RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2026 • DOI 10.32091/RIID0294 • articolo sottoposto a peer review • pubblicato in anteprima il 2 nov. 2026
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Stefano Dorigo

Cybersicurezza e fiscalità: un necessario (ma incerto) ripensamento delle categorie nel tempo della "guerra ibrida"

Il contributo analizza il ruolo della fiscalità quale strumento di promozione della cybersicurezza delle piccole e medie imprese, muovendo dalla constatazione che l'attuale approccio normativo, fondato prevalentemente su obblighi e sanzioni, non è sufficiente a favorire un'effettiva diffusione della cultura della sicurezza informatica. Dopo aver ricostruito il quadro dei rischi connessi alla guerra ibrida, alla protezione dei dati, alla sicurezza economica e alla vulnerabilità delle PMI, vengono esaminati i principali strumenti di incentivo economico e fiscale adottati nell'ordinamento italiano e comparato, evidenziandone limiti e potenzialità. Si evidenzia come la cybersicurezza possa costituire, quanto meno nella sua dimensione sistemica, un bene pubblico e un interesse collettivo, la cui tutela richiede una responsabilità condivisa tra Stato e operatori economici. In questa prospettiva, si propone una riflessione sull'impiego della leva tributaria non solo in funzione agevolativa, ma anche quale strumento pedagogico e solidaristico, idoneo a orientare i comportamenti e a ripartire i costi della sicurezza. In questo senso, va probabilmente ripensata la definizione di capacità contributiva, valorizzando nuove forme di vantaggio connesse all'appartenenza alla comunità e alla fruizione di beni pubblici essenziali, in contesti eccezionali caratterizzati da gravi rischi collettivi.

Cybersicurezza – Fiscalità – PMI – Capacità contributiva – Beni pubblici

Cybersecurity and taxation: a necessary (but uncertain) rethinking of categories in the age of "hybrid warfare"

This paper analyses the role of taxation as a tool for promoting cybersecurity amongst small and medium-sized enterprises, starting from the observation that the current regulatory approach – based predominantly on obligations and penalties – is insufficient to foster the effective spread of a culture of cybersecurity. After outlining the risks associated with hybrid warfare, data protection, economic stability and the vulnerability of SMEs, the paper examines the main economic and fiscal incentive measures adopted under Italian law and in other jurisdictions, highlighting their limitations and potential. It argues that cybersecurity may constitute, at least in its systemic dimension, a public good and a collective interest, the protection of which requires shared responsibility between the State and economic operators. From this perspective, the paper proposes a reflection on the use of taxation not only as a means of providing incentives, but also as an educational and solidarity-based tool, capable of guiding behaviour and sharing the costs of security. In this sense, the notion of "ability to pay" should probably be re-examined, placing greater value on new forms of benefit linked to membership of the community and the enjoyment of essential public goods, in exceptional contexts characterised by serious collective risks.

Cybersecurity – Taxation – SMEs – Ability to pay – Public goods

L'Autore è professore associato di diritto tributario presso l'Università di Firenze

Sommario: 1. Il problema: i rischi *cyber* e la (scarsa) attenzione delle PMI all'adeguamento dei propri sistemi di difesa. – 2. Il ruolo della fiscalità e le soluzioni "tradizionali". – 3. La cybersicurezza come bene comune e l'ipotesi di un tributo su una nuova forma di capacità contributiva.

1. Il problema: i rischi *cyber* e la (scarsa) attenzione delle PMI all'adeguamento dei propri sistemi di difesa

La cybersicurezza è argomento che sta diventando centrale, quanto meno nel dibattito mediatico, al tempo della "guerra ibrida"[1]. Quasi ogni giorno, si hanno notizie di attacchi a reti ed infrastrutture digitali, con conseguenze sia per la vita di ogni giorno dei cittadini, sia per la tenuta dei sistemi di difesa nazionali. Non siamo più, quindi, al cospetto di situazioni di virus informatici che infettano computer privati, con conseguenze più o meno circoscritte. I fenomeni che si verificano sono di portata assai maggiore: furto massiccio di dati, spesso sensibili, destinati ad essere rivenduti nel dark web (come nel recente caso dei documenti di identità dei clienti sottratti ai database degli alberghi) o ad essere impiegati per attività di spionaggio o di interferenza militare (come ci insegna, purtroppo, la guerra russo-ucraina ancora in corso); blocco di servizi essenziali per l'ordinato svolgimento della vita sociale (si pensi alle interferenze sui sistemi di funzionamento degli aeroporti, anche questa diventata realtà assai frequente); sabotaggio di sistemi di sicurezza, con minaccia anche per esponenti di spicco della politica nazionale ed internazionale (è recente la notizia dell'atterraggio di emergenza dell'aereo della Presidente della Commissione Ue Von der Leyen proprio a causa di un attacco hacker ai sistemi di rilevazione GPS)[2]. Si tratta di fenomeni che, peraltro, non restano confinati all'ambito militare, ma influenzano in misura crescente l'ordinato svolgimento della vita politica e sociale, come testimoniano le sempre più diffuse vicende di manipolazione delle informazioni sulla rete e, in particolare, sui social network[3].

Il tema intercetta, quindi, una pluralità di situazioni meritevoli di tutela: la sicurezza nazionale, innanzitutto, ma anche la tenuta del sistema dei diritti fondamentali, che può essere messo a repentaglio nel momento in cui un numero molto elevato di dati personali, sparsi nei database di soggetti pubblici e privati, è esposto al rischio di furto e di conseguente utilizzo improprio. Inoltre, la letteratura ed i documenti di policy, soprattutto sovranazionali, evidenziano la progressiva emersione di un interesse legato alla sicurezza economica e, quindi, alla tutela del mercato[4]. Qui si enfatizza come

1. Parla di "sicurezza cibernetica come problema globale" Pietropaoli 2025, p. 103.
2. Per una prima ricostruzione del fenomeno cibernetico nella prospettiva delle nuove forme di guerra di informazione si veda Bonfanti 2018.
3. Su tale delicatissimo aspetto si rinvia a Ziccardi 2019.
4. Si veda, sul piano delle politiche dell'Unione, la Comunicazione congiunta della Commissione europea e dell'Alto rappresentante sulla *Strategia europea per la sicurezza economica*, doc. JOIN(2023) 20 del 20 giugno 2023, che annovera espressamente, tra i rischi per la sicurezza economica dell'Unione, quelli relativi alla sicurezza fisica e, soprattutto, informatica delle infrastrutture critiche. La direttiva NIS 2, del resto, è adottata sulla base dell'art. 114 TFUE, cioè della competenza in materia di ravvicinamento delle legislazioni per il funzionamento del mercato interno, e fa espressamente salva (art. 2, par. 6) la responsabilità degli Stati membri per la salvaguardia della sicurezza nazionale e delle funzioni essenziali dello Stato.

taluni beni (la resilienza delle catene del valore, la continuità dei servizi e la fiducia degli operatori e dei consumatori nella sicurezza delle transazioni digitali) hanno una dimensione che trascende l'interesse individuale, pur non giustificando un intervento pubblico tale da limitare l'iniziativa economica privata in nome di una generalizzata tutela dell'interesse nazionale.

