbligo per tutti gli Stati membri di predisporre strategie nazionali di cybersicurezza; l'istituzione di una cooperazione interstatale in ambito strategico; la realizzazione di una rete operativa di intervento in caso di incidente informatico; la declinazione di una serie di obblighi per gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD); ed infine, l'obbligo per tutti gli Stati di istituire autorità competenti a livello nazionale, punti di contatto unici e gruppi di intervento. v. A. ROTONDO, *Cyber security e protezione delle infrastrutture critiche: l'efficacia del modello europeo*, in S. MARCHISIO, U. MONTUORO (a cura di), *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa*, Torino, 2019.

[42] I settori in cui operano questi soggetti sono individuati nell'Allegato II della direttiva. Nella categoria degli operatori di servizi essenziali (OSE), rientrano i soggetti pubblici o privati che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali. Affinché un operatore possa essere qualificato come OSE deve fornire servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali e la fornitura del servizio deve dipendere dalla rete e dai sistemi informativi sì che un eventuale incidente avrebbe effetti negativi rilevanti sulla fornitura del servizio Nei fornitori di servizi digitali (FSD), rientrano invece le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio dell'Unione.

nella notifica, senza ingiustificato ritardo, degli incidenti di sicurezza che abbiano un impatto rilevante sulla continuità e sulla fornitura del servizio ai competenti Gruppi di intervento (c.d. CSIRT)[43]; e dall'altra nell'implementazione di misure di sicurezza tecniche e organizzative.

Anche in questo caso il legislatore europeo ha pertanto delegato la competenza normativa in materia agli enti di normazione tecnica, mentre la funzione di controllo e supervisione circa l'implementazione di tali misure è stata affidata alle c.d. autorità NIS, ossia soggetti operanti a livello nazionale e individuati dai singoli Stati membri[44].

Sembra tuttavia doveroso chiedersi all'interno di quale schema siano elaborate tali normative tecniche sulla sicurezza delle reti e delle risorse informatiche. La formula, volutamente ampia e generale, costituisce infatti un chiaro rinvio (mobile) che non specifica a quale normazione gli operatori debbano fare riferimento dovendo questi tener conto delle «conoscenze più aggiornate in materia»[45].

A ben vedere la produzione di "normative tecniche", sia volontarie, sia armonizzate, e di "regole tecniche", nel settore delle cybersicurezza è al momento inesistente, trattandosi di una nozione per molto tempo dibattuta tra gli esperti di settore che solo recentemente ha trovato una propria definizione a livello giuridico nel contesto europeo[46]. Il riferimento sembra pertanto essere rivolto, in via approssimativa e generale, a quel complesso di norme tecniche volontarie che riguardano la sicurezza informatica[47] e la sicurezza delle informazioni[48], prodotte da enti di normazione tecnica che sono parte di organi governativi esteri (nel caso specifico statunitensi) come le prime, o da enti di normazione tecnica internazionale, come le seconde[49].

La crescente rilevanza della materia ha indotto l'Unione a sviluppare progetti sulla creazione di norme armonizzate in questo settore con la partecipazione di rappresentanti

---

[43] Acronimo di *Computer Security Incident Response Team*, il CSIRT è un gruppo di intervento, incaricato di monitorare gli incidenti a livello nazionale; emettere preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; intervenire in caso di incidente; analizzare dinamicamente i rischi e gli incidenti; svolgere attività di sensibilizzazione situazionale; prendere parte alla c.d. rete dei CSIRT che interloquisce con l'Agenzia dell'Unione europea per cybersicurezza (ENISA) v. A. CONTALDO, F. PELUSO, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa, 2018, pp. 70 ss.

[44] Sulla diversa natura delle autorità NIS individuate dai singoli Stati membri v. A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *La Rivista Gruppo di Pisa*, Quaderno monografico abbinato al fascicolo 2, 2021, pp. 529 ss.

