CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Annalisa Ciampi

"SOVRANITÀ TECNOLOGICA QUALE ELEMENTO FONDAMENTALE PER LO SVILUPPO DELL'AUTONOMIA STRATEGICA NAZIONALE"

(AR-SGD-03)

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della Difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.

L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e cyber security; Giuridica.

L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.

L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche.

L'IRAD si avvale altresì per le attività d'istituto di personale qualificato "ricercatore della Difesa, oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato.

L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore dalla Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.

CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Annalisa Ciampi

"SOVRANITÀ TECNOLOGICA QUALE ELEMENTO FONDAMENTALE PER LO SVILUPPO DELL'AUTONOMIA STRATEGICA NAZIONALE"

(AR-SGD-03)

"SOVRANITÀ TECNOLOGICA QUALE ELEMENTO FONDAMENTALE PER LO SVILUPPO DELL'AUTONOMIA STRATEGICA NAZIONALE"

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dell'autore, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali l'autore stesso appartiene.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

Questo volume è stato curato dall'**Ufficio Studi, Analisi e Innovazione dell'IRAD**.

Direttore
Col. c. (li) s. SM Gualtiero Iacono

Capo dell'Ufficio Studi, Analisi e Innovazione
Col. AArnn Pil. Loris Tabacchi

Progetto grafico
Ass. Amm. Massimo Bilotta – 1° Mar. Massimo Lanfranco – C° 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello

Revisione e coordinamento
Ten. Col. (AM) Luigi Bruschi – S.Ten. Elena PICCHI – Funz. Amm. Aurora Buttinelli – Ass. Amm. Anna Rita Marra

Autore
Annalisa Ciampi

Stampato dalla Tipografia del **Centro Alti Studi per la Difesa**

Istituto di Ricerca e Analisi della Difesa
Ufficio Studi, Analisi e Innovazione
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3205
e-mail: irad.usai.capo@casd.difesa.it

chiusa a ottobre 2022

ISBN 979-12-5515-018-3

INDICE

Sommario

Scopo della presente ricerca è: «Fornire un quadro metodologico per l'implementazione di provvedimenti atti a sviluppare la Sovranità Tecnologica della nazione in funzione del perseguimento del massimo livello possibile di Autonomia Strategica».

A tal fine, il Capitolo I definisce, innanzitutto, e qualifica i concetti di Sovranità Tecnologica (a partire dal *Position Paper* del Centro Economia Digitale di marzo 2021) e di Autonomia Strategica (paragrafo 2), anche alla luce degli sviluppi e accelerazioni impressi dalla pandemia da COVID-19 e, più recentemente, dal conflitto russo-ucraino (ancora in corso – da sei mesi – alla data in cui si scrive) (paragrafo 5). Si sofferma, quindi, sulla trasformazione digitale e offre una panoramica dei settori maggiormente coinvolti: i settori produttivi, con un particolare impatto sul comparto Aerospazio, Difesa e Sicurezza (AD&S), ma anche la Pubblica Amministrazione (PA), i servizi pubblici e tutte le funzioni essenziali dello Stato, oltre alla Difesa (paragrafo 3). Passa, infine, in rassegna i diversi attori coinvolti nella Transizione Tecnologica. Soggetti portatori di interesse sono gli attori istituzionali (Ministeri, la Presidenza del Consiglio dei Ministri, le Regioni, e altri) ma anche i privati (produttori e fornitori di beni e servizi), il mondo accademico e della ricerca, e la società civile, intesa sia come beneficiaria dei relativi servizi sia come cittadinanza attiva (paragrafo 4).

L'area della Sovranità Tecnologica e dell'Autonomia Strategica che da essa consegue, risulta quantomai trasversale sia dal punto di vista dei dominii interessati che degli attori coinvolti. Ciò rende la *Governance Digitale* piuttosto complessa e, come si vedrà, la relativa architettura istituzionale abbastanza frammentata.

Un quadro di insieme degli impegni assunti (o da assumere) dall'Italia nell'ambito delle organizzazioni e *fora* internazionali in cui si discute di *Digital Governance*, è essenziale affinché la diplomazia italiana possa essere adeguatamente inserita nei circuiti di informazione, indirizzo e azione che riguardano la Sovranità Tecnologica, affinché la partecipazione italiana possa svolgersi in conformità alle esigenze di Autonomia Strategica nazionale.

Il Capitolo II prende, quindi, in considerazione i molteplici *fora* internazionali cui partecipa l'Italia, sia a livello governativo che attraverso attori privati, e offre un quadro di insieme delle molteplici iniziative – soprattutto nell'ambito di organizzazioni internazionali – rilevanti rispetto al tema della *governance* della Transizione Tecnologica, in particolare Digitale.

Nell'ordine, sono esaminati: il *Global Digital Compact* – iniziativa proposta dal Segretario Generale delle Nazioni Unite a settembre 2021 (paragrafo 2) – e l'*Internet Governance Forum* (IGF), anche nella sua declinazione italiana (c.d. IGF Italia) – anch'esso promosso dalle Nazioni Unite a partire dal 2006 (paragrafo 3); le *Confidence Building Measures* (CBM) adottate dall'Organizzazione per la Sicurezza e la Cooperazione in Europea (OSCE) e le *policies* e gli strumenti elaborati in sede di Organizzazione per la cooperazione e lo sviluppo economico (OECD) (paragrafi 4-5); le iniziative, all'interno e fuori dell'Organizzazione mondiale del commercio (OMC), per la regolamentazione del commercio internazionale digitale (paragrafo 6); la Strategia per la cybersicurezza e la Bussola strategica per la sicurezza e la difesa adottate dall'Unione europea (UE), rispettivamente, a dicembre 2020 e marzo 2022 (paragrafo 7); e, infine, i recenti indirizzi strategici della *North Atlantic Treaty Organization* (NATO), adottati nel Summit di Madrid del 28-30 giugno 2022 (paragrafo 8).

Il Capitolo III prende in esame i fondi stanziati sia attraverso strumenti finanziari nazionali che nell'ambito dei programmi di investimento dell'UE, per intensificare i progetti di sviluppo tecnologico e quindi garantire un adeguato livello di Autonomia Strategica.

Per quanto riguarda i fondi nazionali, vi sono oltre gli strumenti finanziari già assegnati alle Amministrazioni, i fondi derivanti da una quota percentuale (1,2%) degli investimenti nazionali lordi su base annuale da dedicare a specifiche progettualità volte a traguardare il conseguimento dell'autonomia tecnologica in ambito digitale. Sul piano dell'UE, sono rilevanti: il Programma Orizzonte Europa (con un bilancio totale per il 2021-2027 di 95,51 miliardi di Euro); il Programma Europa Digitale (che ha un bilancio totale per il medesimo periodo – 2021-2027 – di 7,59 miliardi di Euro); e il *Next Generation EU* (NGEU), un pacchetto di misure e stimoli economici per i Paesi membri – tra queste, la *Recovery and Resilience Facility* (RRF) a cui sono destinati 672,5 miliardi dei 750 totali di NGEU e per beneficiare il quale l'Italia ha adottato il c.d. Piano Nazionale di Ripresa e Resilienza, o PNRR. Il PNRR transizione digitale, relativo alla Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo" ha un bilancio totale di 122,6 miliardi di Euro, per il periodo 2021-2026.

Il medesimo Capitolo III, *in fine*, accenna anche al ruolo della Agenzia per la Cybersicurezza Nazionale (ACN), istituita dal decreto-legge 14 giugno 2021 n. 82, e del Dipartimento per la Trasformazione Digitale (DTD), istituito nel 2019 presso la Presidenza del Consiglio dei Ministri, quali amministrazioni responsabili della implementazione dei suddetti programmi e titolari dei relativi investimenti e soggetti.

Il Capitolo IV approfondisce quindi taluni aspetti della nuova architettura nazionale *cyber*, introdotta con il decreto-legge 14 giugno 2021 n. 82.

Come vedremo, l'istituzione dell'ACN risponde all'esigenza di riordinare, razionalizzare e semplificare le competenze nazionali in materia di sicurezza cibernetica (prima frammentate e poste in capo a una pluralità di attori istituzionali), creando un ente centrale con competenza in materia, che possa anche rappresentare il punto di raccordo tra i diversi soggetti interessati: oltre ai Dicasteri (Min. Difesa, Interno, MITD, MEF, MAECI, etc.), organismi di coordinamento, Enti di ricerca, Associazioni industriali, etc. Come si vedrà, le funzioni attribuite alla ACN esprimono un approccio olistico alla gestione della cybersicurezza ma anche, più in generale, alla Sovranità Tecnologica. In linea di principio, dunque, la nuova architettura nazionale si presta – sia pure con alcune criticità – a fornire il quadro di riferimento per lo sviluppo della Sovranità Tecnologica del nostro Paese.

Le Conclusioni ricapitolano le *premesse definitorie e metodologiche* illustrate nel Capitolo I. Formulano quindi alcune considerazioni propositive per il rafforzamento dell'unicità di indirizzo e di azione, in funzione del perseguimento dell'Autonomia Strategica nazionale – nel rispetto delle competenze attribuite alle Amministrazioni dalla normativa vigente e tenendo conto dell'insieme degli *impegni assunti o da assumere da parte dell'Italia sul piano internazionale e dell'UE* e delle opportunità offerte dagli *strumenti finanziari* e i *programmi di investimenti* attualmente in essere.

Abstract

The purpose of this research is: “To provide a methodological framework for the implementation of measures to develop the Nation's Technological Sovereignty in pursuit of the highest possible level of Strategic Autonomy”.

To this end, Chapter I first defines and qualifies the concepts of Technological Sovereignty (starting with the Position Paper of the Digital Economy Center of March 2021) and Strategic Autonomy, also in light of the developments and accelerations imprinted by the COVID-19 pandemic and, more recently, the Russian-Ukrainian conflict (still ongoing at the date of writing). It then dwells on Digital Transformation and offers an overview of the sectors most affected: all productive sectors, with a particular impact on Aerospace, Defense and Security (AD&S), but also the Public Administration (PA), public services and all essential functions of the state, in addition to Defense. Chapter I also passes in review the various actors involved in the Technological Transition. Stakeholders include institutional actors (ministries, the Prime Minister's Office, the Regions, and others) but also private actors (producers and suppliers of goods and services), academia and research institutions, as well as civil society – the latter understood both as beneficiary of the relevant services and as active citizenship.

As we shall see, the area of Technological Sovereignty, particularly Digital Sovereignty, and thus the Strategic Autonomy associated with it, is cross-cutting from the perspective of both the domains and the actors involved. This makes the governance of the strategy quite complex and the resulting institutional framework rather fragmented.

An overview of the commitments made (or to be made) by Italy in international organizations and fora in which digital governance is discussed is essential, so that Italian diplomacy can be adequately included in the circuits of information, direction and action concerning Technological Sovereignty, and Italy’s participation can take place in accordance with the requirements of national Strategic Autonomy.

Chapter II thus considers the multiple international fora in which Italy participates both at the governmental level and through private actors and offers an overview of the many initiatives – especially within international organizations – relevant with respect to the issues of governance of digital transformation.

The following are examined, in order: the Global Digital Compact - an initiative proposed by the UN Secretary General in September 2021 - and the Internet Governance Forum (IGF), also in its Italian declination (c.d. IGF Italy) - also promoted by the UN since 2006; the Confidence Building Measures (CBM) adopted by the Organization for Security

and Cooperation in Europe (OSCE); and the policies and tools developed in the Organization for Economic Cooperation and Development (OECD); the initiatives, within and outside the World Trade Organization (WTO), for the regulation of international digital trade; the Cybersecurity Strategy and the Strategic Compass for Security and Defense adopted by the European Union (EU) in December 2020 and March 2022, respectively; and, finally, the recent strategic directions of the North Atlantic Treaty Organization (NATO), adopted at the Madrid Summit of June 28-30, 2022.

Chapter III examines the funds allocated through both national financial instruments and EU investment programs designed to intensify technological development projects and thus ensure an appropriate level of Strategic Autonomy. With regard to national funds, there are in addition to the financial instruments already allocated to the Administrations, funds derived from a percentage share (1.2%) of gross national investment on an annual basis to be dedicated to specific projects aimed at targeting the achievement of technological autonomy in the digital sphere. On the EU level, relevant are: The Horizon Europe Program (with a total budget for 2021-2027 of 95.51 billion euros); the Digital Europe Program (which has a total budget for the same period - 2021-2027 - of 7.59 billion euros); and the Next Generation EU (NGEU), a package of economic measures and stimuli for member countries - among them, the Recovery and Resilience Facility (RRF) to which 672.5 billion of the total 750 of NGEU is allocated and to benefit from which Italy has adopted the c. d. National Recovery and Resilience Plan, or PNRR. The PNRR digital transition, related to Mission 1 "Digitalization, Innovation, Competitiveness, Culture and Tourism" has a total budget of 122.6 billion euros, for the period 2021-2026.

Chapter III also mentions, *in fine*, the role of the National Cybersecurity Agency (NCA), established by Decree-Law No. 82 of June 14, 2021, and the Department for Digital Transformation (DTD), established in 2019 at the Prime Minister's Office, as the administrations responsible for the implementation of the aforementioned programs, and the owners of the related investments.

Chapter IV delves into the recent reform, introduced with Decree-Law No. 82 of June 14, 2021, which designed the new national cyber architecture. The establishment of the ACN responds to the need to reorganize, rationalize and simplify national cyber security competencies (previously fragmented and placed in the hands of a plurality of institutional actors), creating a central body with competence in the field, which can also represent the point of connection between the different stakeholders: Ministries (Min. Defense, Interior, MITD, MEF, MAECI, PCD..), various Agencies and Coordinating Bodies, Research Institutions, Industrial Associations etc.

The establishment of the ACN responds to the aim of enabling the implementation of strategic objectives within a coordinated and harmonized system, in which the uniqueness of the direction defined by the political leadership is guaranteed, in the process of implementation, through the organized action of the actors involved - while respecting the competencies attributed by current legislation to other Administrations.

The functions assigned to the ACN express a “holistic approach" not only to cybersecurity management, but more generally to Technological Sovereignty. The new national architecture for the management of cybersecurity incidents and crises thus lends itself to provide the framework for the development of our country's Technological Sovereignty. This framework, however, need to be implemented keeping in mind – with an equally holistic view – the set of commitments made or to be made by Italy at the international and the EU levels as well as the opportunities offered by the financial instruments and investment programs currently in place.

The Conclusions thus recapitulate the definitional and methodological premises outlined in Chapter I and further advance some proposals for strengthening the unity of direction and action – while respecting the competencies attributed to the Administrations by the current legislation – in the pursuit of national Strategic Autonomy.

Capitolo I. Concetti, settori interessati e soggetti coinvolti

1. Premessa

Scopo della presente ricerca è: «Fornire un quadro metodologico per l'implementazione di provvedimenti atti a sviluppare la Sovranità Tecnologica della nazione in funzione del perseguimento del massimo livello possibile di Autonomia Strategica». Occorre, dunque, innanzitutto, definire e qualificare i concetti di Sovranità Tecnologica (a partire dal Position Paper del Centro Economia Digitale di marzo 2021) e di Autonomia Strategica, anche alla luce degli sviluppi e accelerazioni impressi dalla pandemia da COVID-19 e, più recentemente, dal conflitto russo-ucraino (ancora in corso – da sei mesi – alla data in cui si scrive). Ci si sofferma, quindi, sulla trasformazione digitale con una panoramica dei settori maggiormente coinvolti: i settori produttivi, con un particolare impatto sul comparto Aerospazio, Difesa e Sicurezza (AD&S), ma anche la Pubblica Amministrazione (PA), i servizi pubblici e tutte le funzioni essenziali dello Stato, oltre alla sua difesa. Si passano in rassegna, infine, i diversi attori coinvolti nella transizione tecnologica: soggetti portatori di interesse sono gli attori istituzionali (ministeri, la Presidenza del Consiglio dei Ministri, le Regioni, e altri) ma anche i privati (produttori e fornitori di beni e servizi), il mondo accademico e della ricerca, e la società civile, intesa sia come beneficiaria dei relativi servizi che come cittadinanza attiva.

2. Sovranità tecnologica: che cosa e perché. I concetti di "autonomia" e "partnership affidabili" e i profili di rilevanza della ricerca

Secondo il *Position Paper* pubblicato dal Centro economia digitale (CED) a marzo 2021, è possibile definire la Sovranità Tecnologica come "l'abilità di generare conoscenza tecnologica e scientifica autonomamente o di utilizzare capacità tecnologiche sviluppate altrove attraverso l'attivazione di *partnership* ritenute affidabili" (CED 2021, p. 18). Questa definizione necessita a sua volta di essere specificata con riferimento ai concetti di "autonomia" e "*partnership* affidabili".

Sotto il primo profilo, lo stesso *Position Paper* riconosce che la definizione data "non implica un'autonomia tecnologica *tout court*, che metta in discussione la divisione internazionale del lavoro e che preveda la necessità di sviluppare capacità tecnologiche autonome in tutti i campi ritenuti strategici. Tuttavia, suggerisce la necessità che un singolo Paese (o una federazione di Stati come nel caso dell'UE) sviluppi o preservi, con riferimento a tecnologie fondamentali, una propria autonomia, o una dipendenza strutturale più bassa possibile" (*ibidem*).

Si ritiene al riguardo, che il concetto stesso di “autonomia”, sia esso riferito alle conoscenze tecnologiche e/o scientifiche o alle strategie di cui si dirà più avanti, non possa essere inteso in termini assoluti. L’interdipendenza caratterizza ormai da decenni il modo di essere di tutti i soggetti internazionali (a partire dagli Stati sovrani alle organizzazioni, ivi comprese quelle di tipo transnazionale come l’UE) e non (pubblici e privati, come università, enti di ricerca e imprese). Negare l’interdipendenza significa negare l’evidenza ma anche un dato in qualche misura ineliminabile nella nostra società in tutte le sue dimensioni (scientifica e tecnologica, così come economica, sociale e culturale). Porre l’autonomia assoluta in qualunque settore come obiettivo da raggiungere o cui tendere equivale a fare dell’utopia. Oltre che inutile, ciò potrebbe risultare dannoso, o comunque non virtuoso rispetto alla realizzazione di altri obiettivi, primo fra tutti quello della *competitività*. Per affrontare i problemi di dipendenza, occorrono piani specificamente mirati a ridurre la dipendenza in settori strategici ma anche ad aumentare le proprie quote di mercato nazionale e internazionali, se del caso creando alleanze. Il rischio altrimenti è che la riduzione delle dipendenze si realizzi al prezzo della perdita di quote significative di mercato in settori significativi – a vantaggio degli stessi soggetti verso cui si è ridotta la dipendenza o di altre economie in crescita.

