ISSN 2384-9169
Fascicolo n. 3 - 2025
rivista.eurojus.it

Le misure di armonizzazione dell'Unione europea in materia di cibersicurezza: profili istituzionali e basi giuridiche[*]

di DAVIDE DIVERIO[**]

SOMMARIO: 1. Introduzione. – 2. *Ratio* e obiettivi del regolamento sulla ciberresilienza. – 3. Il regolamento sulla ciberresilienza quale atto di armonizzazione per l'instaurazione e il funzionamento del mercato interno della libera circolazione delle merci. – 4. Il regolamento sulla cibersolidarietà, un atto di politica industriale dell'Unione. – 5. L'applicazione del regolamento sulla cibersolidarietà fra competenze "comunitarie" e PESC. – 6. Considerazioni conclusive. - 7. Considerazioni conclusive.

1. Introduzione.

Per tentare di affrontare il tema dei profili istituzionali e delle basi giuridiche dell'intervento legislativo di armonizzazione dell'Unione europea in materia di cibersicurezza, pare utile svolgere qualche riflessione a partire da alcuni di questi atti, in particolare due, che compongono tale quadro legislativo europeo. Costituiranno oggetto di attenzione, in particolare, il cosiddetto regolamento sulla ciberresilienza[1] e taluni e specifici profili del più recente regolamento sulla cibersolidarietà[2]; regolamento che, per la verità, non costituisce atto di armonizzazione ma che, nondimeno, assume una

[*] Lo scritto riproduce, con alcune modifiche e integrazioni, la relazione tenuta al Convegno *Attacchi ai sistemi cyber-fisici: prospettive di diritto internazionale e dell'Unione europea*, svoltosi il 20 giugno 2025 presso il Dipartimento di Studi Internazionali, Giuridici e Storico-Politici dell'Università degli Studi di Milano. Il testo è stato rivisto dall'Autore e corredato di note bibliografiche che, tuttavia, data la natura del contributo, sono necessariamente limitate al minimo essenziale.
Il lavoro è in parte sostenuto dal progetto SERICS (PE00000014) nell'ambito del programma NRRP MUR finanziato dal NGEU.
[**] Professore ordinario di Diritto dell'Unione europea presso l'Università statale di Milano.
[1] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza), in *GUUE* L 2847 del 20.11.2024, p. 1 ss.
[2] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà), in *GUUE* L 38 del 15.1.2025, p. 1 ss.

posizione centrale nel quadro dell'intervento dell'Unione, e dei suoi Stati membri, in tema di cibersicurezza. Fatalmente, l'attenzione dedicata al regolamento sulla ciberresilienza implicherà anche qualche limitato rinvio ad altri atti di armonizzazione quali, in particolare, la direttiva cosiddetta NIS 2[3] e il regolamento sull'intelligenza artificiale[4]. Alla luce della specifica prospettiva d'indagine evocata dal titolo del mio intervento, occorre premettere che non costituirà puntuale oggetto d'attenzione il (complicato) quadro normativo di disciplina adottato dal legislatore di diritto derivato dell'Unione.

2. *Ratio* e obiettivi del regolamento sulla ciberresilienza.

Il regolamento sulla ciberresilienza, adottato dal Parlamento europeo e dal Consiglio il 23 ottobre 2024 ma destinato ad applicarsi, ad eccezione di talune disposizioni[5], dall'11 dicembre 2027, colma una evidente lacuna nel quadro legislativo armonizzato in tema di cibersicurezza, disponendo un'armonizzazione minima delle pertinenti disposizioni legislative, amministrative e regolamentari degli Stati membri circa i requisiti di cibersicurezza che i prodotti con elementi digitali debbono soddisfare per poter circolare all'interno dell'Unione.