In questo contesto, la responsabilità per adeguate misure di tutela – secondo la scala che comprende misure di prevenzione, di monitoraggio e di reazione – grava evidentemente sui soggetti pubblici, ma un ruolo decisivo spetta alle imprese private. Esse, infatti, non solo detengono una mole vastissima di dati rilevanti per le persone e per lo Stato, ma sono anche titolari e gestori di quote rilevanti delle infrastrutture di rete e di sistemi informativi che costituiscono l'ossatura del cyberspazio, con la conseguenza che mancando un adeguato sistema di sicurezza informatica sorge il pericolo che, specie laddove vi sia un collegamento tra imprese (e tra imprese e pubblica amministrazione) nel contesto di reti informatiche, si realizzi un effetto a cascata idoneo a mettere a repentaglio l'intero sistema nazionale, o una parte significativa del medesimo[5]. Appare al riguardo significativo che già la Comunicazione della Commissione Ue del 2001 sulla sicurezza delle reti e dell'informazione evidenziasse la rilevanza del ruolo degli operatori privati nella gestione delle infrastrutture[6]. Allo stesso modo, la prima strategia europea per la cybersicurezza del 2013 ha fatto proprio un approccio multi-stakeholder, attribuendo espressamente a talune categorie di privati specifiche responsabilità nella gestione del rischio cibernetico[7].

Specie le PMI, che come subito vedremo sono le più restie a dotarsi di adeguati sistemi di cybersecurity, anche a causa dei costi conseguenti, sono considerate l'anello debole della catena di sicurezza, come riconosce realisticamente la direttiva NIS 2[8]: soprattutto con riferimento ad esse, quindi, si pone la questione della realizzazione di adeguati sistemi di protezione che possano costituire una parte del più generale sistema di cybersecurity nazionale.

Come si anticipava, tuttavia, la sensibilità degli operatori economici per questi temi appare, ad oggi, ancora insufficiente. I principali report internazionali e nazionali osservano, infatti, che, sebbene il problema sia effettivamente percepito (anche perché molte imprese hanno già sperimentato attacchi ai propri sistemi informatici, spesso con richiesta di riscatto), esso viene talvolta sottovalutato, più spesso rimandato, considerati i costi eccessivi dell'adeguamento e la sensazione che, sebbene il rischio sia diffuso, sarà comunque possibile intervenire *ex post*, evitando quindi esborsi percepiti come inutili o prematuri rispetto a situazioni avverse di cui è incerta la probabilità di realizzazione[9].

5. Si vedano sul punto le pertinenti considerazioni di Brighi–Chiara 2021, p. 22.
6. Comunicazione della Commissione, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, doc. COM(2001) 298 del 6 giugno 2001.
7. Comunicazione congiunta della Commissione e dell'Alto rappresentante, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, doc. JOIN(2013) 1 del 7 febbraio 2013. Qui si legge che "poiché la vasta maggioranza delle reti e dei sistemi informativi sono di proprietà privata e sono operati da privati, è essenziale coinvolgere maggiormente il settore privato nel rafforzamento della cibersicurezza. Il settore privato dovrebbe elaborare, a livello tecnico, capacità proprie di ciberresilienza e scambiare buone pratiche a livello intersettoriale".
8. Si veda, al riguardo, il considerando 56 della Direttiva 2022/2555 entrata in vigore il 16 gennaio 2023, ove si legge che "le piccole e medie imprese stanno diventando sempre di più il bersaglio di attacchi nella catena di approvvigionamento a causa delle loro misure meno rigorose di gestione del rischio di cibersicurezza e di gestione degli attacchi, nonché della limitata disponibilità di risorse destinate alla sicurezza. Tali attacchi della catena di approvvigionamento non solo hanno un impatto sulle piccole e medie imprese e sulle loro operazioni isolatamente, ma possono anche avere un effetto a cascata su attacchi più gravi nei confronti di soggetti di cui sono fornitori".
9. Si legga, per il caso italiano, il rapporto *Cyber Index PMI 2024*, elaborato dall'Agenzia per la Cybersicurezza Nazionale con il contributo del Politecnico di Milano, reperibile alla pagina Rapporto Cyber Index PMI: una fotografia della sicurezza digitale delle imprese italiane – ACN. Per una proiezione internazionale, si rinvia al *Cisco Cybersecurity Readiness Index 2025* (reperibile in Internet in cisco.com).

A fronte di questo atteggiamento culturale, le pur numerose normative – europee e interne – che riguardano la materia (e che si collocano nell'alveo di una evidente bulimia legislativa sui temi delle nuove tecnologie) non appaiono del tutto soddisfacenti. Esse prevedono obblighi per le imprese di adeguamento delle strutture di prevenzione e reazione del rischio cibernetico; tuttavia, oltre a riferirsi spesso solo ad alcune categorie di imprese (quelle coinvolte in settori di rilevanza strategica per lo Stato), tali obblighi sono presidiati soprattutto da sanzioni, in caso di mancato adempimento, secondo una logica norma-inadempimento-sanzione che non tiene adeguatamente conto, come mostrano le sopra ricordate statistiche, che la questione è culturale, *in primis*, ed economica, in secondo luogo. Non bastano, cioè, le regole e l'apparato sanzionatorio a corredo, perché in assenza di serie misure di formazione e di sostegno agli investimenti che tali regole richiedono, esse rischiano di rimanere sulla carta, poco più delle grida manzoniane che ben rappresentano – nell'immaginario collettivo – l'inutilità di una normazione di dettaglio che resta però estranea al sentire comune.

L'aspetto culturale, come formare le imprese (specie quelle di media e piccola dimensione) alla conoscenza dei rischi del mondo informatico e ai vantaggi che mirati investimenti possono realizzare (sganciando cioè la percezione dell'investimento dall'idea di un costo sostanzialmente inutile a fronte di un rischio futuro ed incerto), si collega del resto ad un profilo economico, nella consapevolezza che proprio le imprese tendono a rimandare investimenti dei quali non percepiscono l'immediata utilità e che la prospettiva di un supporto pubblico per tali investimenti (o al contrario la minaccia di un esborso aggiuntivo conseguente al mancato adeguamento) può influenzare grandemente le scelte dell'imprenditore. Si tratta di un approccio ben noto anche nel nostro ordinamento, nel quale le normative che introducono forme di compliance (si pensi ai modelli organizzativi per prevenire la commissione di certi reati a vantaggio delle imprese di cui al D.lgs. 231/2001) sono numerose e talvolta risalenti, ma in genere sono percepite dalle imprese come strumenti di aggravio della operatività quotidiana, privi di un immediato ritorno in termini di risparmi o di capacità di penetrazione del mercato e forieri di investimenti per i quali, quindi, la tendenza è quella a rimandare nel tempo, con il che la funzione preventiva che tali normative perseguono risulta già in partenza compromessa.