La definizione del *Position Paper* – che per espressa previsione – costituisce il punto di partenza della ricerca, necessita dunque di qualificazione, nel senso che oggetto della “sovranità tecnologica”, alla cui realizzazione il presente lavoro mira a contribuire, non può essere l’autonomia “in senso assoluto” ma neppure l’autonomia “nella più alta misura possibile”. L’autonomia da valorizzare e costruire è quella ottimale per ciascun settore, il cui livello non coincide necessariamente con quella massima possibile realizzabile.

Oltre a non poter essere equiparato a quello massimo realizzabile possibile, il livello ottimale non si presta nemmeno ad essere individuato una volta per tutte e unitariamente con riferimento alle conoscenze tecnologiche e scientifiche. Viceversa, esso dovrà essere stabilito in relazione ai singoli ambiti di conoscenza e/o i settori rilevanti per il loro impiego – con una valutazione destinata a mutare con l’evolversi delle conoscenze, delle trasformazioni da queste generate e dei cambiamenti del quadro geoeconomico e geopolitico generale.

Di qui, un primo profilo di rilevanza della ricerca, che una volta disancorata la Sovranità Tecnologica dal parametro di una irraggiungibile, e neppure desiderabile, autonomia assoluta o comunque della dipendenza strutturale più bassa possibile, non ha neppure l’ambizione di stabilire essa stessa il suo livello ottimale. Più concretamente, obiettivo della ricerca è fornire un quadro metodologico per l’implementazione di provvedimenti atti a

sviluppare la Sovranità Tecnologica della nazione e, quindi – preliminarmente – per l'individuazione del livello ottimale, *caso per caso*, di Autonomia Strategica da perseguire.

L'altro elemento della definizione che occorre specificare riguarda la Sovranità Tecnologica intesa come abilità di "utilizzare capacità tecnologiche sviluppate altrove attraverso l'attivazione di *partnership* ritenute affidabili". A questo riguardo, il *Position Paper* segnala l'opportunità di evitare dipendenze unilaterali, soprattutto nei confronti di *partner* internazionali ritenuti meno affidabili. Si tratta di una componente della massima importanza, di cui occorre esplicitare il significato, a maggior ragione se posto in relazione con la necessaria qualificazione del concetto stesso di "autonomia", come sopra evidenziata.

Evitare "dipendenze unilaterali" è certamente essenziale ai fini dell'Autonomia Strategica, correttamente intesa. Evitare dipendenze unilaterali significa innanzitutto saperle riconoscere ed individuare. Evitarle nei confronti di *partner* internazionali ritenuti non affidabili implica, a sua volta, la capacità di discernere fra *partner* internazionali in relazione alla loro maggiore o minore "affidabilità".

Al riguardo, la bilateralità di una *partnership* non è affatto garanzia di affidabilità. Perché si realizzi una *partnership* affidabile, non basta che la dipendenza sia reciproca, ma occorre che la stessa riguardi prestazioni di importanza strategica analoga o equivalente per le parti interessate. Anche questo elemento può non essere di facile conoscenza, a meno di ridurre il concetto di *partnership* affidabile a poche ipotesi di immediata evidenza. Affidabile, ad esempio, è la *partnership* fra due piccole e medie imprese (PMI) per il reciproco scambio di componenti e/o materie prime. Ma virtuose possono essere anche *partnerships* non direttamente fondate su un rapporto sinallagmatico con scambio di reciproche prestazioni, laddove inserite all'interno di *partnerships* più ampie nell'ambito, ad esempio, del comparto industriale di cui fa parte la PMI coinvolta, a livello statale oppure europeo. Ne consegue che ai fini della "bilateralità" così come della "affidabilità" delle dipendenze *virtuose* nel senso sopra delineato, il concetto stesso di "parti interessate" deve essere definito in maniera ampia: non vi rientra solo la singola impresa che ha necessità di utilizzare la capacità tecnologica sviluppata altrove, il singolo ente o università coinvolta, o la specifica amministrazione nella cui competenza ricade l'oggetto cui è finalizzata la prestazione. "Parte interessata" ai fini della realizzazione o del mantenimento della Sovranità Tecnologica, è lo Stato nel suo complesso, anche alla luce degli accordi di cooperazione esistenti sul piano internazionale sia bilateralmente che a livello multilaterale nell'ambito delle organizzazioni internazionali di cui fa parte – per l'Italia, naturalmente, l'ambito più rilevante è quello della UE.

Di qui, un altro profilo di rilevanza del quadro metodologico obiettivo della presente ricerca: fornire strumenti utili a valutare, di volta in volta, l'opportunità di *partnerships* attraverso la piena conoscenza di tutte le parti coinvolte e del contesto internazionale generale.

Così precisati i concetti di Autonomia e *Partnerships* affidabili quali componenti fondamentali della Sovranità Tecnologica, occorre ora provare a definirne l'ambito con riferimento ai settori più direttamente interessati, prima di individuare gli attori coinvolti.

3. Sovranità Tecnologica: Trasformazione (o Transizione) Digitale e settori interessati

In tema di Sovranità Tecnologica, "particolare attenzione in termini di Autonomia Strategica, è attribuita alle **tecnologie digitali** in quanto trasversali, abilitanti e sensibili dal punto di vista della sicurezza" (CED 2021, p. 18). Tra di esse rientrano – ad esempio – reti e protocolli di comunicazione di ultima generazione (5G e 6G), *blockchain*, intelligenza artificiale (AI), *quantum computing*, High Performance Computing (HPC), *Internet of Things* (IoT), robotica, strumenti crittografici evoluti e altre innovazioni.

Come efficacemente messo in luce nella *Strategia nazionale di cybersicurezza 2022-2026* (d'ora innanzi anche semplicemente "Strategia"): "Velocità di connessione, numerosità di interazioni tra utenti e accessibilità di dati e informazioni *on-line* non sono parametri sufficienti a definire lo sviluppo digitale che caratterizza l'età contemporanea, né riescono a descrivere, nella sua interezza, quell'articolata dimensione che chiamiamo spazio cibernetico. In tale dominio trovano posto, interconnessi e comunicanti, innumerevoli servizi concepiti per il soddisfacimento delle quotidiane esigenze delle nostre comunità e per lo svolgimento delle relative attività economiche: infrastrutture energetiche, mercati finanziari, forniture di acqua potabile, trasporti di massa, e, non ultime, le funzioni essenziali dello Stato, incluse la sua difesa e integrità. La complessità e l'interdipendenza dei sistemi è cresciuta fino a sfumare la dualità tra la dimensione digitale e il mondo reale, rendendo spesso problematica l'identificazione di confini e rispettive caratteristiche" (Strategia, p. 4).

Non vi è praticamente aspetto della vita delle persone, delle imprese e degli Stati che non sia influenzato, toccato o trasformato dalle tecnologie digitali. Si parla al riguardo di Transizione (o Trasformazione) Digitale, ma anche di **Sovranità Digitale**, con riferimento alla capacità di uno Stato di agire in maniera indipendente all'interno del mondo digitale. Secondo il *Position Paper*: "La sovranità digitale è una particolare forma di gestione dello spazio cibernetico che prevede il controllo delle reti e dei dati trasmessi attraverso di esse. Le infrastrutture di rete fissa a banda ultra-larga e di rete mobile 5G saranno le strutture

portanti dello spazio digitale, e dunque delle tecnologie legate al *cloud*, in ogni settore, tra cui quelli strategici quali i trasporti, l'energia, la sanità, la finanza, le telecomunicazioni, la difesa, il settore spaziale e quello della sicurezza. (…) Miliardi di transazioni digitali al giorno includono dati personali, aziendali, di pagamento che passano sul *web* e su *cloud*. In questo ambito assumono particolare rilevanza i *Digital Trust services*, servizi digitali che hanno l'obiettivo di conferire validità legale alle transazioni digitali. (…) D'altra parte, il possesso/controllo dei dati risulta essere un elemento chiave per il benessere e la tutela degli interessi economici e dei valori fondanti della società europea. La raccolta e l'elaborazione di grandi moli di dati rappresentano fattori fondamentali nello sviluppo dei sistemi economici nell'era digitale. Per questo, fenomeni di concentrazione nel possesso dei dati possono condizionare in modo decisivo il potere "tecnologico-digitale" dei diversi Paesi. Il Paese di appartenenza delle imprese che raccolgono le più grandi quantità di dati è un Paese che, oltre a essere forte dal punto di vista tecnologico digitale, è anche un Paese che ha la piena sovranità del proprio patrimonio digitale. Sono infatti le grandi moli di dati di cui si è in possesso che permettono di conoscere le preferenze dei consumatori e di sfruttarle; sono i *big data* che alimentano e consentono l'applicazione di tecnologie come, ad esempio, l'intelligenza artificiale" (CED 2021, pp. 18-19).

Anche secondo la Strategia Nazionale di Cybersicurezza: "I produttori e fornitori di beni e servizi delle ICT (*Information and Communications Technologies*) svolgono un ruolo di primo piano. A loro è richiesto di fornire prodotti e soluzioni tecnologiche che soddisfino adeguati requisiti di cybersicurezza. L'obiettivo è rafforzare la resilienza di dispositivi e apparati ICT, a partire dal 5G e dal *cloud*, anche al fine di aumentare la fiducia dei cittadini" (M. Draghi, Strategia, p. 3)[1].

La stessa Strategia individua espressamente e specificamente l'**Autonomia Strategica nel settore digitale** come una delle cinque sfide da affrontare nel periodo 2022-2026 (insieme a: Transizione digitale *cyber* resiliente della PA e del tessuto produttivo; Anticipazione dell'evoluzione della minaccia *cyber*; Gestione di crisi cibernetiche; e Contrasto alla disinformazione *on-line* nel più ampio contesto della c.d. minaccia ibrida).

"A livello UE, l'eccessiva frammentazione e competizione tra gli Stati Membri ha costituito, fino ad oggi, un grosso ostacolo allo sviluppo di tecnologia "*made in EU*" e alla

[1] Si veda anche il decreto-legge 21 marzo 2022, n. 21, che ha recato, tra le varie, disposizioni sulla ridefinizione dei poteri speciali in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, nonché di ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, ivi inclusi quelli relativi alla tecnologia *cloud*. In particolare, ha ridefinito gli obblighi e le procedure di notifica da parte delle imprese interessate, nonché le procedure di esercizio dei poteri speciali, di monitoraggio e sanzionatori da parte del Governo, prevedendo la partecipazione dell'Agenzia per la Cybersicurezza Nazionale, la possibilità di avvalersi anche del Centro di Valutazione e Certificazione Nazionale (CVCN) e la possibilità di condurre attività ispettive e di verifica.

creazione di grandi aziende di erogazione di servizi digitali. L'UE e, in particolare, l'Italia, si trova in una posizione di dipendenza tecnologica da altri Paesi, *leader* nella produzione di *software* e delle cosiddette Emerging and Disruptive Technologies quali, ad esempio, l'AI e il *quantum computing*. Ciò ha inevitabili ricadute anche sulla possibilità di detenere un controllo diretto sui dati conservati, elaborati e trasmessi attraverso tali tecnologie. Infatti, più si è autonomi dal punto di vista tecnologico e più si possono attuare politiche di sovranità delle informazioni" (Strategia, p. 11).

Per affrontare al meglio le sfide del Paese, la Strategia individua tre obiettivi fondamentali: *Protezione*, *Risposta* e *Sviluppo*. Quest'ultimo è definito come lo "sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato. La costellazione di centri di eccellenza e imprese che compongono, assieme all'accademia, il tessuto della ricerca e dello sviluppo è infatti un patrimonio essenziale per il nostro Paese con importanti potenzialità di espansione. Numerosi sono gli strumenti e le iniziative avviate negli ultimi anni per supportare lo sviluppo delle capacità del sistema nazionale di ricerca, la trasformazione digitale e l'innovazione tecnologica, tra cui si annoverano, in particolare, quelli previsti dal PNRR, dalle ultime leggi di bilancio, e dal Piano Nazionale Impresa 4.0." (Strategia, p. 22).

Così definito l'Obiettivo Sviluppo[2], è evidente che esso va ben oltre il dominio della cybersicurezza, per investire l'intero tema della Sovranità Digitale e della Autonomia Strategica che ne consegue.

L'area della Sovranità Tecnologica è dunque quantomai trasversale. Al pari di altre questioni politiche trasversali come la parità di genere, la transizione verde o lo sviluppo sostenibile, le politiche di trasformazione digitale sono rilevanti in molti ambiti. È, tuttavia, possibile – e necessario ai fini della definizione delle relative politiche – riferirsi ad alcuni settori strategici, quali i trasporti, l'energia, la sanità, la finanza, le telecomunicazioni, la difesa, il settore spaziale e quello della sicurezza. Fra questi, il comparto Aerospazio, Difesa e Sicurezza (AD&S) riveste una importanza particolare.

A livello europeo, l'industria della difesa svolge un ruolo considerevole nel garantire la sicurezza e la difesa dell'Europa. Con un fatturato di 108 miliardi di euro nel 2018, è anche un importante fornitore di crescita e posti di lavoro. La possibilità del c.d. *dual use* rende il comparto ulteriormente rilevante. Difesa e sicurezza sono infine da intendersi in maniera ampia, in correlazione con le esigenze di difesa e di sicurezza a tutti i livelli dei cittadini. E l'industria italiana dell'AD&S è un settore assolutamente strategico per il nostro Paese

[2] Su cui si veda *amplius*, *infra*, Capitolo IV, paragrafo 6.

perché, da un lato, fornisce all'Italia strumenti e capacità fondamentali per la difesa dell'interesse nazionale e per la sicurezza dei cittadini; dall'altro, rappresenta un preziosissimo strumento di influenza geopolitica, in grado accrescere il peso del nostro Paese nel mondo. Il settore AD&S vale 13,5 miliardi di euro (0,65 del Prodotto Interno Lordo (PIL)), pari a circa il 15% del valore dell'intero settore in Europa. Il 70% di tale valore è destinato all'*export*, in virtù del quale tale industria rappresenta una eccellenza del *made in Italy*. Altro dato di eccellenza del comparto Aerospazio e Difesa riguarda gli investimenti in ricerca e sviluppo, al secondo posto in Italia in valore assoluto (1,4 miliardi di euro) e al primo posto (insieme al settore della componentistica elettronica) in percentuale di fatturato (10%).

Non sono tuttavia solo i settori delle telecomunicazioni, della difesa o della componentistica elettronica ad essere interessati direttamente dalla transizione tecnologica in atto.

Le nuove tecnologie sono rilevanti per tutti i settori industriali e non, incluso quello agroalimentare e, in generale, i settori del c.d. Bello e Ben Fatto (BBF). Il BBF racchiude in sé tutti i beni che rappresentano l'eccellenza italiana in termini di *design*, cura, qualità dei materiali e delle lavorazioni. Si tratta di prodotti che si distribuiscono in tutti i comparti produttivi, ma che trovano la loro massima espressione nelle produzioni più legate al gusto e alla creatività: le c.d. "tre F" di *fashion*, *food and furniture*. Da questo punto di vista, il BBF è l'espressione più facilmente riconoscibile del *made in Italy*. L'Italia ha, ad esempio, una produzione consolidata di prodotti agroalimentari di eccellenza con 873 produzioni certificate (in particolare vino) nel 2020, con un valore pari a circa 550 miliardi di euro in tutte le sue componenti, pari ad oltre il 15% del PIL italiano.

Per questi settori, la Transizione Digitale presenta delle opportunità ma anche dei notevoli rischi, soprattutto rispetto alla contraffazione *on-line*.

Uno studio OCSE del 2018 ha stimato in 32 miliardi il valore dei prodotti italiani contraffatti scambiati a livello mondiale, il 16,7% del quale sono prodotti di abbigliamento, 15,4% prodotti legati all'ottica e all'elettronica e il 13,0% legati al comparto alimentare. I prodotti italiani, infatti, risultano essere tra i più richiesti al mondo, anche grazie al potere di attrazione esercitato dal marchio *made in Italy* e, perciò, risultano essere tra i più imitati. Le dimensioni della contraffazione hanno raggiunto livelli ancora più ragguardevoli negli ultimi anni, in particolare nei settori del BBF italiano – tra quali si annidano imitazioni, ossia prodotti contraffatti che tentano di sfruttare in modo fraudolento il *brand* e la fiducia acquisita da alcuni marchi presso i consumatori. Particolarmente preoccupante risulta essere il fenomeno del c.d. *Italian sounding*, cioè l'imitazione di un prodotto – specialmente nel

settore agroalimentare – ottenuta attraverso un rimando, nel nome o nel *packaging*, a una sua supposta italianità. Tale pratica, che svilisce l'immagine della qualità dei prodotti e inganna i consumatori meno attenti portandoli a credere di acquistare un prodotto italiano originale, comporta una perdita di quote per il BBF (e anche un deterioramento della sua immagine).

La contraffazione del BBF, oltre a causare un danno materiale alle imprese italiane, rende anche più difficile la misurazione del fenomeno, rendendo meno affidabili alcune delle statistiche che se ne traggono; verosimilmente le quote italiane ne risultano distorte al ribasso.

Secondo il *report* annuale 2020 sull'azione dell'Autorità antifrode nazionale (ICQRF) – un dipartimento del Ministero delle Politiche Agricole, Alimentare e Forestale – i controlli antifrode sono stati oltre 70.000 e le irregolarità hanno riguardato circa l'11% dei prodotti, con oltre 4.000 contestazioni amministrative e 22 milioni di kg di merce sequestrata per un valore di oltre 21 milioni di euro. Esistono anche specifiche azioni di tutela come: a) il Piano Coordinato di Controllo UE per contrastare pratiche illegali sulle vendite e pubblicità *on-line*, b) i Controlli pratiche sleali che hanno riguardato segnalazioni relative alle modifiche contrattuali sia per quanto riguarda prezzi sia quantitativi pattuiti, c) il Programma di controllo bevande spiritose e alcool mirato a contrastare fenomeni fraudolenti e pericolosi sia dal punto di vista commerciale sia per la salute pubblica.