[45] Artt. 14 e 16 direttiva UE 2016/1148.

[46] Il Regolamento europeo 2019/881, il c.d. "Cybersecurity Act", ha introdotto per la prima volta all'art. 2, n. 1, la nozione di "cybersecurity" intendendo «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».

[47] L'Agenzia statunitense competente nella gestione delle tecnologie (il *National Institute of Standards and Technology* - NIST), definisce la sicurezza informatica «la protezione fornita ad un sistema informativo allo scopo di ottenere, come obiettivo applicabile, la conservazione dell'integrità, della disponibilità e della confidenzialità delle risorse del sistema informativo stesso (includendo hardware, software, firmware, dati e sistemi di telecomunicazione)» (NIST SP 800-14).

[48] Per sicurezza delle informazioni, la norma ISO/IEC 27000:2018 fa riferimento alla «preservazione della riservatezza, integrità e disponibilità delle informazioni», in qualsiasi forma esse siano rappresentate (digitale o materiale), o qualunque sia la loro modalità di trasmissione (comunicazione elettronica, corriere, ecc.).

[49] Il NIS è un'agenzia del governo degli Stati Uniti d'America, parte del Dipartimento del Commercio statunitense. L'ISO, acronimo di *International Organization for Standardization*, è un'organizzazione internazionale indipendente e non governativa.

delle autorità nazionali degli Stati membri e dei Paesi EFTA, degli organismi europei e internazionali di standardizzazione delle TIC e delle organizzazioni delle parti interessate che rappresentano l'industria, le piccole e medie imprese e i consumatori[50].

In particolare, con il Regolamento Ue 2019/881 è stato infatti istituito il "Quadro europeo di certificazione della cybersicurezza", ossia un sistema comune di normative tecniche, utili alla certificazione o valutazione dei prodotti, servizi e processi delle TIC, con il fine di aumentare la fiducia dei cittadini, delle organizzazioni e delle imprese nel mercato unico digitale europeo[51].

4. *Dalla cybersicurezza del mercato unico alla cybersicurezza nazionale italiana*

Sebbene la direttiva NIS abbia costituito un primo passo verso la messa in (cyber)sicurezza delle reti su tutto il territorio dell'Unione, l'applicazione del principio di sussidiarietà ha lasciato fuori dal campo applicativo della normativa diversi settori di indubbia rilevanza per la sicurezza degli Stati membri. Nella nozione di operatori di servizi essenziali vi rientrano infatti i soggetti pubblici impegnati nella fornitura di servizi come la distribuzione di energia, la fornitura di acqua potabile, i trasporti, servizi sanitari, servizi finanziari e bancari, lasciando tuttavia fuori altri soggetti come le pubbliche amministrazioni[52].

Così, con il decreto-legge del 21 settembre 2019, n. 105, convertito con modificazioni in legge 18 novembre 2019 n. 133, l'Italia, istituendo il c.d. Perimetro di

[50] Già nel 2011 era stato istituito l'*European Multi Stakeholder Platform on ICT standardisation* quale piattaforma consultiva in merito a tutte le questioni relative alla politica europea di normalizzazione delle ICT e della sua attuazione (Decisione della commissione che istituisce la piattaforma europea multilaterale sulla standardizzazione delle TIC, del 28 novembre 2011, 2011/C 349/04). Tra le competenze della piattaforma vi è anche l'elaborazione del *Rolling Plan for ICT Standardisation*, il documento annuale che fornisce una panoramica delle esigenze delle attività di standardizzazione delle TIC da intraprendere a sostegno delle attività politiche dell'UE (si rinvia al sito https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/about).