Adottato sulla base giuridica dell'art. 114 TFUE[6], dunque sul fondamento normativo principale in materia di mercato interno, esso declina, del tutto coerentemente, i propri obiettivi attorno a tre linee direttrici: garantire che i produttori migliorino la sicurezza di tali prodotti, dalle fasi della loro progettazione e del loro sviluppo all'intero loro ciclo di vita, a evidente e ultimo vantaggio per i consumatori; completare e aggiornare il quadro normativo vigente sulla cibersicurrezza, rendendo più agevole l'attività di produttori di hardware e di software; migliorare la trasparenza delle caratteristiche di sicurezza di tali prodotti. Per assicurare tali obiettivi, Parlamento europeo e Consiglio (insieme alla Commissione nel momento della presentazione della proposta di regolamento) hanno ritenuto necessario adottare un atto di armonizzazione di carattere "orizzontale", ovverosia non unicamente dedicato a specifici prodotti ma, appunto, destinato ad applicarsi, in linea generale e, ovviamente, in assenza di atti di armonizzazione già vigenti e specificamente rivolti a taluni prodotti[7], a tutti i «prodotti con elementi

[3] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), in *GUUE* L 333 del 27.12.2022, p. 80 ss.

[4] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828, in *GUUE* L 1689, del 12.7.2024, p. 1 ss.

[5] Ai sensi dell'art. 71, par. 2, l'art. 14 del regolamento («Obblighi di segnalazione dei fabbricanti») si applica a decorrere dall'11 settembre 2026 e il suo capo IV (articoli da 35 a 51, «Notifica degli organismi di valutazione della conformità») dall'11 giugno 2026.

[6] Per tutti, in dottrina, T.M. MOSCHETTA, *Il ravvicinamento delle normative nazionali per il mercato interno*, Bari, 2018.

[7] Il regolamento risulta inapplicabile, ad esempio, ai prodotti con elementi digitali a cui si applicano il regolamento (UE) 2017/745, relativo ai dispositivi medici (in *GUUE* L 117 del 5.5.2017, p. 1 ss.), il regolamento (UE) 2017/746, relativo ai dispositivi medico-diagnostici in vitro (in *GUUE* L 117 del 5.5.2017, p. 176 ss.) e il regolamento (UE) 2019/2144, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli (in *GUUE* L 325 del 16.12.2019, p. 1 ss.), *ex* art. 2, par. 2. Ancora, e sempre a titolo esemplificativo, l'art. 3, par. 3, dichiara fuori dall'ambito di applicazione del regolamento i prodotti con elementi digitali che siano stati certificati in conformità del regolamento (UE) 2018/1139, recante norme comuni nel settore dell'aviazione civile e che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea (in *GUUE* L 212 del 22.8.2018, p. 1 ss.)

digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete»[8].

Tale intenzione emerge inequivoca, in particolare, dal considerando 4, ove, da un lato, sono richiamate tutte le condizioni che, in astratto, legittimano un'armonizzazione da parte del legislatore dell'Unione, dall'altro lato, viene giustificato, all'interno di un contesto normativo già presente, questo ulteriore intervento legislativo, evidenziandone altresì e per tale via il rapporto proprio con tale contesto. Così, è esplicitamente l'incertezza del diritto, sia per i fabbricanti sia per gli utilizzatori dei prodotti, pur in presenza di atti di diritto dell'Unione applicabili a determinati prodotti con elementi digitali, a fondare l'esigenza di adottare un «quadro normativo orizzontale»[9] che possa eliminare, o quanto meno attenuare, i difetti di un «mosaico legislativo all'interno del mercato interno»[10] costituito da vari atti e iniziative finora assunte tanto a livello nazionale quanto a livello dell'Unione. Ricordata una intrinseca dimensione transfrontaliera del fenomeno in discorso, oltremodo ovvia in considerazione del fatto che i prodotti con elementi digitali fabbricati in uno Stato membro o in un Paese terzo sono spesso utilizzati in tutto il mercato interno da organizzazioni e da consumatori, quella richiamata frammentazione normativa non può che tradursi in oneri aggiuntivi, e dunque in veri e propri costi, per le imprese coinvolte nei processi di fabbricazione e di commercializzazione di tali particolari beni (con particolare attenzione, in astratto, alle piccole e medie imprese e alle microimprese) e per chi questi ultimi utilizzi.