La frammentazione e mancanza di regolamentazione porta al proliferare di iniziative private relative alla protezione del *made in Italy* – come *authentico*[3]*,* una *start-up*, *leader* in Italia nel settore dell'anticontraffazione alimentare, che ha sviluppato, d'intesa con le PA nel settore agroalimentare e vitivinicolo, una applicazione per riconoscere i prodotti agroalimentari contraffatti. Frutto di iniziativa privata è anche il San Marzano Dop di Solania,[4] il primo pomodoro certificato in *Blockchain*, una certificazione di qualità e di trasparenza ottenuta in collaborazione con l'Azienda Solania, *leader* nella produzione e trasformazione del San Marzano DOP.

La tutela dei prodotti agroalimentari su *web* passa anche per azioni di collaborazione con le piattaforme Ebay, Alibaba, Amazon e Rakuten – per bloccare vendite, annunci ingannevoli e/o evocativi dei prodotti di eccellenza.

Sono tutti fenomeni che contribuiscono a definire gli ambiti – talora angusti – della Sovranità Tecnologica italiana.

---

[3] Prodotti Made in Italy: più tutela sul web - Authentico (authentico-ita.org)

[4] Spaghettitaliani: "Solania presenta il primo pomodoro San Marzano Dop certificato in Blockchain" - Authentico (authentico-ita.org)

4. Sovranità Tecnologica: Transizione Digitale e soggetti coinvolti

Da quanto illustrato risulta evidente che soggetti portatori di interessi sono innanzitutto gli attori istituzionali. Al riguardo, la difficoltà principale consiste nell'individuazione di centri unitari di conoscenza, di indirizzo e di azione.

Le competenze sono state almeno fino alla recente riforma realizzata con l'istituzione dell'ACN nel 2021, estremamente frammentate. Ciò costituisce, almeno in parte, la conseguenza della trasversalità delle trasformazioni tecnologiche e digitali, che però – al tempo stesso – rende imprescindibile un approccio olistico e coordinato, in primo luogo dal punto di vista istituzionale.

La nuova architettura fa perno sull'ACN quale ente di raccordo fra l'autorità di indirizzo politico, individuata nella Presidenza del Consiglio dei Ministri, e gli altri attori (pubblici e privati) coinvolti (*infra*, Capitolo IV).

Sempre dal punto di vista istituzionale, un ruolo particolare è chiamata a svolgere la diplomazia italiana, se adeguatamente inserita nei suddetti circuiti di informazione, indirizzo e azione – con riferimento ai numerosi consessi internazionali ed europei in cui si discute in maniera più o meno frammentata di *digital governance* e di cui si dirà nel prossimo capitolo (Capitolo II).

Per quanto riguarda gli operatori privati, le PMI sono la vera e propria struttura portante del sistema produttivo italiano. Secondo i dati aggiornati al 2021, in Italia le PMI rappresentano il 99,9% del totale delle imprese operanti sull'intero territorio nazionale, generando il 70% del fatturato del nostro Paese e contribuendo ad impiegare oltre l'81% dei lavoratori.

Nel settore della difesa, in particolare, una parte sostanziale della base industriale e tecnologica della difesa europea – e quindi anche italiana – è costituita da PMI: le circa 2.500 PMI che operano a livello europeo sono una parte di importanza critica delle catene di approvvigionamento. Le PMI attive nell'industria della difesa sono fattori chiave per l'innovazione e la crescita, in grado di condurre attività essenziali di ricerca, tecnologia e innovazione.

Anche nel settore delle telecomunicazioni, tradizionalmente appannaggio in Italia del settore pubblico, negli ultimi anni si sono registrati forti investimenti in nuove infrastrutture (reti 5G e a banda ultra-larga fissa) oltre che da parte dell'operatore pubblico ancora oggi dominante (TIM), di numerosi operatori privati. L'Italia si trova invece ancora in posizione di dipendenza da altri Paesi e di svantaggio competitivo rispetto alle grandi aziende di erogazione di servizi digitali, in particolare per quanto riguarda la produzione di *software* e

delle c.d. *Emerging and Disruptive Technologies* quali, ad esempio, l'AI e il *quantum computing*.

Inoltre, indipendentemente dal loro settore specifico di operatività, la transizione tecnologica impatta tutte le imprese almeno sotto due rilevanti e imprescindibili profili: quello del rapporto con i propri dipendenti (in particolare, con riferimento alla possibilità del lavoro agile) e quello del rapporto con la propria clientela (a fini di transazione, fatturazione, *marketing* etc.).

Anche gli operatori nel mondo accademico e della ricerca, sia pubblici che privati, sono ovviamente attori chiave nella Transizione Tecnologica, in particolare Digitale, non solo nella fruizione dei relativi servizi, ma al fine di generare e integrare conoscenze, riutilizzare conoscenze sviluppate altrove, e realizzare solide e affidabili *partnership* internazionali. Come si vedrà (Capitolo III), rispetto al settore della ricerca e dell'innovazione, il PNRR ha destinato cospicue risorse nell'ambito della Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo". Di qui, l'esigenza di garantire informazione e supporto, ma anche il coordinamento e il raccordo fra pubblico e privato e fra accademia e impresa.

La società civile tutta, infine, è *player* cruciale della Transizione Tecnologica sia in quanto beneficiaria dei relativi servizi, che come cittadinanza attiva. Dal primo punto di vista, l'Italia ha ancora passi importanti da compiere per garantire l'accesso universale alle nuove forme di TLC, che richiederebbe innanzitutto il riconoscimento della connettività digitale come servizio essenziale. Inoltre, per essere effettivo, l'accesso alle tecnologie deve accompagnarsi alla messa disposizione degli strumenti e delle conoscenze che ne consentano l'utilizzazione. In relazione a quest'ultimo aspetto, la società civile (in particolare, nelle sue articolazioni come *no profit*) se opportunamente coinvolta, può svolgere una funzione essenziale. Con riguardo al ruolo della società civile come cittadinanza attiva, le spinte di attivisti, esperti e terzo settore possono essere determinanti in tutti i campi: dai piani di azione per la trasparenza, partecipazione e anticorruzione nella PA, alla *cybersecurity*, alla lotta contro la contraffazione (*on-line* e *offline*) dei prodotti *made in Italy* (di cui si è detto nel paragrafo precedente).

5. Accelerazione della Transizione Tecnologica e dell'esigenza di Autonomia Strategica che ne consegue: Pandemia da COVID-19 e Conflitto russo-ucraino

Come è stato da più parti rilevato, la pandemia da COVID-19 e la grave crisi sanitaria, economica e sociale che ne è conseguita, hanno funto da acceleratori, talora perfino da catalizzatori, di processi già in corso. Uno di questi riguarda, ad esempio, le tensioni fra Stati Uniti e Cina nelle relazioni commerciali ma anche nella competizione tecnologica e

industriale. Non vi è processo, tuttavia, che abbia subito accelerazione maggiore della Transizione Tecnologica, in particolare Digitale, delle trasformazioni economiche e sociali che la stessa ha messo in atto.

Il distanziamento sociale che ha accompagnato la pandemia ha accelerato il processo di digitalizzazione, spingendo cittadini e aziende a utilizzare sempre più processi digitali per svolgere diverse attività e interagire con la PA. Ha fatto impennare il numero delle transazioni digitali, soprattutto commerciali, contribuendo alla crescita esponenziale dei grandi giganti dell'*e-commerce*. Ma nel corso della pandemia, è aumentato anche l'uso dei *social networks*, e con esso delle grandi piattaforme – con un enorme impatto sulla quantità e qualità dei dati raccolti.

L'accelerazione della transizione digitale ha riguardato tutti i settori – ivi compresi, quelli pubblici essenziali e i settori educativi – e tutti gli attori[5]. Nella maggior parte dei casi, con effetti positivi.

Il grado di digitalizzazione delle imprese in Italia (misurato sull'uso delle piattaforme digitali), che prima della pandemia ci vedeva in grave ritardo rispetto alla media europea, ad esempio, è passato in un solo anno a valori vicini (14% per le PMI) o addirittura al di sopra (24% per le grandi aziende) della media europea (15%) – segno della capacità di resilienza che dal secondo dopoguerra caratterizza la storia del nostro Paese nei momenti più difficili.

Si tratta di effetti per la maggior parte destinati a stabilizzarsi o diventare permanenti con la fine della pandemia, qualora dovesse avverarsi.

Considerazioni analoghe possono essere estese al conflitto russo-ucraino – ancora in corso al momento in cui si scrive – e i cui effetti sul piano geoeconomico e geopolitico sono ancora più dirompenti e apparentemente di carattere più profondo e duraturo.

Il perdurare della guerra dopo oltre sei mesi, l'incertezza che accompagna ogni ipotesi di soluzione, e l'aggravarsi quotidiano della crisi umanitaria, economica, energetica e alimentare, da un lato, presentano rischi per la capacità di affrontare la Trasformazione Digitale; dall'altro, pongono i settori della difesa e della sicurezza – non solo l'aumento delle spese militari – al centro dell'agenda politica nazionale, internazionale e dell'UE.

---

[5] Queste – schematicamente - tutte tendenze accelerate dalla pandemia, il cambiamento tecnologico e l'ulteriore spinta alla digitalizzazione che ne è conseguita: vendite *on-line* (e la creazione di colossi delle vendite *on-line*); piattaforme digitali per la raccolta di dati, stoccaggio sempre più massivo di informazioni; la riduzione degli spostamenti fisici delle persone; l'affiancamento dei *social media* ai *mass media*, e i nuovi canali di diffusione pubblicitaria e i giganti del *web*, che operano su scala globale con posizioni di rendita oligopolistiche difficilmente scalfibili, almeno nell'immediato, da altri operatori economici.

Ma, più della pandemia, la guerra in Ucraina ha reso centrale a livello globale e intensificato il dibattito sul *decoupling* – precedentemente rilevante soprattutto nell'ambito delle relazioni commerciali fra Stati Uniti e Cina.

Ridurre le dipendenze nei settori strategici è diventata una preoccupazione centrale per i governi delle principali economie non solo in Nord America ma anche in Asia ed Europa[6].

Il consenso politico sembra essersi consolidato ormai anche nell'UE sull'esigenza di ridurre le dipendenze delle economie europee, in particolare, dalla Cina e soprattutto nei settori tecnologicamente rilevanti[7], oltre che dalla Russia, in campo energetico.

[6] Fasulo F. (2022). The EU, US and Asia. Economy as a Weapon?, ISPI Policy Paper, 1-46. testo disponibile sul sito: https://www.ispionline.it/it/pubblicazione/eu-us-and-asia-economy-weapon-35893. Data di consultazione 07/09/2022.

[7] *Infra*, Capitolo II, paragrafo 7.

Capitolo II. Impegni assunti (o da assumere) sul piano internazionale

1. Premessa

Il quadro fin qui delineato non sarebbe completo senza prendere in considerazione le organizzazioni e i *fora* **internazionali** di cui l'Italia fa parte, la cui attività è rilevante per la Sovranità Tecnologica nazionale e/o la *governance* internazionale della transizione tecnologica, in particolare, digitale – c.d *digital governance.*

Un quadro di insieme degli impegni assunti (o da assumere) dall'Italia nell'ambito delle organizzazioni e *fora* internazionali in cui si discute in maniera più o meno frammentata di *digital governance*, è del resto essenziale affinché la diplomazia italiana possa essere adeguatamente inserita nei circuiti di informazione, indirizzo e azione che riguardano la Sovranità Tecnologica, e quindi la partecipazione italiana possa svolgersi in conformità alle esigenze di Autonomia Strategica nazionale.

2. L'Italia fra Trasformazione Digitale come *Self-Driving car* e esigenze di Governance

Come è stato efficacemente osservato, la trasformazione digitale assomiglia a un'auto a guida autonoma senza garanzie di sicurezza – "*a self-driving car without security guarantees*"[8] – a causa del ritardo della regolamentazione.

La regolamentazione è oggetto di scontro e competizione, anziché di cooperazione.

Gli Stati Uniti e la Cina si scontrano tra loro sul terreno della competizione digitale, privando o rendendo difficoltoso l'accesso delle rispettive aziende tecnologiche più importanti ai propri mercati. E, invece che al rafforzamento della cooperazione internazionale, assistiamo alla regionalizzazione dell'architettura della *governance* digitale.

A livello europeo, ad esempio, l'UE ha annunciato una propria strategia di dati nel 2020, tradottasi nell'adozione di un pacchetto di misure volte ad aggiornare, omogeneizzare e, in alcuni casi, introdurre la regolamentazione dei mercati e dei servizi digitali nell'Unione europea – che dovrebbero assicurare l'equità del mercato digitale, l'equilibrio nella competizione digitale nonché la sicurezza, affidabilità e trasparenza dell'AI (il *Digital Market Act* (DMA), il *Digital Service Act* (DSA) e l'*AI Act* (AIA) – di cui si dirà anche *infra*, paragrafo 6, *in fine*). Ciò rende poi difficile la cooperazione nella sicurezza informatica, che richiede la condivisione di informazioni. I rischi per la sicurezza informatica si combattono su un terreno

[8] L'espressione è di P. Magri, alla Conferenza internazionale dell'ISPI *Forum on Digital Transformation. Steering transition through turbulence*, 16 maggio 2022. Registrazione disponibile al sito https://www.ispionline.it/it/eventi/evento/forum-digital-transformation-steering-transition-through-turbulence.

comune globale per la *cybersecurity*, attraverso la cooperazione digitale globale e la gestione comune dei rischi, superando la frammentazione.

Sarebbe necessaria una nuova Bretton Woods sulla Sovranità Tecnologica per accompagnare la Trasformazione Digitale, che costituisce, dal punto di vista dei rischi, una delle tendenze più preoccupanti della nostra epoca ed è in continua evoluzione.

Affinché le nuove tecnologie si trasformino da un lusso per pochi in una opportunità per tutti, occorre il riconoscimento universale dell'accesso ad *internet* e la connettività digitale come servizio pubblico essenziale a livello globale.

Le istituzioni di Bretton Woods, create dopo la Seconda Guerra Mondiale per finanziare la ricostruzione, sostenere lo sviluppo economico e mantenere la stabilità finanziaria – tra cui il Fondo Monetario Internazionale e la Banca Mondiale – sono diventate obsolete. Queste istituzioni non sono in grado di affrontare le minacce alla stabilità e alla sicurezza politica ed economica che sono emerse come risultato del dominio incontrollato delle piattaforme *internet* commerciali. Non sono in grado di farlo tempestivamente.

Ma è proprio in assenza di un quadro globale condiviso, che anche un Paese a media potenza come l'Italia può contare molto nell'ambito delle organizzazioni e *fora* internazionali di cui fa parte, oltre che naturalmente in seno all'UE.

La diplomazia italiana, la cui storia è ricca di successi e riconoscimenti, può svolgere un ruolo propulsivo soprattutto nella direzione della promozione dei valori democratici e di rispetto dei diritti fondamentali, anche al fine del rafforzamento della propria Sovranità Tecnologica e, quindi, Autonomia Strategica.

3. UN Global Digital Compact e SDGs

Vi è innanzitutto la possibilità di contribuire al c.d. *Global Digital Compact*[9]*,* una iniziativa del Segretario generale delle Nazioni Unite che costituisce il punto di approdo di un processo avviato a luglio 2018 – con la convocazione di un Gruppo di alto livello sulla cooperazione digitale per avanzare proposte volte a rafforzare la cooperazione nello spazio digitale tra governi, settore privato, società civile, organizzazioni internazionali, università, comunità tecnica e altre parti interessate.

Il 10 giugno 2019, il gruppo di esperti ha presentato al Segretario generale il rapporto *The Age of Digital Interdependence*, contenente raccomandazioni per migliorare la cooperazione digitale. L'11 giugno 2020, il Segretario generale ha adottato la *Roadmap for Digital Cooperation*: una serie di azioni raccomandate alla comunità internazionale per

[9] Global Digital Compact, https://www.un.org/techenvoy/global-digital-compact.

contribuire a garantire che tutte le persone siano connesse, rispettate e protette nell'era digitale.

La *Roadmap* fornisce una visione e una guida per un mondo digitalmente interdipendente e definisce le azioni che la comunità internazionale dovrebbe intraprendere con il fine di: "*Connect, Respect and Protect*" le persone nell'era digitale. La *Roadmap* è un invito a connettere tutte le persone entro il 2030, a rispettare i diritti umani *on-line* e a proteggere i più vulnerabili dai potenziali rischi del progresso digitale.

A settembre 2020, i *leader* del mondo, in occasione del 75° anniversario delle Nazioni Unite, hanno adottato una dichiarazione politica che riconosce l'importanza della tecnologia come questione globale fondamentale e l'impegno a "migliorare la cooperazione digitale" per essere in grado di massimizzare i benefici delle tecnologie digitali, riducendone al contempo i rischi.

A settembre 2021, il Segretario Generale ha adottato il rapporto *Our Common Agenda*, con cui ha proposto un Patto digitale globale – il *Global Digital Compact*, appunto – da concordare al *Summit of the Future* nel settembre 2023, attraverso un percorso tecnologico che coinvolga tutte le parti interessate: i governi, il sistema delle Nazioni Unite, il settore privato (comprese le aziende tecnologiche), la società civile, le organizzazioni di base, il mondo accademico e gli individui, compresi i giovani. Sia l'attuazione della *Roadmap* sulla cooperazione digitale che il lavoro per il *Global Digital Compact* sono coordinati dall'Ufficio dell'Inviato del Segretario generale per la Tecnologia[10].

4. Internet Governance Forum

Un altro luogo di incontro multilaterale e '*multi-stakeholder*', aperto a tutti, nel quale si discutono i principali temi relativi alla *governance* di *Internet*, ossia le regole, le procedure, le infrastrutture e i programmi che ne determinano il funzionamento e l'evoluzione, è l'*Internet Governance Forum* (IGF)[11] – nel quale i governi, gli organismi privati e la società civile contribuiscono a delineare aspetti non solamente tecnici, ma anche economici e sociali – anche in relazione a temi di ampia portata come democrazia, partecipazione e trasparenza.