Va detto che il diritto europeo non trascura del tutto la dimensione culturale e formativa del fenomeno. La direttiva NIS 2 impone che le strategie nazionali di cibersicurezza comprendano un piano, corredato delle misure necessarie, per aumentare il livello generale di consapevolezza dei cittadini (art. 7, par. 1, lett. h) e che gli Stati membri adottino politiche volte, tra l'altro, a promuovere l'istruzione e la formazione in materia di cibersicurezza, le relative competenze e la diffusione di buone pratiche di igiene informatica presso cittadini, portatori di interessi e soggetti (art. 7, par. 2, lett. f), nonché, ed è ciò che più interessa in questa sede, a rafforzare la resilienza informatica e il livello di igiene informatica delle piccole e medie imprese, in particolare di quelle escluse dall'ambito di applicazione della direttiva, fornendo orientamenti e assistenza facilmente accessibili e rispondenti alle loro esigenze specifiche (art. 7, par. 2, lett. i). Sotto altro profilo, i membri degli organi di gestione dei soggetti essenziali e importanti sono tenuti a seguire una formazione, che gli Stati membri devono incoraggiare a offrire periodicamente anche ai propri dipendenti (art. 20, par. 2)[10]. Specifiche attività di sensibilizzazione e di formazione rivolte alle microimprese e alle piccole imprese sono previste, inoltre, dall'art. 33 del regolamento (UE) 2024/2847 (*Cyber Resilience Act*). A ciò si aggiungano le attività dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e del Centro europeo di competenza per la cibersicurezza (ECCC), che operano per promuovere una solida cultura della cybersicurezza nell'Unione[11].

10. Nell'ordinamento interno, la previsione è stata attuata dall'art. 23, secondo comma lett. b) del d.lgs. n. 138/2024, relativo agli obblighi degli organi di amministrazione e direttivi dei soggetti essenziali e importanti.

11. Si vedano l'art. 10 del regolamento (UE) 2019/881 (*Cybersecurity Act*), che attribuisce all'ENISA compiti di sensibilizzazione e di istruzione in materia di cibersicurezza, nonché il regolamento (UE) 2021/887, istitutivo del Centro europeo di competenza per la cibersicurezza (ECCC). Nella medesima direzione si colloca l'iniziativa della Commissione relativa all'Accademia per le competenze in materia di cibersicurezza, doc. COM(2023) 207 del 18 aprile 2023.

Tuttavia, tali iniziative manifestano un raggio d'azione circoscritto. Esse hanno per lo più una dimensione programmatica, che lascia all'intervento statale la relativa attuazione; inoltre, gli obblighi formativi ivi previsti riguardano prevalentemente i soggetti che rientrano nella disciplina applicativa della normativa, coinvolgendo quindi solo marginalmente le PMI. Soprattutto, tali discipline lasciano in secondo piano l'aspetto economico della formazione, ciò che come accennato costituisce il più rilevante ostacolo ad un adeguamento di tali operatori agli standard di sicurezza stabiliti a livello sovranazionale. Questo è proprio il profilo sul quale, come si vedrà, la leva fiscale può contribuire in misura maggiore.

Sotto questo profilo, la recente legge n. 132 del 23 settembre 2025 assume un approccio assai più propositivo, prevedendo tra le altre cose una serie di sostegni economici pubblici a favore di imprese che operano nel settore della sicurezza cibernetica, sotto forma di partecipazione al capitale di rischio[12]. È, dunque, apprezzabile il cambio di paradigma, dalla mera sanzione per gli inadempienti – rinvenibile anche nel decreto legislativo n. 138/2024 di recepimento della direttiva NIS 2, nonché nella legge n. 90/2024 recante "Disposizioni in materia di rafforzamento della cibersicurezza nazionale e di reati informatici" – a sostegni che sollecitino l'effettuazione di investimenti in strumenti organizzativi interni capaci di realizzare gli obiettivi di protezione dei singoli sistemi informatici e, di conseguenza, di evitare che tramite essi si possano verificare incursioni nel sistema di cybersicurezza nazionale. Tuttavia, la logica dei sussidi sembra poco coerente con gli obiettivi di formazione cui si accennava poc'anzi: il sussidio attinge, infatti, alla fiscalità generale ed il relativo sacrificio non è immediatamente percepibile dal soggetto beneficiato, spezzando così la catena virtuosa che dovrebbe unire il vantaggio ricevuto e l'apprezzamento del ruolo del soggetto pubblico nel reperimento delle relative risorse.

2. Il ruolo della fiscalità e le soluzioni "tradizionali"

Mi pare che, se davvero l'obiettivo è quello di realizzare un cambio culturale che conduca le imprese ad apprezzare la necessità, anche per il sistema nazionale nel suo complesso, di effettuare investimenti in infrastrutture di sicurezza informatica, allora non si possa che volgersi verso strumenti di natura fiscale. I tributi sono, infatti, potenti strumenti di natura pedagogica, nel senso che la prospettiva di ricevere un vantaggio (*sub specie* di agevolazione) ovvero di subire un esborso (sotto forma di maggiore importo da pagare) costituisce elemento di forte incentivazione a tenere certe condotte e, soprattutto, realizza un diretto (e direttamente percepibile) collegamento tra situazione individuale (di vantaggio o svantaggio) ed esigenze della collettività di appartenenza.

La funzione extrafiscale del tributo, visibile in una serie di prelievi di più recente introduzione nel nostro ordinamento come i tributi ambientali ovvero la *sugar tax*, consiste quindi nell'orientare i comportamenti dei consociati tramite la leva fiscale a prescindere dal ritorno che l'apparato pubblico possa averne in termini di gettito: così, il maggior costo pubblico conseguente all'attribuzione di una agevolazione viene compensato dai minori esborsi che conseguono al comportamento virtuoso del beneficiario (ad esempio, in termini di spese per il ripristino dell'ambiente); allo stesso modo, la finalità del tributo pedagogico (come può essere la *sugar tax*) è in questi casi non quella di massimizzare il gettito, bensì al contrario di eliminarlo, ciò che si realizza quando le condotte dei soggetti che ne sarebbero i destinatari si conformano perfettamente agli obiettivi dell'ordinamento, anche in questo caso consentendo allo Stato il risparmio di costi altrimenti inevitabili (per esempio, costi sanitari per cura delle persone obese)[13]. Il tema della fiscalità comportamentale sta, del resto, assumendo una posizione centrale nel dibattito tra gli studiosi, in un'epoca nella quale si moltiplicano stili di vita che appaiono contrari alle esigenze di

12. Si veda l'art. 23 della legge, che peraltro prevede al riguardo una dotazione di un miliardo di euro.

13. Sulla legittimità della *sugar tax,* introdotta nel nostro ordinamento tributario con la legge 160/2019, si è espressa la Corte Costituzionale, la quale con la sentenza 49/2024 ha stabilito che tale prelievo non contrasta con gli artt. 3 e 53 Cost., essendo volto alla realizzazione di condivisibili finalità extrafiscali. Su tale pronuncia, D'Ignazio 2025 e Mondini 2024.

sostenibilità e di tutela dei diritti della collettività, anche in proiezione intergenerazionale[14].