Il Piano del 2020 individuava tra le diverse azioni, raggruppate in quattro aree tematiche (quali fattori abilitanti e sicurezza, sfide sociali, innovazione per il mercato unico e crescita sostenibile), cinque settori prioritari ove la standardizzazione delle TIC era ritenuta necessaria e urgente per il completamento del mercato unico digitale e tra queste rientrava anche la cybersicurezza, ove prevedeva la definizione di una serie di norme e/o specifiche di riferimento relative alla sicurezza delle reti e dell'informazione, comprese, se del caso, norme armonizzate, che serviranno da base per incoraggiare l'adozione coerente di pratiche di standardizzazione in tutta l'UE

[51] Cfr. considerando 7, 48, 69 e art. 46 del Reg. (UE) 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Reg. (UE) n. 526/2013 («regolamento sulla cybersicurezza»). L'art. 2, n. 9 del citato Regolamento, definisce il sistema europeo di certificazione della cybersicurezza come «una serie completa, di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC e processi TIC», mentre al n. 11, trova definizione la nozione di certificato europeo di cybersicurezza, inteso come «un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cybersicurezza».

[52] v. Considerando 45 della direttiva NIS che invita gli Stati membri a garantire la sicurezza delle reti e dei sistemi informativi delle pubbliche amministrazioni che non rientrano nel campo di applicazione della direttiva.

Sicurezza Nazionale Cibernetica (PSNC), è intervenuta sulla protezione delle reti e delle risorse informatiche con un approccio sistematico e integrativo della disciplina NIS, coinvolgendo nel PSNC «tutti quegli operatori pubblici o privati, che, seppur non ricompresi nell'ambito di applicazione della Direttiva NIS, risultino comunque essenziali per la sicurezza nazionale italiana [...]»[53].

L'art. 1 co.1, del decreto-legge 105/2019 dispone infatti che l'obiettivo della normativa è di elevare i livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici «delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica»[54].

La protezione delle reti e delle risorse informatiche acquista pertanto profili di sicurezza nazionale a tutti gli effetti[55].

Tuttavia nonostante i diversi riferimenti alla (cyber)sicurezza nazionale contenuti nel PSNC, è stato con il decreto legge 14 giugno n. 82 del 2021, recante "disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", che è stata introdotta per la prima volta nell'ordinamento italiano la definizione di «cybersicurezza» intesa come «l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3

---

[53] S. MELE, *Il Perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. CASSANO, S. PREVITI, *Il diritto di internet nell'era digitale*, Milano, p. 187.

[54] L'ampia formulazione non consente di individuare i soggetti afferenti al perimetro, atteso che tale compito è stato affidato ad alcune amministrazioni centrali dello Stato – come per la direttiva NIS – conformemente ai criteri di individuazione dettati da un apposito d.P.C.M., n. 131/2020, ove all'art. 2 è previsto che un soggetto svolge una funzione essenziale dello Stato, «laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti». Mentre un soggetto pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, laddove ponga in essere «attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale». Ulteriore categoria di soggetti che facoltativamente possono rientrare nel Perimetro, sono gli Organi costituzionali, i quali possono adottare per le proprie reti e le proprie risorse informatiche, misure di sicurezza analoghe a quelle previste dalla normativa sul PSNC.

[55] Sul concetto di sicurezza nazionale, v. M. VALENTINI, *L'ordinamento del sistema politico dell'informazione per la sicurezza*, in C. MOSCA – G. SCANDONE – S. GAMBACURTA – M. VALENTINI, *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)*, Milano, 2008, pp. 56; ID, *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Napoli, 2017; U. GORI, L. MARTINO, *Intelligence e interesse nazionale*, Roma, 2015; B. VALENSISE, *I settori strategici dopo la riforma*, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, 2020, pp. 101 ss.; P. CAGGIANO, *Covid-19.Misure urgenti sui poteri speciali dello Stato nei settori della difesa e della sicurezza nazionale, dell'energia, dei trasporti e delle telecomunicazioni*, in *federalismi.it*, 2020.

agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico».