L'obiettivo del *Forum*, promosso dalle Nazioni Unite a partire dal 2006, consiste nell'attuare il mandato del Vertice mondiale sulla società dell'informazione (WSIS) che

[10] Office of the Secretary-General's Envoy on Technology, https://www.un.org/techenvoy/.
[11] Internet Governance Forum, https://www.intgovforum.org/en.

prevedeva la convocazione di un *forum* per un dialogo politico democratico, trasparente e multilaterale.

Dopo le consultazioni aperte di febbraio e luglio 2022, il IGF terrà il suo 17° *Annual Meeting* ad Addis Abeba in Etiopia, dal 28 novembre al 2 dicembre 2022, su *Resilient Internet for a Shared Sustainable and Common Future*.

Pur non funzionando come organismo decisionale, l'IGF, mediante le sue declinazioni nazionali, rappresenta un riferimento per lo sviluppo delle politiche relative a *Internet*, anche per l'Italia.

5. OSCE

Il nostro Paese partecipa alle principali iniziative di cooperazione, di *cyber diplomacy* e di *capacity building* nei confronti di Paesi *partner* che stanno sperimentando un rapido sviluppo digitale, anche nell'ambito dell'Organizzazione per la pace e la sicurezza in Europa (OSCE)[12].

Tale cooperazione si realizza, in particolare, attraverso l'implementazione delle c.d. *Confidence-Building Measures* (CBM), adottate in sede OSCE, al fine di evitare l'emergere di tensioni a livello politico-militare derivanti dall'impiego delle tecnologie dell'informazione e della comunicazione (*Information and Communications Technologies* (ICT)).

L'idea alla base delle CBM, che ricalcano pratiche simili dell'epoca della Guerra Fredda, è quella di disporre di un sistema di comunicazione diretta tra gli Stati membri per disinnescare i conflitti e prevenire un'*escalation* involontaria.

L'OCSE ha formulato ad oggi 16 CBM. All'insieme iniziale di 11 CBM adottate nel 2013[13], si sono aggiunte, nel 2016, cinque nuove CBM per ridurre i rischi di conflitto derivanti dall'uso delle ICT, che prevedono, fra l'altro, di: promuovere partenariati pubblico-privato (CBM 14); "adottare accordi nazionali volontari per classificare gli incidenti da ICT in termini di portata e gravità dell'incidente", "[migliorare] la sicurezza delle infrastrutture critiche nazionali e transnazionali basate sulle ICT (...)", "[a]umentare la consapevolezza dell'importanza di proteggere i sistemi di controllo industriale (...)" e condividere informazioni riguardo alle infrastrutture critiche basate sulle ICT (CBM 15).

---

[12] OSCE, https://www.osce.org/.

[13] Su cui si veda, *OSCE Guide on Non-military Confidence-Building Measures*, 30 aprile 2013. Testo disponibile al sito https://www.osce.org/secretariat/91082.

6. OECD

L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD)[14], che riunisce 38 Paesi aventi in comune una economia di mercato a fini di consultazione e studio, *best-practice sharing* e *international standard-setting* sulle principali sfide globali, ha elaborato una serie di indicatori e raccomandazioni per aiutare i Paesi a confrontare il loro sviluppo digitale e realizzare le promesse della Trasformazione Digitale per tutti[15].

Fra questi, di particolare importanza è il *National Digital Strategy Comprehensiveness* (NDSC) consultabile in maniera interattiva sul sito dell'OECD *Going Digital Toolkit*[16]*,* che misura lo stato di sviluppo digitale dei Paesi membri sulla base di sette dimensioni: *Accesso* alle infrastrutture, ai servizi e ai dati di comunicazione; *Uso* effettivo delle tecnologie digitali e dei dati da parte di persone, imprese e governo; *Innovazione*; evoluzione del mercato del *Lavoro*; *Società*; *Fiducia* negli ambienti digitali; e *Apertura dei mercati*[17]*.* L'Italia è l'unico Paese ad assestarsi sui valori più bassi per quasi tutte le dimensioni prese in considerazione[18]. Risulta, peraltro, che la sola fonte presa in considerazione per valutare la *National Digital Strategy* italiana siano gli obiettivi e le iniziative per il digitale ricomprese nel PNRR[19], senza riferimento ad altri programmi o riforme[20]. Di qui, forse, l'esigenza di una migliore rappresentazione del nostro Paese nell'ambito dell'OECD (e anche una conferma dell'utilità di questa ricerca e di studi simili ad essa).

L'NDSC dovrebbe aiutare i singoli Paesi a formulare, e ove necessario correggere, e integrare le relative politiche. Significativo al riguardo è che di tale strumento poco o nulla si sia sentito parlare in Italia[21] – anche questo forse conseguenza di una non completa informazione/comunicazione fra OECD e il nostro Sistema Paese.

---

14 OECD, https://www.oecd.org/.

15 Una visione di insieme di tali indicatori, raccomandazioni e pubblicazioni correlate è disponibile al sito https://www.oecd.org/digital/.

16 OECD *Going Digital Toolkit*, https://goingdigital.oecd.org/, su cui si veda anche Gierten D., Lesher M. (2022), Assessing national digital strategies and their governance, *OECD Digital Economy Papers*, 324: 1-29. Testo disponibile al sito: https://doi.org/10.1787/baffceca-en.

17 Date queste sette dimensioni (*Access*, *Use*, *Innovation*, *Jobs*, *Society*, Trust e *Market Openness*), ognuna delle quali presenta specifici domini di *policy* per un totale complessivo di 38 *domain policies*, alla *National Digital Strategy* di ciascun Paese viene assegnato un punto per ogni dominio di *policy* che questa interessa tra il *pool* complessivo dei 38 individuati. Questi punteggi vengono suddivisi per le sette dimensioni in base al numero di *policy domains* presenti nella *National Digital Strategy* presa in considerazione per ogni categoria; ogni valore risultante per ogni dimensione viene poi diviso per il numero totale di *policy domains* contenuti in ciascuna dimensione.

18 Secondo l'OECD, dunque, la *National Digital Strategy* italiana non coprirebbe gran parte dei domini di *policy* individuati per ciascuna dimensione.

19 Italia digitale 2026, https://innovazione.gov.it/dipartimento/focus/italiadigitale-2026/ e *National Plan of Recovery and Resilience*, https://italiadomani.gov.it/en/home.htm.

20 Su cui si veda, *infra*, rispettivamente, i Capitoli III e IV.

21 Nessun rapporto o indicatore OECD è, ad esempio, menzionato nella Strategia Nazionale di Cybersicurezza 2002-2026.

7. OMC. Lo sfasamento fra Trasformazione Digitale e disciplina del commercio internazionale

Come si è accennato[22], il commercio è sempre più definito da flussi di dati e informazioni ("*increasingly defined by flows of data and information*", McKinsey Global Institute 2016). Inoltre, mentre fino a non molti anni fa, la vendita *retail on-line* avveniva principalmente su territorio nazionale, con acquirenti e venditori che provenivano dal medesimo Paese, dal 2014 abbiamo assistito a un cambio di rotta: i consumatori sono sempre più attratti da marchi e prodotti internazionali.

Nel 2016, circa il 12 % di tutti i beni scambiati a livello internazionale erano acquistati *on-line* e circa la metà del commercio globale era in servizi digitali. Il COVID-19 ha fatto aumentare esponenzialmente queste percentuali[23].

Dal 2014 al 2020 il commercio transnazionale ha risentito di un tasso di crescita annuale del 29,3%. Oggi, circa il 56% delle aziende si avvale di canali digitali per vendere i propri prodotti o servizi ad altre aziende o consumatori stranieri. Il c.d. *Cross-border eCommerce*, ossia il commercio elettronico transfrontaliero riguarda tutti i Paesi, compresa l'Italia.

Secondo il Rapporto 2021 "Esportare la dolce vita", l'incidenza degli acquisti *cross border* è, o in parte è stata, altissima in Russia, il cui valore costituisce il 74% del totale *eCommerce*. Il Rapporto evidenzia un collegamento fra il turismo e gli acquisti *on-line* e *off-line*.

Eppure, la globalizzazione degli ultimi due o tre decenni è stata squilibrata: veloce nella diffusione della finanza, dell'informazione e delle tecnologie di comunicazione; più lenta nella liberalizzazione del commercio di beni e servizi; in ritardo nella circolazione delle persone e nello sviluppo di risposte normative e politiche a livello nazionale e sovranazionale – in particolare, per quanto riguarda la regolamentazione delle piattaforme dei *social media* che sono per la maggior parte non governate a livello nazionale e rispetto alle quali c'è poca o nessuna *governance* internazionale.

Nell'ambito dell'Organizzazione mondiale del commercio (OMC)[24] – l'organizzazione internazionale creata allo scopo di regolamentare e supervisionare gli scambi commerciali fra gli Stati membri che oggi sono 164 e rappresentano il 98% del commercio globale – risale a maggio 1998 la Dichiarazione sul commercio elettronico globale. La Dichiarazione, adottata alla 2ª Conferenza Ministeriale, chiedeva l'istituzione di un Programma di lavoro

---

22 Capitolo I, paragrafo 5.
23 *Supra*, Capitolo I, paragrafo 4.
24 *World Trade Organization* (WTO), https://www.wto.org/.

sul commercio elettronico per esaminare tutte le questioni commerciali relative al commercio elettronico globale. A settembre 1998, il Programma di lavoro è stato adottato dal Consiglio Generale[25], e da allora ha portato a discussioni regolari sul commercio elettronico in vari organi dell'OMC[26].

Esso definisce il commercio elettronico come: "*production, distribution, marketing, sale or delivery of goods and services by electronic means*" e include fra le questioni legate al commercio elettronico da esaminare: la protezione della *privacy* e della morale pubblica; la prevenzione delle frodi; l'accesso e l'uso delle reti e dei servizi pubblici di trasporto di telecomunicazione; regole di origine; la protezione e applicazione dei diritti d'autore e dei marchi commerciali. Il programma esplora anche le opportunità di sviluppo economico offerte dal commercio elettronico ai Paesi in via di sviluppo, in particolare a quelli meno sviluppati e alle loro PMI.

A dicembre 2017, i membri dell'OMC hanno adottato una decisione per rinvigorire il Programma di lavoro e hanno deciso di astenersi dall'imporre dazi doganali sulle trasmissioni elettroniche. Questa decisione, nota come *Moratoria sulle trasmissioni elettroniche*, è stata periodicamente rinnovata – da ultimo, dalla 12ª Conferenza Ministeriale di Ginevra del 12-15 giugno 2022[27].

Problematico rimane, tuttavia, l'approccio dell'OMC, che affrontando le questioni digitali attraverso la lente del commercio elettronico, non rende giustizia alla natura complessa dell'economia digitale.

Inoltre, un gruppo di Stati membri dell'OMC, su iniziativa di Australia, Giappone e Singapore, ha avviato discussioni separate nell'ambito della c.d. *Iniziativa congiunta sul commercio elettronico*[28]*.* Come per tutte le iniziative congiunte, la partecipazione è aperta a tutti i membri dell'OMC: ad oggi, ne fanno parte 86 Paesi (tra cui l'UE), che rappresentano oltre il 90% del commercio globale. Nonostante sia condiviso che il COVID-19 abbia aumentato l'urgenza di sviluppare regole globali sul commercio digitale, tuttavia, i negoziati anche in questo ambito non hanno ancora registrato progressi sostanziali.

---

[25] *Work Programme on Electronic Commerce*, adottato dal Consiglio generale a settembre 1998, https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm.

[26] Su cui si veda *WTO MC12 briefing note*, https://www.wto.org/english/thewto_e/minist_e/mc12_e/briefing_notes_e/bfecom_e.htm.

[27] *WTO MC12, Work Programme on Electronic Commerce Ministerial Decision*, adottata il 17 giugno 2022, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/32.pdf&Open=True.

[28] *WTO Joint Initiative on E-Commerce*, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm.

Mentre, dunque, il commercio globale diviene sempre più digitale, i negoziati per la formulazione di regole globali sul commercio digitale procedono su un doppio binario, nessun dei quali appare allo stato in grado di approdare a risultati concreti.

Un nuovo tipo di accordo commerciale volto a facilitare il commercio e a creare un quadro per l'economia digitale è la *New Digital Economy Partnership Agreement* (DEPA) concluso l'11 giugno 2020 tra Cile, Nuova Zelanda e Singapore[29]. Il DEPA è suddiviso in moduli che trattano argomenti quali la facilitazione degli affari e del commercio, questioni relative ai dati, la fiducia delle imprese e dei consumatori, l'AI, le identità digitali, la cooperazione fra le PMI e l'inclusione digitale. Esso può essere un modello per il modo in cui i membri dell'OMC potrebbero procedere nel concordare regole globali per il commercio digitale, secondo un approccio modulare.

Nel quadro attuale generale, tuttavia, le uniche prospettive per la realizzazione di una disciplina del commercio internazionale digitale sono offerte dalla conclusione di accordi bilaterali o regionali più tradizionali, che possono anche fungere da laboratorio per nuove regole commerciali multilaterali, ma che rappresentano anche una area in cui due diversi modelli di liberalizzazione – statunitense ed europeo – coesistono e competono. E gli stessi Paesi che hanno concluso un accordo di libero scambio con gli Stati Uniti, possono avere una *partnership* commerciale con l'UE, che adotta un linguaggio diverso (e potenzialmente contraddittorio) rispetto al modello statunitense, creando un problema di ulteriore frammentazione.

Si tratta, del resto, della medesima frammentazione che si ritrova anche in altri campi interessati dalla Trasformazione Digitale: la regolamentazione della *privacy*, anzitutto, che vede il mondo diviso in tre blocchi (quello statunitense, quello cinese e quello dell'UE – con l'adozione da parte di quest'ultima del Regolamento generale sulla protezione dei dati); ma anche le politiche di tutela della concorrenza, rispetto alle quali l'UE ha adottato il pacchetto di misure composto dal DSA, il DMA e l'AIA, di cui si è detto *supra*, paragrafo 1).

Di qui, la difficoltà che incontrano le autorità pubbliche nel regolare la condotta dei colossi del *web*. In gioco, al di là degli aspetti economici e dei problemi di concorrenza/*antitrust*, ci sono gli equilibri politici e sociali delle moderne società e l'Autonomia Strategica degli Stati nazione.

---

[29] Il testo dell'accordo (insieme ad una illustrazione completa dei suoi contenuti) è consultabile al sito: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/.

8. UE: la Strategia industriale europea, la Strategia per la cybersicurezza, e la Bussola strategica per la sicurezza e la difesa.

Il 10 marzo 2020, la Commissione europea ha definito la *Strategia di politica industriale* europea: un quadro completo per raggiungere l'Autonomia Strategica dell'UE e sostenere la sua duplice transizione verso una economia verde e digitale. Per la Trasformazione Digitale dell'Europa, la Strategia propone, per il decennio digitale dell'UE, una bussola digitale – *the 2030 Digital Compass Initiative* – che si sviluppa intorno a quattro punti cardinali: Competenze; Infrastrutture digitali sicure e sostenibili; Trasformazione Digitale delle imprese e Digitalizzazione dei servizi pubblici. Il giorno successivo alla presentazione della nuova strategia industriale, l'Organizzazione mondiale della sanità (OMS) ha annunciato la pandemia di COVID-19.

Al fine di tener conto dell'impatto della pandemia, la strategia è stata quindi successivamente aggiornata a maggio 2021[30]. Nel contesto di questo aggiornamento, la Commissione ha condotto una serie di analisi approfondite di settori che possono essere considerati strategici per gli interessi dell'UE.

Il rapporto finale individua *sei aree strategiche in cui l'UE presenta dipendenze* strategiche: materie prime, batterie, ingredienti farmaceutici attivi, idrogeno, semiconduttori, e tecnologie *cloud* ed *edge*[31]*.*

Al fine di ridurre alcune di tali dipendenze, l'Unione ha quindi lanciato una serie di iniziative di incerta efficacia: la *European Battery Alliance* (EBA), con la quale l'UE ritiene che l'Unione potrebbe aumentare la propria quota globale di produzione di batterie al litio al 14% entro il 2024 (nel 2019 era al 5,9%); la *European Raw Materials Alliance* (ERMA), una rete che riunisce le aziende minerarie e i funzionari dei Paesi membri con l'obiettivo di garantire l'accesso alle materie prime critiche, sostenendo i progetti minerari e migliorando il riutilizzo circolare delle risorse, in particolare per i settori industriali chiave quali le energie rinnovabili, la difesa e l'*automotive*; e l'*Industrial Alliance for Processors and Semiconductor Technologies*, sfociata, da ultimo, nell'adozione dell'*EU Chip Act*, l'8 febbraio 2022, che con oltre 43 miliardi di euro di investimenti, in aggiunta ai programmi esistenti nell'ambito di

---

[30] Comunicazione della Commissione europea, *Aggiornare la nuova strategia industriale 2020: Costruire un mercato unico più forte per la ripresa dell'Europa*, COM(2021) 350 final, 5 maggio 2021. Testo disponibile al sito: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_it.

[31] Documento di lavoro della Commissione europea, *Dipendenze e capacità strategiche*, SWD(2021) 352 final, 5 maggio 2022. Testo inglese disponibile al sito: https://ec.europa.eu/info/sites/default/files/strategic-dependencies-capacities.pdf; Analisi approfondite dei settori strategici per gli interessi dell'Europa, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests_it.

Horizon Europe e Digital Europe, mira a raddoppiare la quota dell'UE nella produzione globale di *chip*, raggiungendo una quota di mercato del 20% entro il 2030.

Si tratta di misure che difficilmente raggiungeranno gli obiettivi previsti, se non al prezzo di una perdita di *competitività* – e quindi di quote di mercato globale – per i prodotti europei.

A dicembre 2020, la Commissione europea, insieme al servizio europeo per l'azione esterna (SEAE), ha anche presentato una nuova *Strategia per la Cybersicurezza*[32]*.* L'obiettivo di tale strategia è rafforzare la resilienza dell'UE a fronte delle minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali affidabili e attendibili. La nuova strategia include proposte concrete per l'introduzione di strumenti normativi, strategici e di investimento. Le Conclusioni del Consiglio adottate Il 22 marzo 2021[33], sottolineano che la cybersicurezza è essenziale per costruire un'Europa resiliente, verde e digitale e stabiliscono l'obiettivo fondamentale di raggiungere l'Autonomia Strategica mantenendo, nel contempo, un'economia aperta. Ciò implica anche il rafforzamento della capacità di compiere scelte autonome nel settore della cybersicurezza allo scopo di potenziare la *leadership* digitale e le capacità strategiche dell'UE.