Fra gli atti di armonizzazione già adottati, particolarmente enfatizzato è il collegamento con la direttiva NIS 2 che pare porsi come concreto presupposto, in senso lato potrebbe considerarsi una sorta di fondamento stesso, del regolamento sulla ciberresilienza. Se, infatti, tale direttiva mira a garantire un elevato livello di cibersicurezza dei servizi forniti dai soggetti essenziali e importanti da essa individuati, inclusi i fornitori di infrastrutture digitali che garantiscono i servizi Internet e l'accesso a essi, appare essenziale che i prodotti con elementi digitali necessari proprio a tali fornitori per, di fatto, assicurare le funzioni fondamentali dell'Internet «siano sviluppati in modo sicuro e siano conformi a norme di sicurezza Internet consolidate»[11]. Del resto, poi, il regolamento intende anche facilitare il rispetto dei requisiti relativi alla catena di approvvigionamento a norma della direttiva NIS 2 da parte dei fornitori di infrastrutture digitali, garantendo che i prodotti con elementi digitali che essi utilizzano siano sviluppati in modo sicuro e che abbiano accesso ad aggiornamenti di sicurezza tempestivi per tali prodotti.

Le condizioni per l'utilizzo dell'art. 114 TFUE sono senz'altro presenti e ben evidenziate dal legislatore di diritto derivato dell'Unione. Come noto, e per quanto qui più rileva, infatti, i primi considerando del regolamento sulla ciberresilienza rendono evidente di trovarsi al cospetto di un atto di armonizzazione che trae origine da un complesso normativo, tanto a livello dell'Unione quanto a livello dei singoli Stati membri, troppo frammentato e disomogeneo e, *per se*, costitutivo perciò di un ostacolo per la realizzazione degli obiettivi dell'art. 26 TFUE, ovverosia l'instaurazione e il funzionamento di un mercato interno che comporti uno spazio senza frontiere interne, fra gli Stati così come all'interno di essi, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali.

Significativo, in proposito, è il rinvio, fra gli altri atti[12], alla Comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del

---

[8] Così, l'art. 2, par. 1, del regolamento. Per «prodotto con elementi digitali», poi, l'art. 3, n. 1, afferma debba intendersi «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente».

[9] Regolamento sulla ciberresilienza, cit., considerando 4.

[10] *Ibidem*.

[11] Regolamento sulla ciberresilienza, cit., considerando 24.

[12] Anche la relazione finale della Conferenza sul futuro dell'Europa è espressamente richiamata dal legislatore del regolamento in parola al considerando 7.

20 giugno 2023, dedicata alla «Strategia europea per la sicurezza economica»[13]. Il considerando 58, infatti, mette in diretta correlazione l'introduzione di requisiti specifici in materia di cibersicurezza per i prodotti digitali o connessi e il generale obiettivo dell'approfondimento del mercato unico. Quest'ultimo, in una prospettiva ben più ampia della mera circolazione dei fattori produttivi, viene in effetti presentato come il precipitato (anche) di ulteriori realizzazioni concrete quali, ad esempio, la promozione della resilienza dell'economia europea e delle catene di approvvigionamento, il rafforzamento dell'innovazione e della capacità industriale; il tutto, tuttavia, in un contesto che, ai sensi dell'art. 3, par. 3, TUE, miri pur sempre a preservare l'economia sociale di mercato.