Peraltro, in un contesto come quello tratteggiato nel precedente paragrafo apparirebbe in prima battuta scontato concentrare l'attenzione del tributarista su strumenti di tipo agevolativo, i quali sollecitino le imprese a effettuare i necessari investimenti per la tutela dei propri sistemi tecnologici contro interferenze esterne ed ostili, con la prospettiva di un risparmio di imposta. In questo modo, l'ordinamento raggiunge il suo obiettivo – garantire che il tessuto delle imprese protegga i dati posseduti e, in conseguenza, scudi in modo efficace il sistema informatico nazionale nel suo complesso, contribuisca alla tenuta del mercato e protegga quindi anche i diritti fondamentali dei titolari di tali dati – scaricando il relativo costo sull'intera collettività, ma a fronte in ogni caso di una attività di interesse pubblico che i singoli operatori si sobbarcano, sgravandone di conseguenza i soggetti pubblici che ne sarebbero naturalmente preposti.

Si tratta dell'approccio seguito sin qui dal legislatore italiano in relazione alle innovazioni tecnologiche[15] – sebbene finora la finalità di adeguamento dei sistemi di cybersicurezza sia rimasta nascosta tra le pieghe di provvedimenti agevolativi aventi portata generalissima – e che, proprio con riguardo all'adozione di meccanismi di difesa da parte delle imprese, risulta essere preferito da quegli ordinamenti che se ne sono occupati, a partire dagli Stati Uniti fino ad esperienze europee ed extraeuropee, con l'unica, rimarchevole, eccezione della Nigeria[16].

Pur non sottovalutando l'efficacia delle misure agevolative per guidare le condotte dei destinatari delle stesse, occorre però considerare la particolarità del contesto del quale stiamo discorrendo. Una particolarità che riguarda lo speciale rango degli interessi coinvolti: la sicurezza nazionale (tra l'altro in un contesto di guerra ai confini della nazione), la sicurezza economica, intesa come tutela della resilienza del mercato e delle catene del valore, e il sistema dei diritti fondamentali. Ciò significa che l'agevolazione perde, al cospetto di tali situazioni, il proprio rilievo, dal momento che non si può più parlare di una opzione, di una libera scelta, del contribuente, se agire e ottenere il vantaggio fiscale ovvero se rinunciarvi. E ciò per il fatto che una rinuncia non può essere in ultima analisi consentita, dal momento che da essa possono derivare conseguenze nefaste non solo (e non tanto) per quel contribuente in sé considerato, ma per l'intera collettività nazionale. È quindi un dovere dotare la propria organizzazione di adeguati presidi contro il rischio di attacchi cibernetici, un dovere rispetto al quale non dovrebbe essere ammessa possibilità di scelta, venendo ad essere coinvolti interessi di rango costituzionale: l'esigenza di contribuire alla sicurezza nazionale potrebbe, invero, riconnettersi al dovere di fedeltà alla Nazione, di cui all'art. 54 Cost.; la tutela dei mercati potrebbe giustificare restrizioni alla libera iniziativa economica privata laddove, per l'appunto, occorra evitare danni alla sicurezza cui fa riferimento l'art. 41, comma 2, Cost.; mentre la necessità di agire a tutela dei diritti fondamentali discende direttamente dall'art. 2 Cost. e dall'inestricabile binomio tra diritti fondamentali e doveri inderogabili.

Certo, occorre evitare una eccessiva estensione dei rischi cibernetici nell'ambito delle questioni di sicurezza nazionale, dal momento che non è detto che ogni intrusione nei sistemi informativi di una impresa possa mettere a repentaglio interessi statali di tale rilievo. Si deve, pertanto, limitare

14. Si veda, nella prospettiva dei tributi ambientali, il recente studio di Ficari 2025.

15. Sono note le normative nostrane che prevedono crediti di imposta per investimenti in nuove tecnologie: dal piano transizione 4.0 (legge n. 178/2020) al successivo piano transizione 5.0, di cui al d.l. 19/2024. Il PNRR ha, peraltro, previsto numerose linee di azione a sostegno dell'adeguamento tecnologico delle imprese, non scordando anche l'ambito della cybersicurezza.

16. Gli Stati Uniti, a seguito dell'*Executive Order* del Presidente Biden del maggio 2021 (peraltro significativamente confermato dalla seconda amministrazione Trump), hanno previsto una serie di misure, consistenti principalmente in crediti di imposta, volte a incentivare le PMI all'adozione di adeguati sistemi di difesa informatica. Programmi simili si trovano nell'esperienza di Stati europei (Francia, Spagna), ma anche nel Regno Unito. Solo in Nigeria si assiste ad un intervento di segno diverso, essendo stata introdotta sin dal 2015 una modalità di finanziamento di un apposito fondo per la cybersecurity tramite, tra l'altro, una ritenuta che gli intermediari finanziari effettuano su ciascuna transazione elettronica (c.d. *cybersecurity levy*).

l'affermazione del dovere di cui si discorre ai soli casi nei quali l'impresa detenga dati rilevanti o sia interconnessa con i sistemi pubblici, ovvero ancora risulti inserita nella catena di approvvigionamento di soggetti critici, dal momento che solo in questi casi la sicurezza delle transazioni digitali intercetta un interesse pubblico alla sicurezza delle stesse.

Entro questi limiti, occorre, quindi, riscoprire nella materia in esame il valore del tributo, come strumento di orientamento delle condotte dei consociati e, ancor prima, come veicolo di partecipazione alla collettività, con il corredo di responsabilità che ad essa si connette. Voglio dire che, in un caso come quello della cybersicurezza che coinvolge una serie di situazioni soggettive fondamentali, di rango sia pubblico (la sicurezza dello Stato in tempo di guerra), sia collettivo (la tutela dei mercati e la sicurezza economica), sia individuale (la protezione dei dati e, conseguentemente, la difesa di taluni diritti fondamentali della persona), va enfatizzata la funzione del tributo come strumento solidaristico, attraverso il quale si realizza la compartecipazione dei costi di tutela e, quindi, l'assunzione di una responsabilità condivisa per beni e servizi che ridondano a vantaggio di tutti. Non uno strumento sanzionatorio[17], dunque, bensì il mezzo per una consapevole assunzione di responsabilità, come componenti di una comunità, verso minacce collettive che richiedono un intervento pubblico il cui costo deve necessariamente essere condiviso[18].