Tuttavia, secondo il *Digital Economy and Society Index* (DESI) 2022[34] – l'indice di digitalizzazione dell'economia e della società attraverso cui la Commissione europea monitorizza l*a performance* digitale degli Stati membri – i Paesi dell'UE hanno compiuto progressi nei loro sforzi di digitalizzazione, ma hanno ancora difficoltà a colmare le lacune in termini di competenze digitali, trasformazione digitale delle PMI e diffusione delle reti 5G avanzate. In proposito, per l'Italia, il PNRR (su cui si veda *infra*, Capitolo III, paragrafo 5), con circa 127 miliardi di euro destinati al settore digitale, offre un'opportunità senza precedenti per accelerare la Trasformazione Digitale.

Come parte della Strategia per la cybersicurezza, l'UE sta inoltre lavorando all'aggiornamento di due direttive tese ad affrontare i rischi attuali e futuri *on-line* e *off-line*: la Direttiva sulla *Network and Information Society* (NIS) – 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi – e la Direttiva sulle Infrastrutture Critiche Europee (ICE) – 2008/114 relativa all'individuazione e alla

---

[32] Cybersicurezza: la risposta dell'UE alle minacce informatiche, https://www.consilium.europa.eu/it/policies/cybersecurity/.

[33] Conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, 22 marzo 2021, https://www.consilium.europa.eu/it/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

[34] *The Digital Economy and Society Index* (DESI), 28 luglio 2022, https://digital-strategy.ec.europa.eu/en/policies/desi.

designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

Per proteggere meglio la rete e i sistemi informativi in risposta al panorama di minacce in evoluzione e in considerazione della trasformazione digitale accelerata dalla crisi COVID-19, la Direttiva NIS riveduta (NIS 2) sostituirà la Direttiva NIS, introdotta nel 2016, quale prima misura legislativa in assoluto per tutta l'UE volta ad accrescere la cooperazione tra gli Stati membri sulla questione vitale della cybersicurezza. Essa ha definito obblighi di sicurezza per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, la sanità e la finanza) e i fornitori di servizi digitali (mercati online, motori di ricerca e servizi *cloud*). La nuova normativa sulla sicurezza delle reti e dei sistemi informativi – su cui il Consiglio e il Parlamento europeo hanno raggiunto un accordo provvisorio nel maggio 2022 – rafforzerà la gestione dei rischi e degli incidenti e la cooperazione, e amplierà l'ambito di applicazione delle norme. La Direttiva proposta individua due tipi di "grandi potenziali vittime" che definisce come entità "essenziali" o "importanti", e si applicherà a tutte le grandi e medie imprese appartenenti ai settori identificati, nonché alle piccole imprese di tali settori che rappresentino colli di bottiglia nella catena del valore oppure siano operatori attinenti alle reti o ai servizi digitali. Le entità "essenziali" sono: Energia, Trasporti, Banche, Infrastrutture dei mercati finanziari, Sanità, Acqua potabile, Acque reflue, Infrastrutture digitali, Pubblica amministrazione, e Spazio. La novità interessante è l'ingresso dei seguenti nuovi settori ritenuti "importanti", quindi con obblighi minori, ma comunque attenzionati: Servizi postali e corrieri, Smaltimento rifiuti, Manifattura, produzione e distribuzione di prodotti chimici, Produzione, elaborazione e distribuzione di alimenti, Manifattura, e Provider di servizi digitali.

La nuova direttiva che revisiona la Direttiva ICE (Direttiva ICE 2), dedicata al tema della resilienza delle entità critiche rispetto a minacce fisiche (c.d. cinetiche), imporrà di adottare una strategia nazionale di *cybersecurity* in ogni Stato membro, con una Autorità competente alla attuazione designata per legge. Essa individua i seguenti settori come potenzialmente "critici": Energia, Trasporti, Banche, Infrastrutture dei mercati finanziari, Sanità, Acqua potabile, Acque reflue, Infrastrutture digitali, Pubblica amministrazione e Spazio – che poi sono gli stessi che la Direttiva NIS 2 definisce di livello "essenziale". Gli operatori pubblici e privati, che verranno identificati e designati sulla base di una Analisi del Rischio basata su indicatori standardizzati, avranno obblighi inerenti alla valutazione e la gestione del rischio, obblighi di notifica all'Autorità competente e obblighi di condivisione delle informazioni. La Direttiva ICE 2 si occupa anche di certificazione e standardizzazione di *cybersecurity* e creerà una rete informativa denominata *Cyber Crisis Liaison Organization*

Network (CyCLONe), per la gestione di un *framework* di *cybersecurity* e il rafforzamento delle *supply chain*.

Da richiamare è, infine, Bussola strategica (*Strategic Compass*), adottata a marzo 2022 per rafforzare la sicurezza e la difesa dell'UE nel prossimo decennio[35].

La Bussola copre tutti gli aspetti della politica di sicurezza e di difesa ed è strutturata attorno a quattro pilastri: Azione (con la reazione, fra l'altro, della capacità di dispiegamento rapido forte di un massimo di 5.000 militari per diversi tipi di crisi); Investimenti per rafforzare la nostra base industriale e tecnologica di difesa europea, anche con l'obiettivo di potenziare l'innovazione tecnologica per la difesa al fine di colmare le lacune strategiche e ridurre le dipendenze tecnologiche e industriali; *Partner* quali la NATO, le Nazioni Unite e i *partner* regionali, tra cui l'OSCE, l'Unione Africana e l'Associazione delle Nazioni del Sud-Est Asiatico (ASEAN), partenariati bilaterali mirati e partenariati su misura; Sicurezza, attraverso l'adozione di pacchetti di strumenti contro le minacce ibride, gli attacchi informatici, la manipolazione delle informazioni e le ingerenze da parte di attori stranieri, la diplomazia informatica, e lo sviluppo di una strategia dell'UE per la sicurezza e la difesa nello spazio nonché per la sicurezza marittima.

Per quanto non scontate, la Bussola strategica può avere ricadute positive per l'Italia sullo strumento militare, ma anche sulla base industriale e tecnologica nazionale.

9. I recenti indirizzi strategici della NATO

Il nuovo Concetto strategico della NATO (*North Atlantic Treaty Organization*), adottato il 29 giugno 2022 a Madrid[36], delinea una serie di priorità derivanti dalla guerra della Russia contro l'Ucraina, ma presenta anche novità rilevanti per quanto riguarda la Cina e l'Indo-Pacifico.

Fra le linee guida dell'Alleanza in una prospettiva di medio termine qui rilevanti vi è, innanzitutto, l'attenzione combinata alla guerra spaziale, cibernetica e ibrida. I domini *spaziale* e *cibernetico* sono pienamente integrati nella nuova postura di deterrenza e difesa della NATO.

Vi si legge, infatti, che: "*Un insieme singolo o cumulativo di attività informatiche dannose o di operazioni ostili verso, da o all'interno dello spazio potrebbe raggiungere il*

---

35 Una bussola strategica per l'UE, https://www.consilium.europa.eu/it/infographics/strategic-compass/.

36 *NATO 2022 Strategic Concept*, adottato dai Capi di Stato e di Governo al NATO Summit di Madrid il 29 giugno 2022. Testo disponibile al sito https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

livello di un attacco armato e potrebbe portare il Consiglio del Nord Atlantico a invocare l'articolo 5 del Trattato del Nord Atlantico" sulla difesa collettiva[37].

Questa disposizione non è del tutto nuova, in quanto riflette le dichiarazioni dei precedenti vertici alleati[38]. Tuttavia, la sua inclusione è estremamente importante perché conferisce un mandato più stabile e di alto livello alle strutture della NATO e ai militari alleati per sviluppare dottrine e capacità per le operazioni cibernetiche e spaziali.

Il Concetto Strategico considera anche le tattiche ibride attraverso la lente della difesa collettiva: "*Le operazioni ibride contro gli alleati potrebbero raggiungere il livello di attacco armato e potrebbero portare il Consiglio Nord Atlantico a invocare l'articolo 5*"[39].

Vi è, inoltre, la consapevolezza del rischio per la NATO di perdere il proprio vantaggio militare a causa dei massicci e generalizzati investimenti della Cina nelle nuove tecnologie e delle capacità di nicchia della Russia, ad esempio, nelle armi ipersoniche.

Per questo motivo, con il nuovo Concetto Strategico, gli Stati membri si impegnano – collocando questo obiettivo tra i compiti fondamentali della difesa collettiva – a: "promuovere l'innovazione e ad aumentare i nostri investimenti in *tecnologie emergenti e dirompenti* per mantenere la nostra interoperabilità e il nostro vantaggio militare".

Il riferimento all'*interoperabilità* è importante, perché mentre l'innovazione degli Stati Uniti si muove velocemente, i Paesi europei sono in ritardo a causa della frammentazione degli sforzi. Per l'Italia e gli altri Stati europei, quindi, l'enfasi della NATO sull'interoperabilità significa innanzitutto cooperazione, coordinamento e integrazione delle scelte industriali, sviluppando e producendo al contempo tecnologie europee rilevanti per la difesa nazionale e collettiva[40].

---

37 Come noto, ai sensi dell'articolo 5 del Trattato NATO: "*Le Parti convengono che un attacco armato contro uno o più di loro in Europa o Nord America sarà considerato un attacco contro tutti loro*".

38 Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries: Comparing Models", in IAI Papers, No. 21|05 (February 2021), testo disponibile al sito: https://www.iai.it/en/node/12727; Alessandro Marrone and Michele Nones (eds), "The Expanding Nexus between Space and Defence", in Documenti IAI, No. 22|01 (February 2022), testo disponibile al sito: https://www.iai.it/en/node/14669.

39 Can Kasapoğlu et al., "Countering Hybrid Threats: A New NATO Core Task", in *Clingendael Spectator series: Geopolitics & Global Order*, 22 giugno 2022, testo disponibile al sito: https://spectator.clingendael.org/en/node/5546.

40 Felix Arteaga et al., "To Face the Russian Threat Europeans Need to Spend Together - Not Side by Side", in EURACTIV, 19 aprile 2022, testo disponibile al sito: https://www.euractiv.com/?p=1745658.

Capitolo III. Strumenti finanziari e programmi di investimento

1. Premessa

Come ben messo in luce dal Presidente del Consiglio dei Ministri, Mario Draghi, nella Prefazione alla Strategia per la Cybersicurezza, per intensificare i progetti di sviluppo tecnologico per arrivare a disporre di un adeguato livello di Autonomia Strategica e quindi garantire la nostra Sovranità Digitale, è "cruciale stanziare fondi *adeguati*, *con continuità*" (Strategia, p. 4; *emphasis added*).

Ai fini della propria implementazione, la stessa Strategia richiama una serie di strumenti finanziari e programmi di investimenti, fra i quali: fondi nazionali e leve finanziarie previsti di anno in anno dalle leggi finanziarie, per supportare specifici progetti di interesse; i finanziamenti provenienti dai programmi Orizzonte Europa ed Europa Digitale; e il Piano Nazionale di Ripresa e Resilienza (PNRR).

Poiché ciascuno di questi fondi e programmi è sì relativo alla cybersicurezza ma riguarda più in generale la Sovranità Tecnologica e Digitale e l'Autonomia Strategica – alla cui realizzazione è preordinata questa ricerca e di cui la cybersicurezza costituisce un pilastro fondamentale – è opportuno qui passarli in rassegna, anche nella loro dimensione (più ampia) non menzionate nella Strategia.

2. Fondi nazionali

Per quanto riguarda i fondi nazionali, oltre gli strumenti finanziari già assegnati alle Amministrazioni – si tratta di una quota percentuale (1,2%) degli investimenti nazionali lordi su base annuale da dedicare a specifiche progettualità volte a traguardare il conseguimento dell'autonomia tecnologica in ambito digitale. Tali leve finanziarie potranno anche consistere in *sgravi fiscali* per le aziende o nell'introduzione di aree nazionali a *tassazione agevolata* per la costituzione, ad esempio, di un "parco nazionale della cybersicurezza" e dei relativi "*hub*" delocalizzati sull'intero territorio nazionale (su si veda, *infra*, Capitolo IV, paragrafo 6).

3. Orizzonte Europa

Il Programma Orizzonte Europa, con un Bilancio totale 2021-2027 di 95,51 miliardi di Euro, è il principale programma di finanziamento dell'UE per facilitare la collaborazione e rafforzare l'impatto della ricerca e dell'innovazione nello sviluppo, nel sostegno e nell'attuazione delle politiche dell'UE, affrontando, nel contempo, le sfide globali. Esso sostiene la creazione e una migliore diffusione di conoscenze e tecnologie di eccellenza. Inoltre, crea posti di lavoro, impegna pienamente il bacino di talenti dell'UE, stimola la

crescita economica, promuove la competitività industriale e ottimizza l'impatto degli investimenti all'interno di uno Spazio europeo della ricerca rafforzato.

4. Fondo Europeo per la Difesa

Oltre ad essere integrato dal Programma Euratom di ricerca e formazione, il Programma Orizzonte Europa è attuato anche tramite un altro programma specifico: il Fondo europeo per la Difesa (*European Defense Fund* (EDF)) – entrambi con un programma di lavoro distinto.

Al riguardo, la Commissione europea ha adottato il secondo programma di lavoro annuale del Programma EDF, che assegnerà fino a un totale di 924 milioni di Euro di finanziamenti, introducendo una serie di nuovi strumenti per promuovere l'innovazione nel settore della Difesa.

5. Europa Digitale

Il Programma Europa Digitale ha un Bilancio totale 2021-2027 di 7,59 miliardi di Euro. È il primo piano europeo di finanziamento per espandere le competenze digitali dei cittadini e delle imprese e per velocizzare la ripresa economica e sociale. Il Programma, che mira a colmare il divario tra la ricerca sulle tecnologie digitali e la diffusione sul mercato, finanzia progetti in cinque settori cruciali: Supercalcolo, AI, Cybersicurezza, Competenze digitali avanzate, Uso diffuso delle tecnologie digitali nell'economia e nella società[41].

Gli investimenti sostengono il duplice obiettivo dell'Unione della transizione verde e della Trasformazione Digitale (di cui si è detto *supra*, Capitolo II, paragrafo 8), e rafforzano la resilienza e la sovranità digitale dell'Unione.

6. PNRR

Il PNRR cui si è più volte fatto cenno, è il pacchetto di investimenti e riforme predisposto dall'Italia per beneficiare dei fondi del programma *Next Generation EU* (NGEU), con cui l'Unione mira ad accelerare la transizione ecologica e digitale (oltre che a migliorare la formazione delle lavoratrici e dei lavoratori, e conseguire una maggiore equità di genere, territoriale e generazionale).

L'Italia è la prima beneficiaria dei due principali strumenti del NGEU: il Dispositivo per la Ripresa e Resilienza (*Recovery and Resilience Facility* (RRF)) e il Pacchetto di

[41] *Digital Europe 2021-2027*, https://first.art-er.it/_aster_/viewProgramma/754/digital-europe-2021-2027.

Assistenza alla Ripresa per la Coesione e i Territori d'Europa (REACT-EU). Il dispositivo RRF richiede agli Stati membri di presentare un pacchetto di investimenti e riforme: il PNRR[42], appunto.

Il PNRR si articola in sei Missioni e 16 Componenti. Le sei Missioni del Piano sono: Digitalizzazione, innovazione, competitività, cultura e turismo; Rivoluzione verde e transizione ecologica; Infrastrutture per una mobilità sostenibile; Istruzione e ricerca; Inclusione e coesione e Salute.

Il PNRR Transizione Digitale, relativo alla Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", ha un bilancio totale 2021-2026 di 122,6 miliardi di Euro.

Le risorse stanziate nel PNRR, pari a 191,5 miliardi di euro, sono così ripartite fra le sei Missioni: Digitalizzazione, innovazione, competitività e cultura - 40,32 miliardi; Rivoluzione verde e transizione ecologica - 59,47 miliardi; Infrastrutture per una mobilità sostenibile - 25,40 miliardi; Istruzione e ricerca - 30,88 miliardi; Inclusione e coesione - 19,81 miliardi; Salute - 15,63 miliardi. Per finanziare ulteriori interventi il Governo italiano ha approvato un Fondo complementare con risorse pari a 30,6 miliardi di euro – per cui complessivamente gli investimenti previsti sono pari a 222,1 miliardi di euro[43],

Nel suo ambito, sono incluse le attività di transizione digitale della PA, quali il progetto del *Cloud* Nazionale e la digitalizzazione dei processi e servizi per i cittadini, la cui realizzazione porterà al potenziamento delle capacità di resilienza delle infrastrutture e dei servizi digitali del Paese (Strategia, p. 13). La cybersicurezza e la resilienza sono poste a fondamento della trasformazione digitale della PA. Secondo la Strategia Nazionale di Cybersicurezza, "la transizione verso il *Cloud* della PA, sia verso tecnologie di *Public Cloud* che mediante la creazione di un Polo Strategico Nazionale (PSN), rappresenta un elemento fondante per garantire adeguate garanzie di autonomia tecnologica del Paese" (*ibidem*, p. 18)[44].

---

[42] Italia digitale 2026, https://innovazione.gov.it/dipartimento/focus/italiadigitale-2026/ e *National Plan of Recovery and Resilience*, https://italiadomani.gov.it/en/home.htm

[43] PNRR - Piano Nazionale di Ripresa e Resilienza, https://www.mise.gov.it/index.php/it/pnrr/piano.

[44] La strategia Cloud Italia è stata adottata nell'ambito del Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022 e definita dal Dipartimento per la trasformazione digitale in collaborazione con l'Agenzia per la Cybersicurezza Nazionale, al fine di incentivare la diffusione di soluzioni basate sul *cloud computing* nel circuito delle Pubbliche Amministrazioni.