Rilevante appare sottolineare come sia appunto la nozione di «sicurezza economica» a costituire un interessante, e forse inedito, *trait d'union* fra il profilo più concreto e, per così dire, settoriale, qui appunto rappresentato dall'introduzione di requisiti essenziali per i prodotti con elementi digitali, e il generale obiettivo dell'instaurazione e del funzionamento del mercato interno. Non è, cioè, o non è più, la realizzazione di un semplice mercato interno, ma fondamentale è la ricerca dell'instaurazione di un mercato interno che non può prescindere dalle ricordate ulteriori realizzazioni concrete e che, in definitiva, conduce al cuore della disciplina armonizzata, alle scelte, necessariamente non neutre, del legislatore dell'Unione perché ispirate a logiche plurivaloriali operate dal legislatore dell'Unione. Il ragionamento ricavabile dai considerando del regolamento è, in merito, stringente e chiarissimo. Il punto di partenza è rappresentato dalla qualificazione degli attacchi informatici come «questione di interesse pubblico»[14]. Così sono definiti, e questo è il profilo essenziale, in virtù dell'impatto determinante che essi producono, in un chiaro *climax*, «non solo sull'economia dell'Unione, ma anche sulla democrazia, nonché sulla sicurezza dei consumatori e sulla salute»[15].

Si tratta, del resto, del medesimo approccio utilizzato da Parlamento europeo e Consiglio per l'adozione della direttiva NIS 2, anch'essa fondata sull'art. 114 TFUE. I colegislatori dell'Unione muovono dalla duplice constatazione, da un lato, delle disparità esistenti (talvolta dei veri e propri conflitti), nelle legislazioni degli Stati membri, circa gli obblighi di cibersicurezza imposti agli operatori che forniscono servizi o svolgono attività economicamente rilevanti in rete (con l'evidente conseguenza di produrre difficoltà e costi aggiuntivi per tali soggetti), dall'altro lato, dell'effetto negativo che un incidente informatico può provocare al corretto funzionamento del mercato interno. Sotto quest'ultimo profilo, in particolare, l'accento viene espressamente posto sulla circostanza per cui tale mal funzionamento del mercato interno possa concretamente tradursi in perdite finanziarie, nella determinazione di un *vulnus* nella fiducia degli utenti e di un grave danno all'economia e alla società dell'Unione[16].

Ancor più esplicitamente, e in quella medesima logica di *escalation* appena evocata, il considerando 70 della direttiva NIS 2 ben esemplifica la strumentalità, per dir così, del mercato interno rispetto a obiettivi (soltanto) a prima vista a esso estranei. Sicurezza dell'Unione e protezione dei suoi cittadini (ma pure delle sue imprese e delle sue istituzioni) da incidenti e minacce informatiche assumono, allora, una posizione di primo piano fra le "preoccupazioni" del legislatore di diritto derivato dell'Unione che, con tale direttiva, intende dettare norme minime di armonizzazione per assicurare la disponibilità di sistemi informatici e di rete ciberresilienti, oltre che la disponibilità, la riservatezza e l'integrità dei dati. Obiettivo ultimo è, dunque, sì la creazione di un ciberspazio aperto, libero e sicuro

[13] Comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo, al Consiglio europeo e al Consiglio sulla «strategia europea per la sicurezza economica», documento JOIN(2023)20 final.
[14] Regolamento sulla ciberresilienza, cit., considerando 1.
[15] *Ibidem*.
[16] Si vedano, ad esempio, i considerando 3 e 4 della direttiva NIS 2, cit.

ma perché (o, se si vuole, anche perché) «basato sui diritti umani, le libertà fondamentali, la democrazia e lo stato di diritto»[17].