Si tratta di una formulazione elaborata sulla scorta di un processo di composizione multidisciplinare che ha il pregio di accogliere al suo interno diversi aspetti caratterizzanti la materia, tra cui anche i riferimenti alle normazioni tecniche relative alla sicurezza informatica e delle informazioni, il cui fine è proprio quello di garantire le tre proprietà fondamentali delle risorse informatiche e delle informazioni sicure, ossia, la loro riservatezza (*confidentiality*), integrità (*integrity*) e disponibilità (*availability*), spesso indicate con l'acronimo R.I.D (o C.I.A. in lingua inglese)[56].

5. *Conclusioni*

Appurata la natura intrinsecamente rischiosa delle tecnologie informatiche, riprendendo il pensiero di Beck sembra ragionevole chiedersi chi abbia il diritto di prendere decisioni su tali rischi e quindi sulla regolazione di tali beni[57].

Oggi i poteri pubblici svolgono questa azione attraverso politiche adottate alla luce del principio di precauzione, ossia politiche di *risk assesment*, quali analisi di natura scientifica[58], e di *risk management,* circa l'attuazione di piani di gestione del rischio[59].

Tuttavia, in entrambe le ipotesi, le correlate decisioni su questioni di ordine tecnico-scientifico rinviano alla normazione tecnica che si inserisce in ambiti di interesse più pubblicistico e nello specifico, quello della sicurezza è un settore particolarmente sensibile in quanto da sempre legato al concetto di sovranità statale[60].

L'analisi sin qui condotta mostra come nel contesto globalizzato l'uso della normazione tecnica risulti sempre più essere il veicolo di una tutela indiretta degli interessi pubblici.

[56] La riservatezza (o confidenzialità), è la proprietà per cui tali risorse possono essere accedute solo da chi è stato autorizzato o ne abbia il diritto; l'integrità concerne invece la garanzia della correttezza, coerenza e affidabilità e quindi anche la certezza che il sistema informativo e l'informazione non siano stati alterati o modificati da soggetti non autorizzati; infine, per disponibilità, si intende la proprietà secondo cui le risorse informatiche e le informazioni devono essere utilizzabili ed accessibili ogni qualvolta il soggetto autorizzato lo richieda.

[57] U. BECK, *op. cit*., p. 329.

[58] Il concetto di rischio, considerato scientificamente assume la forma del calcolo di probabilità espresso nella formula: rischio= impatto x probabilità (*likelihood*).

[59] Sul punto v. M SIMONCINI, *La regolazione del rischio e il sistema degli standard. elementi per una teoria dell'azione amministrativa attraverso i casi del terrorismo e dell'ambiente*, Napoli, 2010; P. SAVONA, *Il governo del rischio. Diritto dell'incertezza o diritto incerto?*, Napoli, 2013.

[60] E.A. IMPARATO*, Sovranità e sicurezza. Un connubio ancora vincente?*, in *federalismi.it*, n. 1, 2019.

GRUPPO di PISA
Dibattito aperto sul Diritto e la Giustizia Costituzionale

INFORMAZIONI SUI CURATORI E SUGLI AUTORI

CURATORI

Daniele Casanova, Ricercatore universitario di Istituzioni di Diritto pubblico presso l'Università degli Studi di Brescia

Alessandro De Nicola, Dottorando di ricerca in Discipline giuridiche presso l'Università degli Studi «Roma Tre» – Componente del Comitato dei Giovani Costituzionalisti

Maria Chiara Girardi, Assegnista di ricerca in Diritto costituzionale presso l'Università degli Studi «Federico II» di Napoli – Componente del Comitato dei Giovani Costituzionalisti

Pietro Villaschi, Assegnista di ricerca in Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano – Componente del Comitato dei Giovani Costituzionalisti

AUTORI

Nicola Abate, Dottorando di ricerca in Giurisprudenza presso l'Università «Pompeu Fabra» di Barcellona

Abdoul Kader Abou Koïni, Dottorando di ricerca in Diritto pubblico presso l'Università «Gaston Berger» di Saint-Louis (Sénégal)