7. Soggetti responsabili della relativa implementazione

La recente riforma dell'architettura nazionale *cyber*, che è stata attuata attraverso l'adozione del decreto-legge 14 giugno 2021 n. 82[45], ha istituito l'*Agenzia per la Cybersicurezza Nazionale* (ACN), di cui si dirà più ampiamento nel prossimo Capitolo (Capitolo IV).

In questa sede, preme rilevare che l'ACN non è solo l'autorità responsabile per la gestione dei fondi nazionali. Vi sono anche i finanziamenti che l'Agenzia è chiamata a gestire in quanto, sempre ai sensi del citato decreto, è designata quale *Centro Nazionale di Coordinamento* (*National Coordination Centre* (NCC)) ai sensi dell'articolo 6 del Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (*Network of National Coordination Centres* (NCCs)).

Quale NCC, l'ACN convoglia in particolare i finanziamenti provenienti dai programmi Orizzonte Europa ed Europa Digitale.

Nell'ambito della Missione 1 del PNRR ("Digitalizzazione, innovazione, competitività, cultura e turismo"), lo specifico Investimento 1.5 "Cybersecurity" – pari a 623 milioni di euro – rimesso all'ACN quale *Soggetto Attuatore*, prevede la realizzazione di specifiche progettualità per la creazione e lo sviluppo di servizi all'avanguardia per la gestione del rischio *cyber*, con strette connessioni, a livello nazionale e internazionale, con tutti i principali *partner* della PA, dell'impresa e dei fornitori di tecnologia.

Il piano di attuazione, d'intesa con il *Dipartimento per la Trasformazione Digitale (DTD)* – istituito con decreto del Presidente del Consiglio dei Ministri nel 2019[46] – nella sua veste di *Amministrazione Titolare* dell'investimento, è organizzato in tre principali aree d'intervento: Servizi *cyber* nazionali (174 M€), Potenziamento della resilienza *cyber* per la PA (301.7 M€); e Laboratori di scrutinio e certificazione tecnologica (147.3 M€).

In accordo alle regole tecnico-organizzative del PNRR, esso coinvolgerà tutti i principali attori nazionali, pubblici e privati, del mondo della *cybersecurity*.

---

[45] Il decreto-legge 14 giugno 2021 n. 82, recante Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, è stato convertito, con modificazioni, dalla legge 4 agosto 2021 n. 109.

[46] Su cui, ugualmente, si veda *amplius*, Capitolo IV, paragrafo 4.

Capitolo IV. Attori responsabili e altri soggetti portatori di interessi

1. Premessa

La recente riforma dell'architettura nazionale *cyber* ha istituito l'Agenzia per la cybersicurezza nazionale (ACN) con l'obiettivo – nel rispetto delle competenze attribuite dalla normativa vigente ad altre Amministrazioni – di razionalizzare e semplificare il frammentato sistema di competenze, esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico (articolo 5 del decreto-legge 14 giugno 2021 n. 82)[47].

Nella Strategia Nazionale di Cybersicurezza si legge che: "la cybersicurezza, che è divenuta una questione di importanza strategica, deve porsi *a fondamento del processo di digitalizzazione del Paese, quale elemento imprescindibile della Trasformazione Digitale*, anche nell'ottica di conseguire *l'Autonomia Nazionale Strategica nel settore*" (Strategia, p. 5, *emphasis added*)[48].

Il Presidente del Consiglio ha affermato la necessità di garantire la nostra Sovranità Digitale. Vi è ormai una chiara convergenza di opinioni tra le parti sociali e le forze politiche, che la cybersicurezza tanto della nazione come delle imprese rappresenti un pilastro della Sovranità Digitale.

Ha senso dunque approfondire la nuova architettura nazionale *cyber*, relativamente poco conosciuta, attuata attraverso l'adozione del decreto-legge 14 giugno 2021 n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021 n. 109.

2. Direzione politico-strategica della Presidenza del Consiglio dei Ministri, CIC e CISR

Il livello politico è rappresentato dal Presidente del Consiglio dei ministri, dall'Autorità delegata per la sicurezza della Repubblica e dal Comitato Interministeriale per la Sicurezza della Repubblica (CISR). Sempre a livello politico-strategico, primaria importanza riveste il Comitato Interministeriale per la Cybersicurezza (CIC), che esercita l'alta sorveglianza sulla implementazione della strategia.

---

[47] Il decreto-legge 14 giugno 2021, n. 82, recante Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, è stato convertito, con modificazioni, dalla legge 4 agosto 2021 n. 109.

[48] Il concetto della sicurezza e resilienza cibernetica quale fondamento del processo di digitalizzazione del Paese è ulteriormente ribadito, per esempio, a p. 7 della Strategia.

Il *Presidente del Consiglio dei ministri*, vertice dell'architettura istituzionale e organo d'indirizzo politico-strategico in materia, esercita l'alta direzione e detiene la responsabilità generale delle politiche di cybersicurezza.

Questi può delegare all'Autorità delegata per la sicurezza della Repubblica, di cui all'articolo 3 della legge 3 agosto 2007, n. 124, le funzioni che non sono ad esso attribuite in via esclusiva[49]. Il decreto-legge 14 giugno 2021 n. 82 assegna al Presidente del Consiglio il potere di adottare, sentito il Comitato interministeriale per la Cybersicurezza (CIC), le linee di indirizzo. Il Presidente del Consiglio a sua volta è tenuto a presentare al Parlamento (e alla cittadinanza) una relazione annuale sull'attività svolta dalla ANC.

Il *CIC*, istituito presso la Presidenza del Consiglio dei ministri, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, rappresenta la sede politica nella quale esaminare e indirizzare le problematiche relative alla cybersicurezza, condividere gli obiettivi strategici e gli indirizzi, nonché monitorare l'attuazione delle politiche in materia. A tal fine, il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, dal Ministro degli affari esteri e della cooperazione internazionale (MAECI), dal Ministro dell'Interno, dal Ministro della Giustizia, dal Ministro della Difesa (Min. Difesa), dal Ministro dell'Economia e delle Finanze (MEF), dal Ministro dello Sviluppo Economico (MISE), dal Ministro della Transizione Ecologica, dal Ministro dell'Università e della Ricerca (MUR), dal Ministro delegato per l'innovazione tecnologica e la transizione digitale (MITD) e dal Ministro delle infrastrutture e della mobilità sostenibili.

In particolare, il CIC è sentito dal Presidente del Consiglio ai fini dell'adozione della strategia nazionale di cybersicurezza ed esercita l'alta sorveglianza sulla sua attuazione. Contribuisce, inoltre, alla realizzazione della strategia stessa proponendo al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza e promuovendo l'adozione delle iniziative necessarie a favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, alla condivisione delle informazioni e all'adozione di migliori pratiche e di misure e allo sviluppo industriale, tecnologico e scientifico in materia.

Il Comitato interministeriale per la sicurezza della Repubblica (CISR) è un organismo con composizione analoga al CIC, di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza.

---

[49] Il 13 settembre 2021, il Presidente del Consiglio ha conferito la delega in materia di *cybersecurity* al Sottosegretario di Stato, ora Autorità delegata per la sicurezza della Repubblica, Prefetto Franco Gabrielli.

3. L’ACN

L’ANC costituisce al tempo stesso autorità di raccordo con il livello politico-strategico e di coordinamento degli attori coinvolti in materia, nonché di regolamentazione, certificazione e vigilanza del settore.

Ciò al fine di assicurare iniziative coerenti, rappresentare un chiaro e aggiornato quadro situazionale all’Autorità politica, nonché fornire un’*interfaccia unica a livello nazionale, europeo e internazionale*, assicurando una *postura nazionale unitaria* (così il Piano di implementazione della Strategia nazionale di cybersicurezza 2022-2026 – d’ora innanzi anche semplicemente “Piano di implementazione” – p. 26; *emphasis added*).

L’ACN svolge molteplici compiti istituzionali (ai sensi dell’articolo 7 del decreto-legge 14 giugno 2021 n. 82).

In qualità di *Autorità nazionale per la cybersicurezza*, essa ha tra i suoi compiti quello di predisporre la strategia nazionale di cybersicurezza (lett. b); assicura inoltre il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza; e promuove, anche in un’ottica di rafforzamento della *partnership* pubblico-privato, la realizzazione di una cornice di sicurezza e resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle PA, nonché per il conseguimento dell’autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore.

È designata quale *Autorità nazionale competente in via esclusiva e punto di contatto unico (PoC) in materia di sicurezza delle reti e dei sistemi informativi*, per le finalità di cui al decreto (legislativo di attuazione della direttiva) NIS, a tutela dell'unità giuridica dell'ordinamento (lett. d).

È *Autorità nazionale di certificazione della cybersicurezza* ai sensi dell’articolo 58 del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al MISE (lett. e).

È designata quale *Centro Nazionale di Coordinamento* (NCC) ai sensi dell’articolo 6 del Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell’ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (NCCs, di cui è detto *supra*, Capitolo III, paragrafo 6) (lett. aa).

Assume, inoltre, tutte le funzioni già attribuite al MISE (lett. f) e all'Agenzia per l’Italia digitale (lett. m) in materia di cybersicurezza, nonché tutte le funzioni attribuite alla

Presidenza del Consiglio dei ministri in materia di Perimetro di sicurezza nazionale cibernetica (PSNC) (lett. h).

A seguito delle modifiche introdotte in sede di conversione del decreto-legge, ai sensi del medesimo articolo 7, l'ACN assume anche le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza: "In particolare, l'*Agenzia attiva ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia*, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali" (lett. m-*bis* [aggiunta in sede di conversione del decreto-legge]; *emphasis added*). E provvede alla qualificazione dei servizi *cloud* per la PA nel rispetto della disciplina dell'UE (m-*ter* [aggiunto in sede di conversione del decreto-legge]).

Nel dominio della cybersicurezza, inoltre, l'ACN cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale (lett. p); coordina, in raccordo con il MAECI, la cooperazione internazionale e cura i rapporti con i competenti organismi, istituzioni ed enti, nell'ambito dell'UE e a livello internazionale (lett. q)[50].

Mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, l'ACN supporta lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche e il trasferimento tecnologico dei risultati della ricerca nel settore, anche attraverso il finanziamento di specifici progetti ed iniziative (lett. r); stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza (lett. s); promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'UE e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali (lett. t); svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza (lett. u); e nel medesimo campo, promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane sulla base di apposite convenzioni con soggetti pubblici e privati (lett. v).

Le funzioni attribuite alla ACN esprimono "un approccio olistico" non solo alla gestione della cybersicurezza (come efficacemente messo in luce nel Piano di implementazione, p. 27), ma più in generale alla Sovranità Tecnologica. Lo stesso Piano di implementazione

[50] Ai fini dello svolgimento delle funzioni sopra illustrate, operano presso l'Agenzia: il *Computer Security Incident Response Team* (CSIRT) Italia, la cui azione è volta alla prevenzione, al monitoraggio, al rilevamento, all'analisi e alla risposta ad incidenti cibernetici; il Centro di Valutazione e Certificazione Nazionale (CVCN), che si occupa di verificare la sicurezza e l'assenza di vulnerabilità note in beni, sistemi e servizi ICT in uso nelle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese; il Centro Nazionale di Coordinamento in materia di cybersicurezza nell'ambito industriale, tecnologico e della ricerca.

afferma che parte integrante della scelta strategica è "la creazione di un ecosistema nazionale di cybersicurezza, nel quale i diversi soggetti interessati possano operare in modo coordinato per garantire al sistema Paese di sfruttare al meglio le molteplici opportunità offerte dai processi di innovazione tecnologica, contribuendo così alla prosperità e allo sviluppo economico-sociale dell'Italia"; e che questa scelta è alla "base della recente riforma dell'architettura nazionale cyber – realizzata con il decreto-legge 14 giugno 2021 n. 82 – attraverso cui il legislatore ha inteso riordinare e razionalizzare le competenze nazionali in materia di sicurezza cibernetica (prima frammentate e poste in capo a una pluralità di attori istituzionali), creando un ente centrale con competenza in materia, che possa anche rappresentare il punto di raccordo tra i diversi soggetti interessati. Ciò, anche al fine di consentire l'attuazione degli obiettivi strategici all'interno di un sistema coordinato e armonizzato, nel quale l'unicità dell'indirizzo definito dal vertice politico sia garantita, in via di attuazione, tramite l'azione organizzata degli attori coinvolti" (Piano di implementazione, p. 24).

4. Il necessario raccordo con le altre Amministrazioni

Il decreto-legge 14 giugno 2021 n. 82 afferma la necessità per l'ACN: di assicurare "il necessario raccordo con *le altre amministrazioni* a cui la legge attribuisce competenze in materia di cybersicurezza e, *in particolare, con il Ministero della difesa* per gli aspetti inerenti alla ricerca militare e a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa" e di rispettare le competenze del MAECI (articolo 7, lettere r-t; *emphasis added*).

Il disegno complessivo dell'architettura istituzionale di cybersicurezza rende imprescindibile il concorso in stretta sinergia con altre Amministrazioni, cui la normativa vigente assegna prerogative esclusive in aderenza ai rispettivi mandati istituzionali (così il Piano di implementazione, p. 29).

La stessa Strategia considera la *cooperazione sul piano interno* uno dei "fattori abilitanti" rispetto al raggiungimento dei tre obiettivi fondamentali previsti[51]: Protezione, Risposta e Sviluppo. Per tutte le misure destinate all'implementazione dell'Obiettivo Sviluppo – su cui si veda *infra*, paragrafo 6) – individua come "Attori responsabili" accanto

[51] Tale cooperazione si specifica, fra l'atro, nella Misura #74 prevista nel Piano di implementazione che prevede di: "*Istituire tavoli operativi permanenti con i soggetti Perimetro, suddivisi per settore, che svolgano a livello operativo specifici compiti in materia di prevenzione, allertamento, risposta agli incidenti e ripristino*". Soggetto responsabile per la sua attuazione è l'ACN, mentre "Altri soggetti interessati" sono "Amministrazioni centrali, Regioni e Province autonome, Associazioni di categoria, Operatori privati" (Piano di implementazione, p. 20).

all'ANC, i dicasteri di volta in volta coinvolti (MISE, MITD, MEF, Min. Difesa, MUR e MAECI)[52], mentre designa come "Altri soggetti interessati": altre Amministrazioni centrali, Regioni e Province autonome, Operatori privati, Associazioni di categoria, Atenei e/o Enti di ricerca.

La riforma ha anche istituito presso la Presidenza del Consiglio dei ministri, il **Comitato interministeriale per la cybersicurezza (CIC)**, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Come si è sopra ricordato (paragrafo 2), il CIC è presieduto dal Presidente del Consiglio dei ministri ed è composto dal MAECI, dal Ministro dell'Interno, dal Ministro della Giustizia, dal Min. della Difesa, dal MEF, dal MISE, dal Ministro della transizione ecologica, dal MUR, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili. Tuttavia, il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, i direttori del Dipartimento delle informazioni per la sicurezza (DIS) e dell'Agenzia informazioni e sicurezza esterna (AISE)[53], nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare (articolo 4 del decreto-legge 14 giugno 2021 n. 82).

Il **Dipartimento per la Trasformazione Digitale (DTD)**, istituito con decreto del Presidente del Consiglio dei Ministri nel 2019 (di cui si è detto *supra*, Capitolo III, paragrafo 6), è la struttura di supporto al Presidente del Consiglio dei ministri per la promozione ed il coordinamento delle azioni del Governo finalizzate alla definizione di una strategia *unitaria* in materia di trasformazione digitale della PA e di modernizzazione del Paese attraverso le tecnologie digitali, anche al fine di realizzare gli obiettivi dell'Agenda digitale italiana; lavora anche a supporto del MITD e svolge, inoltre, tutte le attività volte ad assicurare, in raccordo con le amministrazioni interessate, lo sviluppo e la diffusione delle competenze necessarie per un adeguato uso delle tecnologie digitali nei mondi della scuola, dell'università e della ricerca, della PA centrale e locale, della giustizia, dell'impresa, del lavoro e dell'attività sociale. Esso dà attuazione alle direttive del Presidente in materia e assicura il coordinamento e l'esecuzione dei programmi di trasformazione digitale[54].

---

[52] Sulle principali prerogative esclusive e competenze trasversali in materia dei vari ministeri, si veda il Piano di implementazione, pp. 29-30.

[53] Si tratta dell'Agenzia informazioni e sicurezza esterna di cui all'articolo 6 della legge 3 agosto 2007 n. 124.

[54] Oltre che alla definizione delle politiche per la modernizzazione del Paese con le tecnologie digitali e al coordinamento e all'attuazione dei programmi di trasformazione digitale, il DTD fornisce supporto al Presidente del Consiglio dei Ministri per l'esercizio delle funzioni di cui all'articolo 8, commi 1-*ter* e 3, del decreto-legge 14 dicembre 2018 n.135,

Fondamentale e decisivo apporto è inoltre fornito dalle Amministrazioni componenti dei diversi **tavoli interistituzionali**, istituiti a fini di coordinamento interministeriale.

Particolare rilievo ha il **Nucleo per la Cybersicurezza (NCS)**, che, istituito presso l'ACN, opera a supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla prevenzione e alla preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. L'NCS può facilitare, in particolare, il raggiungimento dell'Obiettivo Risposta; esso garantisce, infatti, l'allineamento tra l'ACN, il Consigliere militare del Presidente del Consiglio dei ministri, il Comparto *intelligence*, il MAECI, il Ministero dell'interno, il Ministero della Giustizia, il Min. Difesa, il MEF, il MISE, il Ministero della transizione ecologica, il Ministero delle infrastrutture e della mobilità sostenibili, il MUR, e il Dipartimento per la trasformazione digitale. Al contempo, il Nucleo, cui spetta il compito di formulare proposte di iniziativa in materia di cybersicurezza, è anche una piattaforma nella quale discutere le diverse iniziative promosse dalle Amministrazioni con riflessi sulle politiche di cybersicurezza e può, pertanto, rappresentare la sede principale attraverso cui assicurare lo sviluppo coordinato di iniziative concernenti anche gli altri Obiettivi della Strategia – Protezione degli *assets* strategici nazionali e Risposta alle minacce *cyber*. In tale contesto, possono essere chiamati a partecipare i soggetti interessati anche privati.