Nello stesso senso è probabilmente ancora più esplicito il regolamento sull'intelligenza artificiale nel cui primo considerando è possibile individuare, contestualmente e in via circolare, innanzitutto il saldo inquadramento dell'atto nella "famiglia" degli atti di armonizzazione adottati per l'instaurazione e il funzionamento del mercato interno – anche il regolamento in parola, del resto, trova nell'art. 114 TFUE la propria principale base giuridica[18] – con l'esplicita menzione del suo scopo, ovverosia «migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale […] nell'Unione»[19]; il richiamo, poi, al necessario rispetto dei valori dell'Unione, al fine di promuovere la diffusione di un'intelligenza artificiale «antropocentrica e affidabile»[20] e assicurando «un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea […], compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente»[21]; infine, il "ritorno" d'attenzione al contesto del mercato interno, con l'affermazione per cui tale regolamento «garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento»[22]. Certamente, l'enfasi qui ancora maggiore e più esplicita rispetto agli atti precedenti, da parte del legislatore di diritto derivato dell'Unione, sulla garanzia dei valori *ex* art. 2 TUE e dei diritti e delle libertà fondamentali sanciti dai Trattati istitutivi così come dalla Carta dei diritti fondamentali è, nella sostanza, imposta dai rilevantissimi rischi che l'uso dell'Intelligenza artificiale può direttamente arrecare a un consistente elenco di interessi pubblici in materia di salute, sicurezza e diritti fondamentali. Da tali premesse deriva, così, l'esigenza di predisporre «un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici»[23], fra i quali, espressamente, sono inclusi «la democrazia, lo Stato di diritto e la protezione dell'ambiente, come riconosciuti e tutelati dal diritto dell'Unione»[24]. Pur in tale ampia prospettiva, il regolamento resta in ogni caso, prima di tutto, un atto di armonizzazione emanato per l'instaurazione e il corretto funzionamento del mercato interno, occupandosi, in definitiva, di una particolare merce di cui vengono disciplinati «l'immissione sul mercato, la messa in servizio e l'uso di determinati sistemi di IA, […] consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi»[25].

---

[17] Direttiva NIS 2, cit., considerando 70.

[18] In questo caso l'art. 114 TFUE non è l'unica disposizione posta a fondamento del regolamento sull'intelligenza artificiale. Esso, infatti, è nell'occasione affiancato dall'art. 16 TFUE, che, come noto, afferma per ogni persona il diritto alla protezione dei dati di carattere personale che la riguardano e il cui par. 2 costituisce base giuridica per l'adozione di «norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e [di] norme relative alla libera circolazione di tali dati».

[19] Regolamento (UE) 2024/1689, cit., considerando 1.

[20] *Ibidem*.

[21] *Ibidem*.

[22] *Ibidem*.

[23] Regolamento (UE) 2024/1689, cit., considerando 8.

[24] *Ibidem*.

[25] *Ibidem*.

3. Il regolamento sulla ciberresilienza quale atto di armonizzazione per l'instaurazione e il funzionamento del mercato interno della libera circolazione delle merci.

Tornando al regolamento sulla ciberresilienza, anche tale atto, in buona sostanza, va inquadrato nell'ambito degli strumenti di armonizzazione minima adottati per la creazione e l'efficace funzionamento del mercato interno, proponendosi esso, come ricordato, l'obiettivo di rendere possibile la libera circolazione di specifiche merci, i prodotti con elementi digitali. Cifra caratteristica e a prima vista del tutto originale del regolamento in parola è rappresentata dal suo approccio orizzontale che, peraltro, se da un lato determina la complessa questione del coordinamento fra tale atto e quelli già in vigore, dall'altro lato sta a confermare la salda collocazione del regolamento fra gli atti di armonizzazione emanati *ex* art. 114 TFUE in tema di libera circolazione delle merci.

Innanzitutto, occorre tuttavia osservare come questo approccio orizzontale, di per sé, non sia certamente novità assoluta nel contesto del mercato interno, come sta a dimostrare, per quanto riferita a una differente libertà economica di circolazione, l'adozione della direttiva relativa ai servizi nel mercato interno[26], certamente direttiva di armonizzazione *sui generis* ma pur sempre idonea a realizzare effettivamente, per taluni aspetti concreti della disciplina dei servizi a livello nazionale, un'evidente armonizzazione puntuale[27].