La questione che si pone – a parte considerazioni politiche, sulle quali non mi soffermo, circa la "presentabilità" di un nuovo tributo, in un contesto di iper-tassazione propria del nostro ordinamento tributario – è dunque quella della giustificazione di un simile tributo e, in conseguenza, della sua strutturazione.

È qui che si incontrano le principali difficoltà teoriche, che rimandano in parte al mai sopito dibattito circa il modo di essere della capacità contributiva nel nostro ordinamento.

La via in astratto più semplice, siccome già ampiamente arata con riferimento alle imposte ambientali, è quella del tributo *pigouviano*, che conduca all'internalizzazione delle esternalità negative che si connettono alla scelta dell'impresa di non dotarsi di adeguati meccanismi di cybersecurity e, quindi, costringono l'ordinamento – tramite la fiscalità generale – a rimediare a tale fallimento[19]. Si tratta di un tema che incontra ampio sostegno in dottrina, specie con riferimento all'impiego della leva fiscale per governare l'evoluzione dell'intelligenza artificiale[20], e che, tuttavia, si scontra con le innegabili difficoltà pratiche di realizzazione di un simile tributo, testimoniate dalla sostanziale assenza nel nostro ordinamento di prelievi di tal genere.

Si tratta, dunque, di immaginare nuove vie, peraltro in qualche modo necessitate dalla novità delle fattispecie di cui ci stiamo occupando, seguendo gli spunti che, sebbene in altri contesti, dottrina e giurisprudenza stanno già suggerendo a parziale superamento della concezione tradizionale del tributo e della capacità contributiva ad esso sottesa.

3. La cybersicurezza come bene comune e l'ipotesi di un tributo su una nuova forma di capacità contributiva

Possiamo muovere questa riflessione dalla valutazione della possibilità di considerare la cybersicurezza come un bene pubblico. Il tema dei "beni comuni" appassiona da tempo la dottrina costituzionalistica, trattandosi di un concetto che evoca naturalmente una dimensione che oltrepassa il singolo individuo, collocandosi in una prospettiva collettiva, in termini di appartenenza, e in un approccio centralizzato per quanto riguarda la relativa definizione e gestione[21]. Rispetto alla cybersicurezza occorre assumere, al riguardo, un approccio improntato alla cautela.

17. Su questo tema si suggerisce la lettura di Marello 2021.
18. Come osserva Antonini 2022, p. 6, "il dovere tributario, in conclusione, si configura come un dovere che attiene, come fine, prevalentemente alla relazione di solidarietà tra i componenti della società (anche se implica, come mezzo, l'istituzione statale), piuttosto che alla relazione verticale tra individuo e Stato (com'era nei doveri di soggezione)".
19. Per una applicazione del principio *pigouviano* alla tassazione ambientale, sia consentito rinviare a Dorigo 2024.
20. Si veda, tra gli altri, Pontillo 2022.
21. Per un inquadramento generale della categoria, cfr. Rodotà 2008.

Nella dottrina statunitense si registrano da tempo posizioni favorevoli ad annoverare in questa categoria la cybersecurity, collegando la sua corretta gestione alla realizzazione di interessi pubblici, come per l'appunto la difesa nazionale, la stabilità e la fiducia del mercato ed il sistema dei diritti individuali[22], che appaiono fondamentali nella moderna società dell'informazione[23]. Tuttavia, la tendenza prevalente è quella di individuare questa possibile qualificazione solo in alcuni specifici ambiti caratterizzanti la cibersicurezza, segnatamente quello della robustezza dei sistemi, escludendone viceversa altri che non appaiono essenziali per la sicurezza dei sistemi, come la responsività e la resilienza dei medesimi[24]. Molti prodotti e servizi di cibersicurezza (software antivirus, firewall, servizi di monitoraggio e di consulenza) sono, del resto, beni rivali ed escludibili, che il mercato è in grado di offrire e che l'impresa acquista a proprio beneficio; per contro, i caratteri della non rivalità e della non escludibilità si rinvengono essenzialmente nella robustezza dei sistemi, cioè nella loro capacità di resistere agli attacchi grazie a una progettazione sicura, e nella condivisione delle informazioni sulle vulnerabilità, mentre le funzioni di resilienza e di risposta, implicando attività di monitoraggio e di rilevamento delle minacce, richiedono un delicato bilanciamento con i diritti fondamentali che sconsiglia di attrarle integralmente nella logica del bene pubblico. A ciò si aggiunga che il livello di sicurezza di un sistema interconnesso dipende in larga misura da quello del suo anello più debole, ciò che fa della sicurezza complessiva della rete un bene pubblico del tipo c.d. *weakest link*, esposto per sua natura a comportamenti opportunistici[25]. È dunque in questa accezione, circoscritta alla dimensione sistemica della sicurezza della rete, che la qualificazione in termini di bene pubblico appare fondata.

L'approccio è, del resto, condivisibile nella misura in cui prende realisticamente atto che la cibersicurezza è fenomeno composito, che tocca ambiti, funzioni e finalità differenti, non tutti collegati ad un immediato interesse pubblico. La selezione di quali di questi elementi può essere trattato come bene pubblico è, quindi, rilevante, dal momento che ciò si traduce nella limitazione dell'ingerenza statale nelle scelte dei privati (e del mercato) e, allo stesso tempo, nella concentrazione delle (scarse) risorse disponibili solo dove viene in considerazione un genuino interesse collettivo.

Accogliendo questa prospettiva, allora, la sicurezza della rete così intesa non può essere valutata con la logica del mercato e dell'economia, ma deve essere classificata secondo "vincoli morali di reciprocità e solidarietà"[26]. In questo senso si muovono, del resto, quelle ricostruzioni del fenomeno che enfatizzano come la protezione della sicurezza delle reti debba essere valutata non soltanto con il metro degli interessi nazionali e sovranazionali ma, prima ancora, con il "riferimento a nuovi valori"[27]. Come oggetto di una "responsabilità condivisa" avente per l'appunto a oggetto valori da proteggere nell'interesse di tutti, discendente proprio dall'appartenenza solidaristica a una comunità, appare ragionevole attribuire ai componenti di questa il dovere di assumere comportamenti consapevoli, nella direzione di minimizzare i rischi e, quindi, di contribuire alla protezione dell'ambiente, della difesa nazionale e dei diritti e libertà fondamentali.