Ulteriori sedi sempre ai fini del coordinamento interistituzionale, oltre all'NCS, sono rappresentate dal **Tavolo interministeriale** per l'attuazione del Perimetro di sicurezza nazionale cibernetica (PSNC), nonché dal **Comitato tecnico di raccordo** di cui al decreto di attuazione della direttiva NIS – entrambi previsti per il raggiungimento degli obiettivi della Strategia (Piano di implementazione, p. 32)

5. Partnership Pubblico-Privato (PPP)

Gli operatori privati – di carattere economico ma anche l'accademia e la ricerca – e la società civile tutta sono *players* essenziali della Transizione Digitale e possono giuocare un ruolo cruciale per la Sovranità Tecnologica nazionale (*supra*, Capitolo I, paragrafo 4).

La Strategia nazionale di cybersicurezza, improntata ad un approccio "*whole-of-society*", che vede il settore pubblico agire sinergicamente con quello privato, considera la *Partnership* Pubblico-Privato (PPP) imprescindibile per la resilienza del Sistema-Paese e trasversale rispetto ai citati Obiettivi di Protezione, Risposta e Sviluppo, nonché ai fattori abilitanti della formazione, della promozione della cultura della cybersicurezza e della

per l'esercizio della vigilanza sulla società di cui all'articolo 8, comma 2, del decreto-legge 14 dicembre 2018 n.135, e nella partecipazione alle sedi istituzionali internazionali nelle quali si discute di innovazione tecnologica ed agenda digitale europea.

cooperazione, che concorrono alla loro realizzazione. Del resto, lo spazio cibernetico è costituito da prodotti e servizi ICT realizzati ovvero erogati principalmente da soggetti privati.

Per tale ragione, la Strategia: “non può prescindere da una piena collaborazione e costante consultazione pubblico-privato, che si traduce in una serie di azioni strutturate come, a titolo di esempio, il monitoraggio dello spazio cibernetico attraverso la cooperazione dei SOC [*Security Operation Center*], la mitigazione degli incidenti mediante la collaborazione tra CSIRT e l’*incident response* qualificato, la rete di laboratori di prova, la formazione e la diffusione della consapevolezza” (Strategia, p. 26).

“In tal senso, anche attraverso il fondamentale stimolo e contributo offerto dall’ACN e sulla base delle funzioni ad essa attribuite per legge, andrà ricercata e sostenuta una costante collaborazione, da incrementare tramite specifiche intese e convenzioni, fra le amministrazioni pubbliche sopra elencate, le università, gli enti di ricerca e gli operatori privati (anche attraverso le associazioni di categoria). Ciò al fine di garantire una proficua interazione tanto con i soggetti che gestiscono asset ICT strategici, quanto con l’intero tessuto produttivo nazionale, incluse le PMI e le *startup*.

Frutto di un’efficiente collaborazione pubblico-privata è, ad esempio, il *Framework* Nazionale per la *Cybersecurity* e la *Data Protection*, realizzato dal CIS-Sapienza e dal Consorzio Interuniversitario Nazionale per l’Informatica (CINI). Il *framework* fornisce una metodologia applicabile, a livello trasversale e indipendentemente dalla dimensione, da organizzazioni pubbliche e private, per supportare l’avvio di iniziative orientate alla *cybersecurity* e alla protezione dei propri *asset*, così da ridurre le vulnerabilità e i rischi a cui tali organizzazioni sono esposte[55].

Ulteriori iniziative volte ad accrescere la *partnership* pubblico-privata e con il mondo dell’accademia e della ricerca sono quelle avviate in materia di promozione e rafforzamento della consapevolezza circa l’importanza della sicurezza informatica. Tra queste, si annoverano le conferenze e gli eventi organizzati su scala nazionale quali ITASEC, nonché quelle finalizzate alla creazione di una solida forza lavoro nazionale di giovani talenti altamente specializzati nel settore della sicurezza cibernetica, come CyberChallenge.it, programma di formazione avviato dal CINI e che proseguirà beneficiando anche della collaborazione dell’ACN.

[55] Il documento viene periodicamente aggiornato e integrato, al fine di assicurare piena aderenza alle più recenti normative di settore, dal Regolamento Generale sulla Protezione dei Dati (GDPR), al *Cybersecurity Act* e alle misure in materia di sicurezza della *supply chain*.

Dal punto di vista dello sviluppo della ricerca nel campo della *cybersecurity*, rilevano, inoltre, gli otto centri di competenza istituiti dal MISE – in cui la *partnership* pubblico-privata è orientata a realizzare attività di addestramento e supporto nella realizzazione di progetti innovativi nel settore Impresa 4.0 – i *Digital Innovation Hub* (DIH) e i dodici *Cluster* tecnologici istituiti dal MUR[56]." (Piano di implementazione, pp. 32-33).

6. L'Obiettivo "Sviluppo" secondo la Strategia nazionale di cybersicurezza

Come si è accennato, la Strategia individua tre obiettivi fondamentali: Protezione, Risposta e Sviluppo, quest'ultimo definito come "*lo sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato*" (Strategia, p. 22). Si tratta di un obiettivo che va oltre l'ambito specifico della cybersicurezza per abbracciare l'intero dominio della Transizione Digitale e, quindi, della Sovranità Tecnologica.

Per il raggiungimento di questo obiettivo – che potrebbe essere utilmente ridenominato "**Obiettivo Sviluppo per la Sovranità Tecnologica**" – la Strategia individua cinque misure fondamentali. Tali misure si aggiungono ai numerosi strumenti e iniziative già avviati negli ultimi anni (in particolare, quelli previsti dal PNRR)[57].

La prima misura è il già menzionato **Centro Nazionale di Coordinamento (NCC)** "che, in stretto raccordo con il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, è chiamato a supportare lo sviluppo e il potenziamento dell'autonomia strategico-tecnologica e digitale dell'UE e del nostro Paese. Ciò, *coordinando le attività di ricerca e sviluppo*, favorendo l'osmosi con il mondo industriale, accademico e della ricerca per l'avvio di progetti e *partnership* pubblico-private in cybersicurezza, mediante l'*accesso a finanziamenti nazionali ed europei*. In questo senso, risultano fondamentali le *sinergie con i Centri di competenza ad alta specializzazione e i Digital Innovation Hub (DIH) attivi sul territorio nazionale*" (Strategia, p. 23).

La seconda misura è lo **sviluppo di tecnologia nazionale ed europea**, "così da ridurre la dipendenza da tecnologie extra-UE, attraverso l'avvio di dedicate progettualità che saranno realizzate – grazie a specifici stanziamenti utilizzando sia fondi nazionali che europei – nell'ambito di un "parco nazionale della cybersicurezza" destinato, a tendere, ad

---

[56] Simili iniziative di cooperazione continueranno ad essere sviluppate sinergicamente dai soggetti interessati, nell'ambito del coordinamento operato dall'ACN e nel rispetto degli indirizzi del Presidente del Consiglio dei ministri, dell'Autorità delegata e del CIC, con il fine di contribuire al continuo innalzamento dei livelli di sicurezza del Paese.

[57] Per ciascuna misura, la Strategia individua gli attori coinvolti, distinguendo fra soggetti responsabili dell'implementazione e altri soggetti a vario titolo interessati (Strategia, pp. 23-24), mentre il Piano di implementazione individua una o più misure specifiche da porre in essere per il suo conseguimento (Misure ##46-58, Piano di implementazione, pp. 13-16).

inglobare i *Cluster* tecnologici che svolgono attività in materia. Tale tecnologia consentirà di sviluppare un'industria nazionale ed europea competitiva, anche attraverso una specializzazione virtuosa di *startup* e PMI innovative, in grado di fornire tecnologie e servizi abilitanti ad elevato grado di sicurezza, con particolare riguardo alle infrastrutture critiche digitali" (*ibidem*).

Come terza misura è prevista la realizzazione di un "**parco nazionale della cybersicurezza**" che, "mettendo a sistema competenze e risorse provenienti dalla PA, dall'industria e dal mondo accademico e della ricerca, fornisca tutte le infrastrutture tecnologiche necessarie allo svolgimento di attività di ricerca e sviluppo nell'ambito della *cybersecurity* e delle tecnologie digitali quali, a titolo di esempio, l'AI, il *quantum computing & cryptography* e la robotica. Con la sua creazione si intende conseguire nel tempo una maggiore autonomia strategica nazionale sulle tecnologie *cyber*, sostenendo lo sviluppo e la produzione di *software* e *hardware* nazionali da impiegare nelle reti e nei sistemi di maggiore rilevanza strategica. Il parco è concepito come un incubatore di capacità e tecnologie, al cui interno giovani talenti e *startup* possano entrare in contatto con le grandi aziende e con le diverse realtà nazionali che, a vario titolo, operano nel settore. Per tale motivo, il parco deve poter disporre di una struttura "diffusa" nella quale, accanto ad un "*hub*" centrale, sussistono ramificazioni distribuite sull'intero territorio nazionale" (*ibidem*).

La quarta misura è "l'introduzione di nuovi meccanismi e soluzioni incentivanti per continuare a supportare lo **sviluppo industriale, tecnologico e della ricerca**, con particolare riferimento allo sviluppo di competenze e al trasferimento tecnologico (specie nei settori avanzati della cybersicurezza). Ciò, anche con l'obiettivo di: continuare a favorire la competitività del sistema produttivo del Paese, sostenendo le imprese nella loro transizione digitale ed ecologica, agevolandone l'internazionalizzazione e l'attrazione di investimenti; realizzare prodotti e servizi ICT ad alta affidabilità, anche incoraggiando la creazione di *Product Security Incident Response Team* (PSIRT) da parte degli operatori privati, per accrescere le loro capacità di gestire le vulnerabilità di prodotti ICT" (Strategia, pp. 23-24).

Infine, la quinta misura consiste nel "continuo impulso all'innovazione tecnologica e alla digitalizzazione della PA e del tessuto produttivo del Paese, assicurando una costante rispondenza ai principi di cybersicurezza e facendo ricorso alle risorse messe a disposizione dal PNRR. Ciò va di pari passo con la promozione di iniziative volte a rafforzare l'autonomia industriale e tecnologica dell'Italia".

È evidente che si tratta di misure tutte atte a "sviluppare la Sovranità Tecnologica della nazione in funzione del perseguimento del massimo livello possibile di Autonomia

Strategica", per la cui implementazione la presente ricerca mira a fornire un quadro metodologico.

7. La cooperazione internazionale come "fattore abilitante" secondo la Strategia

Ultimo tassello della nuova architettura *cyber* – rilevante, però, come ormai più volte rilevato per la Sovranità Tecnologica in generale e, quindi, per l'Autonomia Strategica nazionale – è la cooperazione internazionale, dei cui principali ambiti ci siamo occupati nel Capitolo II.

Secondo la Strategia Nazionale di Cybersicurezza, uno dei "fattori abilitanti" per poter realizzare fattivamente gli obiettivi ivi descritti[58], fra cui l'Obiettivo Sviluppo descritto nel paragrafo precedente, è la cooperazione sia sul fronte nazionale (di cui si è già detto *supra*, paragrafo 4) che in ambito internazionale. Riguardo a quest'ultima, la Strategia mira ad incrementare la partecipazione proattiva dell'Italia alle iniziative europee e internazionali e promuovere collaborazioni bilaterali.

"A livello internazionale, l'Italia collabora nella promozione del rispetto dei diritti umani, delle libertà fondamentali e dei valori democratici nel dominio *cyber*, per far sì che questo rimanga uno spazio globale, aperto, stabile e sicuro, in cui il diritto internazionale ed i principi condivisi siano rispettati. A tal fine, il nostro Paese partecipa alle principali iniziative di cooperazione, di *cyber diplomacy* e di *capacity building* nei confronti di Paesi *partner* che stanno sperimentando un rapido sviluppo digitale. Ciò, anche attraverso l'implementazione di *Confidence Building Measure* (CBM) dell'OSCE[59], al fine di evitare l'emergere di tensioni a livello politico-militare derivanti dall'impiego delle tecnologie ICT. Inoltre, l'Italia condivide le metodologie e gli strumenti di deterrenza e risposta ad attacchi cibernetici definiti a livello UE e NATO. In tale contesto, la partecipazione alle iniziative internazionali e la prosecuzione dei dialoghi e delle relazioni con i Paesi di interesse, sono elementi indispensabili per rafforzare ulteriormente il posizionamento dell'Italia, per favorire lo scambio di conoscenze e per promuovere l'internazionalizzazione delle imprese nazionali attive nel settore" (Strategia, p. 26).

Il Piano di Implementazione individua quindi otto misure specifiche per incrementare la cooperazione, di cui sette relative alla cooperazione internazionale[60]. Si tratta delle misure #75-81 che consistono nel: "Rafforzare il ruolo dell'Italia all'interno dei consessi multilaterali

---

58 La Strategia individua tre "fattori abilitanti": Formazione, Promozione della cultura della sicurezza cibernetica e Cooperazione; e trasversalmente ad essi e agli obiettivi di protezione, risposta e sviluppo: la *Partnership* Pubblico-Privato (su quest'ultima si veda *supra*, paragrafo 5) (p. 24-26).

59 *Supra*, Capitolo 2, paragrafo 5.

60 Sulla cooperazione a livello nazionale – cui è dedicata la misura #74 – si veda *supra*, nota 52.

impegnati in ambito di sicurezza cibernetica (quali UE, NATO, G7, OSCE e Consiglio d'Europa) e il posizionamento strategico nazionale in Europa e nel mondo, promuovendo sinergie con i Paesi "*like-minded*" (Misura #75); Assicurare l'implementazione delle CBM dell'OSCE in materia di sicurezza cibernetica (Misura #76); Rafforzare la cooperazione con altri Paesi, per contribuire alla stabilità e alla sicurezza dello spazio cibernetico (Misura #77); Realizzare un ecosistema nazionale volto a sviluppare capacità di *capacity building* a favore di Paesi terzi (Misura #78); Stipulare accordi bilaterali e multilaterali con i Paesi di interesse strategico, prevedendo anche lo sviluppo di attività di *capacity building* (Misura #79); Contribuire attivamente, in ambito UE, alla definizione di *policy*/regolamentazioni in materia di cybersicurezza (Misura #80) e infine: Contribuire attivamente, in ambito UE, all'individuazione delle priorità di ricerca e sviluppo per traguardare l'obiettivo dell'autonomia tecnologica UE in ambito digitale (Misura #81) (Piano di implementazione, pp. 20-21).

Confrontate con il quadro degli impegni assunti o da assumere da parte dell'Italia, delineato nel Capitolo II, queste misure appiano, da un lato, non sufficientemente comprensive – nessuna azione di coordinamento è prevista, ad esempio, per quanto riguarda la partecipazione italiana in sede OECD; dall'altro, esse rimangono allo stato di mere enunciazioni, senza indicare – con l'eccezione della implementazione delle CBM – i passi concreti da intraprendere.

Complessivamente, comunque, sia gli obietti, in particolare l'Obiettivo Sviluppo, che le misure previste per la sua realizzazione nella Strategia nazionale per la cybersicurezza e nel relativo Piano di implementazione, sono in linea con lo sviluppo della Sovranità Tecnologica e conseguente Autonomia Strategica alla cui realizzazione la presente ricerca mira a contribuire.

Occorre dunque ora trarre le conclusioni delle considerazioni fin qui svolte, dopo averle ricapitolate nelle parti essenziali.

Conclusioni

Come si è ricordato *in incipit*[61]*,* scopo della ricerca è: "Fornire un quadro metodologico per l'implementazione di provvedimenti atti a sviluppare la Sovranità Tecnologica della nazione in funzione del perseguimento (…) di Autonomia Strategica" – la cui importanza è solo cresciuta a seguito della pandemia da COVID-19 e lo scoppio e il perdurare del conflitto russo-ucraino ad oltre sei mesi dal suo inizio[62].

Sviluppare la Sovranità Tecnologica significa sia acquisire, sviluppare e rafforzare le capacità nazionali, sia costruire e mantenere nel tempo *partnership* "affidabili" (da intendersi queste ultime, nel senso ampio di cui si è detto)[63].

Dato che ogni dipendenza può essere sfruttata come arma, l'interesse dell'Italia non è solo quello di ridurre le dipendenze esistenti, ma anche di prevenire l'insorgere di nuove. È quindi urgente non solo ridurre le dipendenze, ma anche mantenere e magari aumentare la propria **competitività** e, quindi le proprie quote di mercato, nei settori strategici per evitare future esposizioni.

Al pari di altre questioni politiche trasversali come la parità di genere, la crescita verde o lo sviluppo sostenibile, le politiche di Trasformazione Digitale sono rilevanti in molti ambiti[64]. Il che richiede un **approccio olistico e coordinato** alla definizione, implementazione e monitoraggio delle relative politiche.

La recente riforma, introdotta con il decreto-legge 14 giugno 2021 n. 82[65], che ha disegnato la nuova architettura nazionale *cyber*, risponde all'esigenza di riordinare, razionalizzare e semplificare le competenze nazionali in materia di sicurezza cibernetica (prima frammentate e poste in capo a una pluralità di attori istituzionali), creando un ente centrale – l'**Agenzia per la Cybersicurezza Nazionale (ACN)**[66]**,** con competenza in materia, che possa anche rappresentare il punto di raccordo tra i diversi soggetti interessati ai vari livelli: il *livello politico*, rappresentato dal Presidente del Consiglio dei ministri, dall'Autorità delegata per la sicurezza della Repubblica e dal CISR[67]; il *livello operativo*, costituito dal NCS, supportato dall'ACN in raccordo con le strutture competenti delle

---

61 Capitolo I, paragrafo 1.
62 Capitolo I, paragrafo 5.
63 Capitolo I, paragrafo 2.
64 Capitolo I, paragrafo 3.
65 Il decreto-legge 14 giugno 2021, n. 82, recante Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, è stato convertito, con modificazioni, dalla legge 4 agosto 2021 n. 109.
66 Capitolo IV, paragrafo 3.
67 Capitolo IV, paragrafo 2.

Amministrazioni NCS e il *livello tecnico*, realizzato dallo CSIRT Italia, in raccordo con le altre articolazioni tecniche delle Amministrazioni NCS[68].

A seguito della propria istituzione, l'ACN ha adottato per la prima volta la **Strategia nazionale di cybersicurezza** e il relativo **Piano di implementazione 2022-2026** – entrambi resi pubblici il 25 maggio 2022.