Adriana Apostoli, Professoressa ordinaria di Diritto costituzionale presso l'Università degli Studi di Brescia

Elia Aureli, Dottorando di ricerca in Studi giuridici comparati ed europei presso l'Università degli Studi di Trento

Marta Aurino, Dottoranda di ricerca in Diritto costituzionale con cotutela internazionale di tesi presso l'Università degli Studi «Federico II» di Napoli e l'Università di Bordeaux

Michele Barone, Dottore di ricerca in "Innovazione e gestione delle risorse pubbliche" presso l'Università degli Studi del Molise

Luca Bartolucci, Dottore di ricerca in "Teoria dello Stato e Istituzioni politiche comparate" presso l'Università degli Studi «la Sapienza» di Roma

Stefano Bissaro, Assegnista di ricerca in Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano

Vinicio Brigante, Ricercatore universitario di Diritto Amministrativo presso l'Università degli Studi «Federico II» di Napoli

Domenico Bruno, Dottorando di ricerca in Diritti Umani. Teoria, storia e prassi presso l'Università degli Studi «Federico II» di Napoli

Simone Cafiero, Dottorando di ricerca in Diritto dell'economia presso l'Università degli Studi «Federico II» di Napoli

Daniele Camoni, Assegnista di ricerca in Diritto pubblico comparato presso l'Università degli Studi «la Statale» di Milano

Valentina Cavanna, Dottoranda di ricerca in Diritti e istituzioni presso l'Università degli Studi di Torino

Giuliano Costa, Dottorando di ricerca in Diritto costituzionale presso l'Università degli Studi di Foggia

Marilisa D'Amico, Professoressa ordinaria di Diritto costituzionale e Prorettrice con Delega a Legalità, Trasparenza e Parità di Diritti presso l'Università degli Studi «la Statale» di Milano – Ex-Presidente dell'Associazione «Gruppo di Pisa»

Nicola D'Anza, Dottorando di ricerca in Teoria dei diritti fondamentali, giustizia costituzionale e comparazione giuridica, area Diritto costituzionale presso l'Università di Pisa.

Maria Francesca De Tullio, Ricercatrice di Diritto costituzionale presso l'Università degli Studi «Federico II» di Napoli.

Lavinia Del Corona, Ricercatrice universitaria di Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano

Camilla Della Giustina, Dottoranda presso l'Università degli Studi della Campania «Luigi Vanvitelli»

Vincenzo Desantis, Assegnista di ricerca presso l'Università degli Studi di Trento

Viviana Di Capua, Ricercatore di Istituzioni di Diritto pubblico presso l'Università degli Studi di Napoli «Federico II»

Christophe Doubovetzky, Dottore di ricerca presso l'Università *«Capitole»* di Tolosa (*Toulouse I*)

Teresa Esposito, Dottoressa in Giurisprudenza presso l'Università degli Studi «Federico II» di Napoli

Nannerel Fiano, Ricercatrice universitaria di Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano

Virgilia Fogliame, Ricercatrice universitaria di Diritto costituzionale presso l'Università degli Studi «Federico II» di Napoli

Aniello Formisano, Dottorando di ricerca in Diritto pubblico presso l'Università degli Studi «Parthenope» di Napoli

Paolo Gambatesa, Dottorando di ricerca in Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano

Tony Giorgio, Dottorando di ricerca in Diritto pubblico comparato presso l'Università degli Studi di Teramo

Luisa Giurato, Dottoressa di ricerca in Diritto pubblico, comparato ed internazionale dell'Università degli Studi «la Sapienza» di Roma

Aldo Iannotti Della Valle, Dottore di Ricerca presso l'Università degli Studi «Suor Orsola Benincasa» di Napoli

Erika La Fauci, Dottoranda di ricerca in Diritto costituzionale con cotutela internazionale di tesi presso l'Università degli Studi di Messina e l'Università di Tolone