Peraltro, la considerazione della cybersicurezza quale bene pubblico (quanto meno nella sua componente riconducibile alla robustezza), comporta che essa non è escludibile, nel senso che deve essere garantita a tutti. Da qui l'emersione, come osservato in dottrina[28], del fenomeno dei *free riders*, ovvero di coloro che decidono di non assumersi alcuna responsabilità (nella specie, come sostenimento del costo di conformità agli standard di sicurezza),

22. Si veda l'opera di Mulligan–Schneider 2011. Si può, inoltre, rinviare a Weber 2017.
23. Tra gli altri, Floridi 2014.
24. Nel senso indicato si esprime Taddeo 2019.
25. Sul modello del c.d. *weakest link* applicato all'affidabilità dei sistemi informatici, Varian 2004 che riprende la classificazione dei beni pubblici proposta da Hirshleifer 1983.
26. Villani 2021, p. 125.
27. Così Brighi–Chiara 2021 p. 20.
28. De Benedetti 2018, p. 12.

nella consapevolezza che essi potranno comunque accedere ai benefici dell'azione pubblica che spetta, per l'appunto, a tutti. Ne consegue che è legittimo l'intervento pubblico per redistribuire il costo di tali misure su tutti i consociati, attraverso forme di obbligatoria partecipazione alle spese tramite prestazioni patrimoniali imposte, e quindi anche tramite tributi[29]. Un intervento – giova ripeterlo – che, coerentemente con la distinzione sopra tracciata, dovrebbe peraltro concentrarsi sulla componente sistemica della sicurezza, lasciando al mercato, e agli ordinari strumenti della responsabilità civile, della disciplina sulla protezione dei dati personali e dell'assicurazione, la gestione dei rischi che restano confinati entro la sfera dell'impresa e dei suoi interlocutori diretti.

Secondo questa prospettiva, allora, l'essenzialità e la natura pubblica del bene[30] giustificano il concorso di tutti ai relativi costi, secondo un'ottica fondata sulla solidarietà (l'appartenenza alla medesima comunità implica che tutti siano responsabili delle misure necessarie a difenderla) e sull'uguaglianza.

A ben vedere, è questo il medesimo esito al quale conduce la teoria della "capacità contributiva del non fare", coniata qualche anno or sono in relazione alla sentenza *Obamacare* della Corte Suprema Federale degli Stati Uniti[31]. In quella pronuncia, la Corte ritenne che la scelta di coloro che non erano disposti a sottoscrivere una polizza assicurativa sanitaria costituisse una rottura del patto di solidarietà tra i consociati, con la conseguenza che ad essi può imporsi l'obbligo di una prestazione patrimoniale che ripristini il sistema delle responsabilità reciproche all'interno della collettività, al fine di finanziare un fondo per l'accesso alla sanità di coloro che fossero privi dei relativi mezzi[32]. *Mutatis mutandis*, si può allora sostenere che l'impresa che non effettui gli investimenti necessari per dotarsi di un adeguato (nel senso di robusto) sistema di controllo del rischio cibernetico sta spezzando il vincolo di appartenenza con i relativi doveri, danneggiando non solo e non tanto se stessa, bensì gli altri individui, e – potenzialmente – il sistema economico e la nazione nel suo complesso, laddove essa sia inserita nella catena di approvvigionamento di soggetti critici o sia interconnessa con i sistemi pubblici, costringendo tali soggetti ad impiegare risorse per evitare il rischio, sviandole da altri impieghi a vantaggio (anche) della collettività.

Si tratta insomma, sembrano suggerire questi approdi, di mutare approccio laddove siano in gioco interessi così essenziali per la comunità (la sanità, nella vicenda dell'*Obamacare*, la sicurezza nazionale, economica ed individuale, nel caso che ci occupa) da giustificare deviazioni rispetto alle regole ordinarie della tassazione, perché l'esigenza di avere condotte responsabili ovvero di disporre (come gettito del tributo) di risorse aggiuntive

29. Risulta interessante osservare che, anche nella dottrina non tributaristica, il tema delle esternalità negative, scaturenti da una non corretta gestione del rischio cibernetico, viene declinato in termini economici, come possibilità per gli attori privati responsabili di tali fallimenti di scaricare il relativo costo sugli utenti finali (Brighi–Chiara 2021, p. 27). Si tratta di una interpretazione che richiama l'esigenza di azioni di riequilibrio da parte della mano pubblica, ciò che potrebbe avvenire – come si dirà a breve – anche mediante l'imposizione di specifiche prestazioni tributarie. Secondo un'autrice, "just like street-lights and national defence – both involve costs, while allowing all citizens of a state to access them and maintain them through their taxes – cybersecurity can function as a non-rivalrous, non-excludable good, if its costs are shared equitably among the relevant stakeholders" (Taddeo 2019, p. 351): anche in questo caso, è implicito un riferimento alla contribuzione fiscale come strumento ottimale per realizzare tale condivisione dei costi.

30. La robustezza dei sistemi di cybersecurity non è di per sé un bene pubblico, ma lo diventa laddove essa svolga una funzione essenziale per la collettività organizzata (così, ancora, Taddeo 2019, p. 352).

31. *National Federation of Independent Business v. Sebelius*, 567 U. S. 519 (2012). Sulla portata di tale sentenza, e sul concetto di "capacità contributiva del non fare" cui essa pare far riferimento, si veda l'analisi di Rosembuj 2012.

32. Gallo 2013 osserva che la "sanzione" di cui parla la sentenza sull'*Obamacare* "è, in realtà, una sovraimposta sul reddito (…), dalla quale ci si può sottrarre solo stipulando una polizza assicurativa sanitaria personale", ed aggiunge che tale posizione offre la dimostrazione che "anche la Corte Suprema è favorevole a considerare legittimi tributi che non hanno come esclusivo e diretto presupposto sostanziale la produzione di un reddito, la titolarità di un patrimonio o un atto di consumo" (p. 333).

deve prevalere, specie in situazioni di concreto pericolo come quelle che stiamo vivendo nel tempo presente.

È, del resto, ciò che la Corte costituzionale ha in qualche modo delineato nella sentenza n. 111/2024, laddove essa ha ritenuto legittimo un prelievo, che pure deviava da taluni elementi essenziali del nostro sistema tributario, in ragione sia dell'eccezionalità degli avvenimenti che lo avevano propiziato, sia della destinazione solidaristica del suo gettito[33]. Una presa di posizione, questa, che appare assai rilevante nella riflessione che si sta svolgendo, siccome indica che la concezione del tributo e la stessa ricostruzione della capacità contributiva possono subire mutamenti, adattandosi alle fattispecie estreme e inattese che il mondo contemporaneo produce, pur dovendo tuttavia continuare ad ancorarsi, per non sconfinare nell'arbitrio, sui capisaldi dell'art. 2 e dell'art. 3 della Costituzione.