La Strategia individua quale uno degli obiettivi fondamentali da perseguire "lo sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato" (Strategia, p. 22). Si tratta di un obiettivo che va *oltre l'ambito specifico della cybersicurezza* per abbracciare l'intero dominio della Transizione Digitale e che pertanto potrebbe essere utilmente ridenominato "**Obiettivo Sviluppo per la Sovranità Tecnologica**". Le cinque misure considerate fondamentali per la sua realizzazione[69], che si aggiungono agli strumenti finanziari e ai programmi di investimento già avviati negli ultimi anni (in particolare, quelli previsti dalle leggi di bilancio e dal PNRR)[70], paiono tutte idonee a contribuire al perseguimento dell'Autonomia Strategica nazionale.

Ha un senso dunque capitalizzare sulla recente riforma dell'architettura nazionale *cyber*, che ha istituito l'ACN, al fine di massimizzare l'impatto dello **sforzo non solo legislativo, ma soprattutto organizzativo e finanziario**, nonché delle **competenze ed esperienze** che di esso rappresentano il naturale prodotto e fanno dell'ACN una struttura di eccellenza e *asset* per Sistema-Paese.

Le *funzioni* attribuite all'ACN "esprimono un approccio olistico" alla gestione della cybersicurezza (come efficacemente messo in luce nel Piano di implementazione, p. 27), ma anche, più in generale, allo sviluppo della Sovranità Tecnologica nazionale.

Inoltre, l'*architettura nazionale* per la gestione degli incidenti e delle crisi di cybersicurezza (che si incardina perfettamente nella piattaforma definita dalla Raccomandazione UE 2017/1584; c.d. *Blueprint*) appare idonea, in linea di principio, a garantire l'unicità istituzionale di indirizzo e di azione resa indispensabile dalla trasversalità dei settori e la pluralità degli attori coinvolti. In proposito, lo stesso Piano di implementazione rileva come "il successo della strategia nazionale potrà essere assicurato soltanto tramite l'azione sinergica di istituzioni, industria, accademia e società civile, il cui rispettivo contributo, attraverso il conseguimento di singole azioni nei rispettivi ambiti, è essenziale per il raggiungimento degli obiettivi generali" (Piano di implementazione, p. 24).

---

[68] Capitolo IV, paragrafo 4, e nota 51.

[69] Tra le quali, ad esempio, la digitalizzazione della PA attraverso la migrazione a tecnologie *Cloud*, siano esse del PSN o del *Public Cloud* (Capitolo IV, paragrafo 6).

[70] Capitolo II, paragrafi 2-6.

Un aspetto problematico, al riguardo, è tuttavia quello della **complessità**, che rimane oltremodo elevata – nonostante le intenzioni dichiarate e lo sforzo di razionalizzazione e semplificazione, che pure in parte è stato realizzato con la riforma attuata attraverso l'adozione del decreto-legge 14 giugno 2021 n. 82. Ciò per la varietà dei ruoli attribuiti all'ACN e la molteplicità dei tavoli (ministeriali, interministeriali e *multi-stakeholder*) con cui la stessa è chiamata a dialogare.

L'altro aspetto dell'attuale architettura, su cui né la riforma né le misure descritte nella Strategia e nel Piano di Implementazione appaiono sufficientemente comprensive e articolate, attiene alla **cooperazione internazionale**[71]**.**

In **assenza di un quadro globale condiviso**[72]**,** anche un Paese a media potenza come l'Italia può contare molto nell'ambito delle organizzazioni e *fora* internazionali di cui fa parte, oltre che naturalmente in seno all'UE.

La **diplomazia italiana**, la cui storia è ricca di successi e riconoscimenti, può svolgere un ruolo propulsivo soprattutto nella direzione della promozione dei valori democratici e di rispetto dei diritti fondamentali, anche al fine del rafforzamento della propria Sovranità Tecnologica.

Inoltre, l'Italia condivide le metodologie e gli strumenti di deterrenza e risposta ad attacchi cibernetici definiti a livello UE e NATO. In tale contesto, la partecipazione alle iniziative internazionali e la prosecuzione dei dialoghi e delle relazioni con i Paesi di interesse, sono elementi indispensabili per rafforzare ulteriormente il posizionamento dell'Italia, per favorire lo scambio di conoscenze e per promuovere l'internazionalizzazione delle imprese nazionali attive nel **settore AD&S e altri settori rilevanti**.

In considerazione di questo duplice rilievo, la costituzione di un nuovo Comitato interministeriale potrebbe utilmente contribuire – operando in stretto contatto con l'ACN – al rafforzamento delle capacità nazionali e all'unicità di indirizzo e di azione sul piano internazionale ed europeo, ai fini dell'Autonomia Strategica nazionale. Di tale Comitato si auspica la costituzione in una composizione più snella e fluida possibile, e la collocazione preferibilmente presso il Segretariato generale del Min. Difesa sia per la sua centralità come organismo istituzionale collettore di informazioni e punto di riferimento per il settore AD&S (della cui importanza per lo sviluppo della Sovranità Tecnologica si è detto)[73], che per la sua rilevanza in molte organizzazioni internazionali di cui l'Italia fa parte (NATO, UE *et al.*).

---

71 Capitolo IV, paragrafo 7.
72 Capitolo II, paragrafo 1.
73 Capitolo I, paragrafo 3.

Acronimi

AD&S	Aerospazio, Difesa e Sicurezza
ENISA	Agenzia dell'Unione Europea per la Cybersicurezza
ACN	Agenzia per la Cybersicurezza Nazionale
ASEAN	Associazione delle Nazioni del Sud-Est Asiatico
BBF	Bello e Ben Fatto
CVCN	Centro di Valutazione e Certificazione Nazionale
CIC	Comitato Interministeriale per la Cybersicurezza
CISR	Comitato Interministeriale per la Sicurezza della Repubblica
CSIRT	Computer Security Incident Response Team
CBM	Confidence Building Measure
CyCLONe	Cyber Crisis Liaison Organization Network
DEPA	New Digital Economy Partnership Agreement
DTD	Dipartimento per la Trasformazione Digitale
EDT	Emerging and Disruptive Technologies
HPC	High Performance Computing
ICT	Information and Communications Technologies
ICE	Infrastrutture Critiche Europee
AI	Intelligenza Artificiale
IoT	Internet of Things
MAECI	Ministero degli Affari Esteri e della Cooperazione Internazionale
Min.	Difesa Ministero della Difesa
MEF	Ministero dell'Economia e delle Finanze
MISE	Ministero dello Sviluppo Economico
MUR	Ministero dell'Università e della Ricerca
MITD	Ministero per l'Innovazione Tecnologica e la Transizione Digitale
NCC	National Coordination Centre
NIS	Network and Information Security
NCCs	Network of National Coordination Centres
NATO	North Atlantic Treaty Organization
NCS	Nucleo per la Cybersicurezza
NGEU	Next Generation EU
OMC	Organizzazione Mondiale del Commercio
OMS	Organizzazione mondiale della sanità

OSCE	Organizzazione per la Sicurezza e la Cooperazione in Europea
OECD	Organizzazione per la cooperazione e lo sviluppo economico
PPP	Partnership Pubblico-Privato
PSNC	Perimetro di sicurezza nazionale cibernetica
PNRR	Piano Nazionale di Ripresa e Resilienza
PMI	Piccole e medie imprese
PSN	Polo Strategico Nazionale
PCM	Presidenza del Consiglio dei Ministri
PIL	Prodotto Interno Lordo
PA	Pubblica Amministrazione
PoC NIS	Punto di contatto unico NIS
GDPR	Regolamento Generale sulla Protezione dei Dati
RRF	Recovery and Resilience Facility
SOC	Security Operation Center
SMD	Stato Maggiore della Difesa
UE	Unione europea
UN	United Nations

Bibliografia

- Autolitano S., Pawlowska A. (2021). Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study, *IAI papers,* 21|14: 1-23.
- Bacchus J. (2021). The Digital Decide How to Agree on WTO rules for digital trade. *Cigion-line.* testo disponibile al sito: https://www.cigionline.org/static/documents/TheDigitalDecide-Bacchus.pdf. Data di consultazione 07/09/2022.
- Basu A. (2021). Can the WTO build consensus on digital trade?. *Hinrich foundation advancing.* testo disponibile al sito: https://www.hinrichfoundation.com/research/article/wto/can-the-wto-build-consensus-on-digital-trade/. Data di consultazione 07/09/2022.
- Bendiek A., Stürzer I. (2022). Advancing European Internal and External Digital Sovereignty, The Brussels Effect and the EU-US Trade and Technology Council, *SWP comments,* 20: 1-8.
- Bernabè F. (2021). La sfida della tecnologia tra Stati Uniti ed Europa. *Aspenia on-line*. testo disponibile al sito: https://aspeniaonline.it/la-sfida-della-tecnologia-tra-stati-uniti-ed-europa/. Data di consultazione 07/09/2022.
- Bilotta N. (2020). Beyound the Digital Tax: The Challenges of the EU's Scramble for Technological Sovereignty, *IAI papers,* 20|14: 1-20.
- Burwell F. G., Propp K. (2020). The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?, *Atlantic Council issue brief.* testo disponibile al sito: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/. Data di consultazione 07/09/2022.
- Caravella S., Costantini V., Crespi F. (2021). Mission-Oriented Policies and Technological Sovereignty: The Case of Climate Mitigation Technologies, *Energies,* 14: 6854-6870.
- Celeste E. (2020). Digital Sovereignty in the EU: Challenges and Future Perspectives. In: Fabbrini F., Celeste E. e Quinn J. Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty. Oxford: Hart Publishing.
- Cerra R. e Crespi F., a cura di (2021). *Sovranità Tecnologica. Elementi per una strategia Italiana ed Europea.* Roma: Centro Economia Digitale. testo disponibile al sito: https://www.centroeconomiadigitale.com/. Data di consultazione 07/09/2022.

- Coletti G., Panico G., Catapano C. (2018). Prodotti Made in Italy: più tutela sul web. *Authentico-ita.org.* testo disponibile al sito: https://www.authentico-ita.org/prodotti-made-in-italy-tutela-web/. Data di consultazione 07/09/2022.
- Coletti G., Panico G., Catapano C. (2022). Spaghettitaliani: "Solania presenta il primo pomodoro San Marzano Dop certificato in Blockchain". *Authentico-ita.org.* testo disponibile al sito: https://www.authentico-ita.org/spaghettitaliani-solania-presenta-il-primo-pomodoro-san-marzano-dop-certificato-in-blockchain/. Data di consultazione 07/09/2022
- Cory N., Dascoli L. (2021). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. *Information Technology & Innovative Foundation.* testo disponibile al sito: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/. Data di consultazione 07/09/2022.
- Credi O., Viviani C. (2021). Spazio e sovranità digitale europea, *IAI papers*, 21|11: 1-11.
- Crespi F., Caravella S., Meneghini M., Salvatori C. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy, *Inter economics,* 56: 348-354.
- Curioni A. (2022). Tessere senza chip/ Un altro colpo alla perduta sovranità tecnologica dell'Italia. *Il Sussidiario.net*. testo disponibile al sito: https://www.ilsussidiario.net/news/tessere-senza-chip-un-altro-colpo-alla-perduta-sovranita-tecnologica-dellitalia/2399933/. Data di consultazione 07/09/2022.
- Darnis J. P. (2020). A COVID-19 Moment for Technological Sovereignty in Europe?, *IAI commentaries,* 20|29: 1-6.
- Darnis J. P. (2021). L'unione Europea tra autonomia strategica e sovranità tecnologica: problemi e opportunità, *IAI papers*, 21|19: 1-25.
- Fasulo F. (2022). The EU, US and Asia. Economy as a Weapon?, *ISPI Policy Paper*, 1-46. testo disponibile sul sito: https://www.ispionline.it/it/pubblicazione/eu-us-and-asia-economy-weapon-35893. Data di consultazione 07/09/2022.
- Fay R. (2021). Can Regulation Keep Up With The Pace of Innovation?. *Ispi on-line.* testo disponibile al sito: https://www.ispionline.it/it/pubblicazione/can-regulation-keep-pace-innovation-30261. Data di consultazione 07/09/2022.
- Ferrari P. (2021). Sovranità tecnologica: cos'è e perché è importante?. *Money.it.* testo disponibile al sito: https://www.money.it/Sovranita-tecnologica-cos-e. Data di consultazione 07/09/2022.

- Floridi L. (2019). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, *Philosophy & Technology,* 33: 369–378.
- Görlich D. (2021). How Does the Digital Transformation Change Global Value Chains?. *Ispi on-line*. testo disponibile al sito: https://www.ispionline.it/it/pubblicazione/how-does-digital-transformation-change-global-value-chains-30272. Data di consultazione 07/09/2022.
- Ghiretti F. (2020). Europe's Manouvering on the 5G Technology: The Case of Italy, *IAI commentaries,* 20|67: 1-6.
- Ghiretti F. (2021). Technological Competition: Can the EU compete with China?, *IAI papers,* 21|15: 1-18.
- Gierten D., Lesher M. (2022), Assessing national digital strategies and their governance, *OECD Digital Economy Papers*, 324: 1-29. testo disponible al sito: https://doi.org/10.1787/baffceca-en. Data di consultazione 10/09/2022
- Guidi A. (2022). EU and US: Cyber Friends or Digital Foes?. *Ispi on-line*. testo disponibile al sito: https://www.ispionline.it/it/pubblicazione/eu-and-us-cyber-friends-or-digital-foes-35466. Data di consultazione 08/09/2022.
- Hold A., Wunsch-Vincent S. (2011). Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral versus Preferential Trade Negotiations*. World Trade Institute*. 251: 1- 33
- Iossa E., Madio L. (2021). Piattaforme e regole, la rincorsa continua. *Lavoce.info.* testo disponibile al sito: https://www.lavoce.info/archives/90439/piattaforme-e-regole-la-rincorsa-continua/. Data di consultazione 07/09/2022.
- Kalomeni K. (2018). Digital Regulations and the Risk of a Securitized Internet, *IAI commentaries,* 18|66: 1-6.
- Nisticò F. (2022). L'elemento cyber nella guerra russo-ucraina. *Aspenia on-line*. testo disponibile al sito: https://aspeniaonline.it/lelemento-cyber-nella-guerra-russo-ucraina/. Data di consultazione 07/09/2022.
- Pagnanelli V. (2021). Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali, *Rivista italiana di informatica e diritto,* 3(1): 11-26.
- Pergamo R. (2021). La Caccia alle frodi al made in Itali corre anche sulle piattaforme dell'e-commerce. *Agrifoodtoday.* testo disponibile al sito: https://www.agrifoodtoday.it/blog/agralimenta/la-caccia-alle-frodi-al-made-in-italy-corre-anche-sulle-piattaforme-dell-e-commerce.html. Data di consultazione 07/09/2022.

- Polito C. (2021). La governance globale dei dati e la sovranità digitale Europea, *IAI papers,* 21|11: 1-12.
- Polo M. (2020). Big Tech e antitrust, non solo un problema di concorrenza. *Lavoce.info.* testo disponibile al sito: https://www.lavoce.info/archives/68864/big-tech-non-solo-un-problema-di-concorrenza/. Data di consultazione 07/09/2022.
- Scaccia G. (2017). Il territorio fra sovranità statale e globalizzazione dello spazio economico, *Krytyka Prawa,* 9: 110-152.
- Scopsi M. (2019). The Expansion of Big Data Companies in the Financial Services Industry, and EU Regulation, *IAI papers,* 19|06: 1-15.
- Serri N. (2021). L'Europa in ritardo sull'AI: politica industriale e diritti. *Aspenia,* 94: 246-252.
- Visco I. (2019). Stabilità e sviluppo in un'economia globale, *Moneta e credito,* 72: 3-13.

Webgrafia

- Agenzia per la Cybersicurezza Nazionale, Strategia Nazionale di Cybersicurezza 2022-2026, https://www.acn.gov.it/strategia-nazionale-cybersicurezza. Data di consultazione 06/09/2022.
- Agenzia per la Cybersicurezza Nazionale, Piano di Implementazione Strategia Nazionale di Cybersicurezza 2022-2026, https://www.acn.gov.it/strategia-nazionale-cybersicurezza. Data di consultazione 07/09/2022.
- European Commission, Blockchain Strategy, https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy. Data di consultazione 07/09/2022.
- European Commission, Digital contract rules, https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/digital-contract-rules_en, Data di consultazione 07/09/2022.
- European Union, EU4Digital Initiative, https://eufordigital.eu/discover-eu/the-eu4digital-initiative/. Data di consultazione 07/09/2022.
- European Union, EU Digital Single Market, https://eufordigital.eu/discover-eu/eu-digital-single-market/. Data di consultazione 07/09/2022.
- European Union, The Digital Economy and Society Index (DESI), https://digital-strategy.ec.europa.eu/en/policies/desi. Data di consultazione 07/09/2022.
- European Union, Eastern partnership regulators for electronic communications, https://eapereg.org/. Data di consultazione 07/09/2022.
- Italia digitale 2026, https://innovazione.gov.it/italia-digitale-2026. Data di consultazione 08/09/2022
- National Plan of Recovery and Resilience, https://italiadomani.gov.it/en/home.htm. Data di consultazione 08/09/2022
- Nato 2022 Strategic Concept, 290622-strategic-concept.pdf (nato.int), Data di consultazione 07/09/2022.

Nota sull'IRAD e Nota sull'Autore

IRAD[74]

L'Istituto di Ricerca e Analisi della Difesa (IRAD) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito come Centro Militare di Studi Strategici (Ce.Mi.S.S.) nel 1987 e riconfigurato come IRAD nel 2021 a seguito dell'entrata in vigore della Legge 77/2020 - art. 238 bis, l'IRAD svolge la propria opera avvalendosi di esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

Annalisa Ciampi

Annalisa Ciampi è professore ordinario di diritto internazionale presso l'Università di Verona e Avvocato iscritto all'Albo del Consiglio dell'Ordine di Firenze e degli Avvocati Cassazionisti. Le sue aree di *expertise* includono il contenzioso internazionale, il diritto dell'Unione europea e delle organizzazioni internazionali, e i diritti umani.

[74] http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pagine/default.aspx

ISBN 979-12-551-5018-3