Circa l'esigenza del (necessario) coordinamento fra differenti atti di armonizzazione già in vigore e il regolamento sulla ciberresilienza, quest'ultimo detta le linee generali per dipanare quella che, rispetto a taluni precedenti regolamenti in particolare, si presenta, invero, come una complessa "matassa" normativa[28]. Così, appare prima di tutto essenziale stabilire che, rispetto al regolamento 2023/988, relativo alla sicurezza generale dei prodotti[29], quest'ultimo sia destinato a trovare applicazione, in luogo del regolamento sulla ciberresilienza, laddove il prodotto con elementi digitali comporti «altri rischi di sicurezza che non sono sempre connessi alla cibersicurezza ma che possono essere la conseguenza di una violazione della sicurezza»[30]. Rispetto al regolamento sull'intelligenza artificiale, se il prodotto con elementi digitali ai sensi di tale regolamento è qualificabile anche come un sistema di IA ad alto rischio, la sua conformità ai requisiti posti dal regolamento sulla ciberresilienza dovrebbe farlo ritenere conforme anche ai requisiti richiesti dal regolamento sull'intelligenza artificiale «nella misura in cui tali requisiti siano contemplati dalla dichiarazione di conformità UE, o da sue parti,

---

[26] Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno (nota anche come «direttiva Bolkestein»), in *GUCE* L 376 del 27 dicembre 2006, p. 36 ss. Nella sconfinata dottrina, pare qui sufficiente il rinvio a C. BARNARD, *Unravelling the Services Directive*, in *Comm. Mark. Law Rev.*, 2008, pp. 323-394; S. D'ACUNTO, *Direttiva servizi (2006/123/CE): genesi, obiettivi e contenuto*, Milano, 2009; A.-C. SIMON, M. FALLON, *La directive «services»: quelle contribution au marché intérieur?*, in *Journal Dr. Eur.*, 2007, pp. 33-43.

[27] Sul punto, e con specifico riferimento agli artt. 14 e 16 della direttiva servizi, si vedano le conclusioni dell'Avvocato generale P. CRUZ VILLALÓN del 10 marzo 2015, nella causa C-593/13, *Rina Services e a.*, ECLI:EU:C:2015:159, punti 22-24.

[28] L'art. 2, par. 5, del regolamento sulla ciberresilienza prevede che «l'applicazione del presente regolamento ai prodotti con elementi digitali contemplati da altre norme dell'Unione, che stabiliscono requisiti che affrontano tutti o alcuni rischi contemplati dai requisiti essenziali di cibersicurezza di cui all'allegato I, può essere limitata o esclusa, qualora: a) tale limitazione o esclusione sia coerente con il quadro normativo generale applicabile a tali prodotti; e b) le norme settoriali conseguano lo stesso livello o un livello maggiore di protezione rispetto a quanto previsto dal presente regolamento».

[29] Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio, in *GUUE* L 135 del 23.5.2023, p. 1 ss.

[30] Regolamento sulla ciberresilienza, cit., considerando 50.

rilasciata a norma del […] regolamento»[31] sulla ciberresilienza. Ancora, i sistemi di IA ad alto rischio di cui al regolamento sull'intelligenza artificiale e che sono anche prodotti con elementi digitali importanti o critici di cui al regolamento sulla ciberresilienza e ai quali si applica la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI del regolamento (UE) sull'intelligenza artificiale dovrebbero essere soggetti alle procedure di valutazione della conformità di cui al regolamento sulla ciberresilienza per quanto riguarda i requisiti essenziali di cibersicurezza stabiliti nello stesso; in tale caso, per tutti gli altri aspetti contemplati dal regolamento sull'intelligenza artificiale, è opportuno applicare le pertinenti disposizioni in materia di valutazione della conformità basata sul controllo interno di cui all'allegato VI di tale regolamento. Rispetto al regolamento 2023/1230, relativo alle macchine[32], i fabbricanti di prodotti compresi nell'ambito di applicazione di tale regolamento che siano tuttavia anche prodotti con elementi digitali ai sensi del regolamento sulla ciberresilienza «dovrebbero rispettare sia i requisiti essenziali di cui [a tale] regolamento sia i requisiti essenziali di cibersicurezza di cui [a tale] regolamento e di tutela della salute di cui al regolamento (UE) 2023/1230»[33]. A parere del legislatore del regolamento sulla ciberresilienza, potrebbe peraltro darsi una sovrapposizione fra i requisiti essenziali di cibersicurezza di cui al regolamento e alcuni requisiti essenziali previsti dal regolamento 2023/1230 e ciò comportare un vantaggio per il fabbricante: la conformità ai requisiti essenziali di cibersicurezza di cui al regolamento sulla ciberresilienza potrebbe infatti rendere più agevole la conformità ai requisiti essenziali che coprono anche taluni rischi di cibersicurezza di cui al regolamento 2023/1230; resta evidentemente in capo al fabbricante stesso dimostrare un tale effetto e, in ogni caso, l'obbligo di seguire le procedure di valutazione della conformità applicabili previste da entrambi tali regolamenti[34].