Ragionando di capacità contributiva, è pur vero che il dibattito è ancora aperto tra coloro che la ricostruiscono riferendosi a indici di forza economica "autosufficienti"[34] e quanti, invece, postulano l'esigenza di sganciarsi dagli indici tradizionali (reddito e patrimonio) e di ancorare la tassazione anche a situazioni che, pur essendo valutabili economicamente, si limitano a segnalare una posizione di vantaggio del contribuente, a prescindere dalla disponibilità di "moneta" che esse gli procurano[35].

Mi pare però che rimanere fermi a tale contrapposizione, ormai consolidatasi da decenni, conduca a perdere di vista le nuove situazioni che si materializzano davanti ai nostri occhi per effetto di un mondo in continuo e rapido mutamento[36]. Non solo cambiano le fattispecie con le quali tocca confrontarsi, le quali spesso discendono da circostanze – la dematerializzazione dei beni e dei servizi – che rendono poco praticabile una loro riconduzione ad una o all'altra delle forme tradizionali di ricchezza; vi è anche che le situazioni di diseguaglianza si manifestano sempre più frequentemente in forme nuove, pensiamo alla povertà energetica, venuta alla ribalta in occasione della crisi indotta dallo scoppio della guerra russo-ucraina, ovvero alla possibilità di accesso alle nuove tecnologie e ai dispositivi fisici che ne sono il tramite, esplosa in tutta la sua drammaticità in occasione della crisi pandemica, ove il lockdown imposto a tutti ha rivelato come vi fossero intere fasce della popolazione non solo prive di tali strumenti, ma addirittura prive delle necessarie conoscenze di base[37].

Non solo, uno dei portati più significativi dell'epoca delle crisi in cui viviamo è che la logica proprietaria ed individualista, che fungeva da solida base della prima tesi, si è in qualche modo affievolita a fronte della necessitata ripresa del ruolo dello Stato e del suo intervento in funzione redistributiva. La pandemia del Covid-19 ha in effetti reso evidente che gli effetti del blocco delle attività economiche conseguente all'interruzione della libera circolazione delle persone sono stati resi meno dirompenti proprio grazie all'intervento pubblico, anche con risorse provenienti dall'ordinamento europeo. Tanto è vero che le istanze solidaristiche e redistributive sono diventate assolutamente preponderanti nella ricostruzione dell'obbligazione tributaria, anche al di fuori dei confini nazionali: mi riferisco, in particolare, al caso del contributo di solidarietà europeo a fronte dell'aumento del prezzo del gas in conseguenza dello scoppio della guerra russo-ucraina[38].

33. Su tale sentenza si veda il commento di Giovannini 2024, il quale si chiede se "gli eventi straordinari della storia possono influenzare l'interpretazione dei principi costituzionali, fra i quali quelli di solidarietà e d'uguaglianza contemplati negli artt. 2 e 3 e quello di capacità contributiva fissato nell'art. 53, comma 1, della Carta", osservando che "nella sentenza in esame la Corte risponde in modo affermativo".
34. Tra i tanti fautori dell'interpretazione citata, si può citare Moschetti 2006.
35. Per una recente rivisitazione di tale posizione, si veda Fedele 2023, partic. p. 7 ss.
36. Mi pare questa la posizione manifestata da Carpentieri 2024.
37. Per una disamina dei fenomeni accennati, proprio nella prospettiva della fiscalità e della finanza pubblica, si veda Supino–Voltaggio 2019. Sul tema della povertà tecnologica al tempo della pandemia, si rimanda a Zuddas 2020.
38. Regolamento (UE) 2022/1854 del Consiglio del 6 ottobre 2022 relativo a un intervento di emergenza per far fronte ai prezzi elevati dell'energia, ove nel considerando n. 14 si legge che "l'introduzione di un contributo

Il maggiore intervento richiesto all'apparato pubblico nel contesto della digitalizzazione e della moltiplicazione dei rischi cibernetici, anche al fine di tutelare diritti fondamentali individuali e collettivi, richiede risorse, onde non si può prescindere da un contributo di coloro che, come partecipi di una collettività organizzata, si avvantaggiano in ultima analisi da siffatto intervento. Proprio tale situazione di vantaggio può, dunque, essere valorizzata per quantificare il contributo di ciascuno al finanziamento delle spese pubbliche, in una prospettiva di uguaglianza e razionalità del prelievo.

Gli indici di vantaggio e di benessere, idonei ad evidenziare disuguaglianze in seno alla società, si sono del resto moltiplicati ed occorre prenderne atto, per evitare vuoti di tutela e di doverosa contribuzione, e proporre letture del fenomeno tributario che ne tengano adeguatamente conto.

Non è detto, del resto, che ogni tributo debba necessariamente passare attraverso una rigida applicazione della capacità contributiva *ex* art. 53 Cost. Come osservato da un autore, che ha proposto una provocatoria ricostruzione dei contorni del principio costituzionale[39], si potrebbe sostenere che tale disposizione si riferisca solo ai tributi che insistono su ricchezza e patrimonio, restando aperta la possibilità che esistano prestazioni patrimoniali imposte in relazione ad altri presupposti indicativi di una situazione di vantaggio.

Si tratta di spunti sui quali occorrono ulteriori riflessioni e che però potrebbero avere il pregio di offrire una prospettiva nuova che in qualche modo si impone al cospetto di fenomeni del pari nuovi e difficilmente inquadrabili nelle concezioni tradizionali, se non al prezzo di relegarli nell'irrilevanza, con approfondimento quindi delle disuguaglianze in una società già di per sé percorsa da tanti, troppi, divari in via di progressivo approfondimento. Viviamo un'epoca di disparità clamorose, all'interno dei singoli ordinamenti ma anche tra aree diverse del mondo: la funzione del tributo, come strumento redistributivo, è quindi da rivalutare, ma solo al prezzo di ammodernarne le categorie di base.

Il dibattito resta aperto ed i suoi approdi incerti, e forse la consapevolezza della rilevanza sociale e collettiva della cybersicurezza può contribuire a rendere urgente un serio dibattito su nuove concezioni del tributo e dei suoi presupposti. Certo che è venuto il tempo per ripensare il sistema di partecipazione alle spese pubbliche[40], valorizzando la comunità come luogo della solidarietà e, soprattutto, accettando che in situazioni di particolare ed eccezionale rilievo per la collettività nel suo complesso (situazioni coinvolgenti, ad esempio, la salute, l'ambiente, la difesa e la sicurezza individuale e collettiva) il concorso alle spese pubbliche possa essere ancorato a presupposti nuovi, in grado di esprimere, pur nella loro minimale valenza economica, le ragioni di una responsabilità condivisa e del doveroso afflato solidaristico, a prescindere dalla possibilità di rinvenire in essi gli elementi di ricchezza che tradizionalmente sono posti a base dei tributi[41]. Il tormentato esempio della *sugar tax* e della *plastic tax*[42] evidenzia quanto ancora lunga sia la strada che conduce a tali nuovi approdi. E tuttavia forse più che l'ambiente o la qualità delle bevande che assumiamo, è il pericolo alla

di solidarietà costituisce pertanto una misura congiunta e coordinata che, in uno spirito di solidarietà, permette la generazione di entrate supplementari a favore delle autorità nazionali per prestare sostegno finanziario alle famiglie e alle imprese pesantemente colpite dall'impennata dei prezzi dell'energia, garantendo condizioni di parità in tutta l'Unione".