Luana Leo, Dottoranda di ricerca in Diritto Costituzionale presso la Libera Università Mediterranea «Jean Monnet» di Bari

José Levi Mello do Amaral Jr., Professor Associado de Direito constitucional presso l'Università di São Paulo (Brasile)

Antonello Lo Calzo, Assegnista di ricerca in Diritto costituzionale presso l'Università degli Studi del Sannio di Benevento – Vice-Presidente del Comitato dei Giovani Costituzionalisti

Isabella Maria Lo Presti, Ricercatrice universitaria di Diritto pubblico comparato presso l'Università degli Studi di Palermo

Xavier Magnon, Professeur de Droit public presso l'Università di Aix-Marseille

Chiara Malinverno, Dottoranda di ricerca in Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano

Allegra Vycinfleur Mamfouana, Dottoranda in Diritto pubblico presso l'Università di Tolone

Marco Marazzini, Dottorando di ricerca di Diritto costituzionale presso l'Università degli Studi di Genova

Luca Mariantoni, Dottorando di ricerca in Diritto Costituzionale e Diritto Pubblico Generale presso l'Università degli Studi «la Sapienza» di Roma

Giuseppe Martinico, Professore ordinario di Diritto pubblico comparato presso la Scuola Superiore Sant'Anna di Pisa

Alessandra Mazzola, Dottoranda di ricerca in Diritto costituzionale presso l'Università degli Studi «Parthenope» di Napoli

Giuseppe Naglieri, Dottore di Ricerca in Diritto pubblico comparato con cotutela internazionale di tesi presso l'Università degli Studi di Bari e l'Università di Malaga

Rocco Neri, Funzionario dell'Ufficio per il processo presso il Tribunale di Rimini – Dottore magistrale in Giurisprudenza presso l'Università degli Studi di Teramo

Leonardo Pace, Ricercatore di Istituzioni di Diritto pubblico presso l'Università degli Studi «Roma Tre» – Segretario del Comitato dei Giovani Costituzionalisti

Mariella Pittari, Dottoranda e Assegnista di ricerca presso l'Università degli Studi di Torino

Bruno José Queiroz Ceretta, Dottorando in Direito do Estado presso l'Università di San Paolo (Brasile) in cotutela con l'Università degli Studi «La Sapienza» di Roma

Ilaria Rivera, Dottoressa di ricerca in Diritto pubblico, giustizia penale ed internazionale presso l'Università degli studi di Pavia

Chiara Sagone, Assegnista di ricerca in Diritto costituzionale presso l'Università degli Studi di Catania

Giulia Scoppetta, Dottoranda di ricerca in Diritto pubblico presso l'Università degli Studi «la Sapienza» di Roma

Giuliano Serges, Ricercatore di Diritto costituzionale presso l'Università degli Studi «Roma Tre» – Presidente del Comitato dei Giovani Costituzionalisti

Federico Serini, Dottorando di ricerca in Diritto pubblico, comparato e internazionale presso l'Università degli Studi «la Sapienza» di Roma

Miguel Angel Sevilla Duro, Dottorando di ricerca in Diritto costituzionale presso l'Università «Castilla-La Mancha»

Cecilia Siccardi, Ricercatrice universitaria in Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano – Vice-Presidente emerita del Comitato dei Giovani Costituzionalisti

Lorenzo Sottile, Dottorando di ricerca in Istituzioni di diritto pubblico presso l'Università degli Studi di Genova

Rolando Tarchi, Professore ordinario in Diritto pubblico comparato presso l'Università di Pisa

Veronica Valenti, Dottoranda di ricerca in Diritto comparato dell'ambiente presso l'Università degli Studi di Genova

Giuseppe Verrigno, Dottore magistrale in giurisprudenza e borsista per la Fondazione «Falcone 2021» presso l'Università degli Studi di Palermo

Pietro Villaschi, Assegnista di ricerca in Diritto costituzionale presso l'Università degli Studi «la Statale» di Milano