Come si anticipava, pare di poter ben sostenere che il regolamento sulla ciberresilienza appartenga a pieno titolo al novero degli atti di armonizzazione in tema di libera circolazione delle merci nel mercato interno dell'Unione. Vale la pena soltanto di evidenziare, semmai, la (a prima vista) singolarità della situazione in cui un regolamento che abbia a oggetto specifiche merci dichiari espressamente di trovare il proprio fondamento (anche) in una direttiva, la NIS 2, essenzialmente dedicata alla libera prestazione di servizi quando, di norma, l'ordine è inverso intervenendo prima la liberalizzazione delle merci e poi quella dei servizi. Anche sotto questo profilo occorre, tuttavia, prendere atto di un'ulteriore caratteristica del diritto derivato del mercato interno che, per dir così, si autoalimenta sulla base di atti di armonizzazione che costituiscono, di volta in volta, presupposto per l'adozione di atti successivi. In questo caso, la prima esigenza, concretizzatasi nella direttiva NIS 2 (peraltro, appunto, evoluzione essa stessa di un atto di armonizzazione già presente), è stata quella di dedicarsi alla messa in sicurezza dei sistemi informatici e di rete in quanto spazio nel quale, sempre più,

---

[31] Regolamento sulla ciberresilienza, cit., considerando 51.

[32] Regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio, del 14 giugno 2023, relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio, in *GUUE* L 165 del 29.6.2023, p. 1 ss.

[33] Regolamento sulla ciberresilienza, cit., considerando 53.

[34] Fra le altre fonti di diritto derivato di armonizzazione per l'instaurazione e il funzionamento del mercato interno, con le quali il regolamento sulla ciberresilienza è tenuto a coordinarsi, si segnala anche la direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio, in *GUUE* L 2024/2853, del 18.11.2024, p. 1 ss. Il considerando 31 del regolamento in parola stabilisce un rapporto di complementarità fra esso e tale direttiva. Quest'ultima afferma, in via generale, che il fabbricante di un prodotto è responsabile dei danni causati da una mancanza di sicurezza nel suo prodotto indipendentemente dalla colpa, prefigurando così un regime di responsabilità oggettiva. Se tale mancanza di sicurezza consiste nell'assenza di aggiornamenti di sicurezza dopo l'immissione sul mercato del prodotto e ciò causa un danno, questo potrebbe far scattare la responsabilità del fabbricante. A stabilire quali siano gli obblighi dei fabbricanti relativi alla fornitura di tali aggiornamenti di sicurezza è, appunto, il regolamento sulla ciberresilienza.

vengono forniti servizi di rilevanza economica ai sensi del TFUE; su tale base, dunque, si è poi provveduto a individuare, dettando per esse una disciplina armonizzata, quelle specifiche merci che, come sottolineato, i fornitori di infrastrutture digitali che garantiscono i servizi Internet e l'accesso a essi utilizzano quotidianamente.