39. Salanitro 2023.

40. Come già preconizzava, oltre venticinque anni or sono, Tremonti 1998.

41. Si tratta in qualche modo di una rivisitazione della teoria di Franco Gallo, ma limitata nei suoi effetti dal requisito dell'eccezionalità. Si veda in questo senso ancora Giovannini 2024, p. 6, il quale sostiene che "i diritti hanno due nuclei essenziali a seconda dell'estensione del dovere di solidarietà: uno valevole per i tempi ordinari, e in questi tempi quel nucleo non può essere scalfito; e un altro per i tempi straordinari, che invece possono legittimarne l'incisione per il prevalere del dovere solidaristico funzionale all'uguaglianza sostanziale e all'attuazione dei diritti sociali straordinariamente colpiti dagli eventi".

42. Sulla *sugar tax*, si veda Bartolazzi Menchetti 2025. Per un inquadramento della *plastic tax*, si veda Scuderi 2021.

sopravvivenza collettiva in tempo di guerra ibrida che può accelerare un nuovo modo di concepire l'appartenenza alla comunità e, quindi, i mezzi finanziari per assumersi le relative responsabilità.

Riferimenti bibliografici

L. Antonini (2022), *Introduzione*, in V. Mastroiacovo, G. Melis (a cura di), "Il diritto costituzionale tributario nella prospettiva del terzo millennio", Giappichelli, 2022

E.M. Bartolazzi Menchetti (2025), *"Sugar tax", tributi con scopi extrafiscali e tutela della salute*, in "Tax News - Supplemento online alla Rivista Trimestrale di Diritto Tributario", 7 marzo 2025

A. Bonfanti (2018), *Attacchi cibernetici e cyber war: considerazioni di diritto internazionale*, in "Notizie di Politeia", 2018

C. Brighi, P.G. Chiara (2021), *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in "federalismi.it", 2021, n. 21

L. Carpentieri (2024), *Nuovi presupposti d'imposta e nuovi criteri di determinazione delle basi imponibili: riflessioni de iure condito e de iure condendo*, in "Rivista telematica di diritto tributario", 11 gennaio 2024

M. De Benedetti (2018), *La cyber sicurezza come nuova dimensione della difesa dello Stato: bene meritorio o bene pubblico?*, in "federalismi.it", 25 aprile 2018

M. D'Ignazio (2025), *La Sugar Tax al vaglio della Corte costituzionale: alcune riflession*i, in "Rivista trimestrale di diritto tributario", 2025

S. Dorigo (2024), *Transizione ecologica, agevolazioni fiscali ed affievolimento del divieto di aiuti di Stato: un assetto in cerca di equilibrio*, in "Rivista trimestrale di diritto tributario", 2024

A. Fedele (2023), *Nuove ricchezze ed elementi essenziali della capacità contributiva nella dimensione postmoderna*, in "Rivista di diritto tributario", 2023

V. Ficari (2025), *Fiscalità e sostenibilità ambientale nella transizione ecologica delle attività economiche*, Giappichelli, 2025

L. Floridi (2014), *The fourth revolution. How the infosphere is reshaping human reality*, Oxford University Press, 2014

F. Gallo (2013), *Ancora in tema di uguaglianza tributaria*, in "Rivista di diritto finanziario e scienza delle finanze", 2013

A. Giovannini (2024), *La capacità contributiva ai tempi straordinari della storia: un appunto*, in "Rivista telematica di diritto tributario", 28 settembre 2024

J. Hirshleifer (1983), *From weakest-link to best-shot: The voluntary provision of public goods*, in "Public Choice", 1983

E. Marello (2021), *Pulsioni oscure: l'imposta come sanzione*, in "Rivista di diritto finanziario e scienza delle finanze", 2021

A. Mondini (2024), *Il fine extrafiscale giustifica i mezzi (con la virtù della scienza). Considerazioni intorno alla costituzionalità della sugar tax e della fiscalità comportamentale*, in "Rivista di diritto finanziario e scienza delle finanze", 2024

F. Moschetti (2006), *Il principio di capacità contributiva, espressione di un sistema di valori che informa il rapporto tra singolo e comunità*, in L. Perrone, C. Berliri (a cura di), "Diritto tributario e Corte costituzionale", Edizioni Scientifiche Italiane, 2006

D.K. Mulligan, F.B. Schneider (2011), *Doctrine for cybersecurity*, in "Daedalus", 2011

S. Pietropaoli (2025), *Informatica criminale. Diritto e sicurezza nell'era digitale*, Giappichelli, 2025

M. Pontillo (2022), *Robot Tax: possibili modelli di prelievo tra consensi e resistenze*, in "Rivista telematica di diritto tributario", 30 giugno 2022

S. Rodotà (2008), *I beni comuni. L'inaspettata rinascita dei beni collettivi*, La Scuola di Pitagora, 2008

T. Rosembuj (2012), *La capacità contributiva del 'non fare'. Il concetto di imposta. A proposito di una importante sentenza della Corte Suprema degli USA*, in "Diritto e pratica tributaria", 2012

G. Salanitro (2023), *Sugar tax e plastic tax. Quando il tributo litiga con la capacità contributiva…*, in "Rivista di diritto tributario", 2023

E. Scuderi (2021), *Towards a plastic-free economy: The Italian plastic tax*, in "Rivista telematica di diritto tributario", 7 aprile 2021

S. Supino, B. Voltaggio (2019), *La povertà energetica. Strumenti per affrontare un problema sociale*, il Mulino, 2019

M. Taddeo (2019), *Is cybersecurity a public good?*, in "Minds & Machines", vol. 29, 2019

G. Tremonti (1998), *La fiscalità nel terzo millennio*, in "Rivista di diritto finanziario e scienza delle finanze", 1998

H.R. Varian (2004), *System reliability and free riding*, in L.J. Camp, S. Lewis (eds.), "Economics of Information Security", Springer, 2004

S. Villani (2021), *Spunti per una rivoluzione fiscale che acceleri la transizione ecologica e la riduzione delle disuguaglianze dopo la pandemia da COVID-19*, in "Rassegna tributaria", 2021

S. Weber (2017), *Coercion in cybersecurity: What public health models reveal*, in "Journal of Cybersecurity", 2017

G. Ziccardi (2019), *Tecnologie per il potere*, Raffaello Cortina Editore, 2019

P. Zuddas (2020), *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in "Osservatorio costituzionale", 2020, n. 3