I rinvii che, numerosi, il regolamento sulla ciberresilienza fa a molti atti di armonizzazione già adottati e costituenti il vero e proprio cuore della disciplina dell'Unione in tema di libera circolazione delle merci, poi, costituiscono ulteriore conferma di tale inquadramento. Al di là degli esempi già riportati, con riferimento alla necessità di coordinare gli ambiti di applicazione di tali differenti atti, pare significativo ricordare il rinvio alle discipline previste dal regolamento n. 765/2008[35] e dal regolamento n. 1025/2012[36]. Rispetto al primo regolamento, in particolare, l'art. 29 del regolamento sulla ciberresilienza afferma infatti che «la marcatura CE è soggetta ai principi generali stabiliti all'articolo 30 del regolamento (CE) n. 765/2008». Si tratta, pare importante ricordarlo, di rinvii attuati non soltanto rispetto a prodotti, quali ad esempio i sistemi di IA ad alto rischio, che, di per sé e pacificamente, possono presentare tratti comuni ai prodotti con elementi digitali di cui al regolamento sulla ciberresilienza, ma pure a più generici «prodotti di consumo» *ex* art. 1, par. 2, del regolamento n. 2023/988 o alle «macchine» di cui alla direttiva 2006/42/CE e al regolamento n. 2023/1230.

Del resto, tale regolamento offre, inequivoco in merito, disciplina e struttura in larghissima parte sovrapponibili a quelle dei consueti atti di armonizzazione in tema di libera circolazione delle merci; disciplina e struttura che, in estrema sintesi, possono essere ricondotti a un unico schema che si articola attorno ad alcuni imprescindibili elementi.

Il primo è costituito dall'armonizzazione minima fissata dall'atto di diritto derivato dell'Unione che impone i requisiti essenziali che la merce deve soddisfare. Certamente, in proposito, non è priva di rilevanti conseguenze la scelta di adottare una direttiva ovvero un regolamento, ponendosi in conflitto due esigenze contrapposte, parimenti essenziali: il rispetto del generale principio di proporzionalità, da un lato, che farebbe preferire la direttiva al regolamento; la piena efficacia della disciplina armonizzata, obiettivo pacificamente meglio raggiungibile ove, al contrario, si possa fare a meno del puntuale e corretto recepimento dell'atto di diritto derivato ad opera degli Stati membri.

Il secondo elemento è quello della previsione di obblighi in capo ai fabbricanti (e, poi, a cascata, agli importatori, laddove si tratti di prodotti con elementi digitali di persone fisiche/giuridiche stabilite al di fuori dell'Unione, e ai distributori) volti a consentire che taluni dei prodotti oggetto del regolamento, quelli con elementi digitali importanti[37], possano liberamente circolare nel mercato interno

---

[35] Regolamento (CE) 765/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) 339/93, in *GUUE* L 218 del 13.8.2008, p. 30 ss.

[36] Regolamento (UE) 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione 1673/2006/CE del Parlamento europeo e del Consiglio, in *GUUE* L 316 del 14.11.2012, p. 12 ss.

[37] Si tratta dei prodotti di cui all'allegato III del regolamento, suddivisi nelle classi I e II, che soddisfino, ai sensi dell'art. 7, par. 2, del regolamento sulla ciberresilienza, almeno uno dei seguenti criteri: « a) il prodotto con elementi digitali svolge principalmente funzioni essenziali per la cibersicurezza di altri prodotti, reti o servizi, tra cui la sicurezza dell'autenticazione e dell'accesso, la prevenzione e il rilevamento delle intrusioni, la sicurezza dei terminali o la protezione della rete; b) il prodotto con elementi digitali svolge una funzione che comporta un rischio significativo di avere effetti negativi in ragione della sua intensità e capacità di perturbare, controllare o danneggiare un gran numero di altri prodotti o la salute, la sicurezza o l'incolumità dei suoi utenti attraverso la manipolazione diretta, come una funzione centrale di sistema, compresi la gestione della rete, il controllo di configurazione, la virtualizzazione o il trattamento dei dati personali». Fra i prodotti inclusi nella classe I si trovano, ad esempio, browser autonomi e incorporati, sistemi di gestione delle password, prodotti con elementi digitali con funzione di rete privata virtuale (VPN), sistemi operativi, router, modem per la connessione a Internet

una volta effettuata una valutazione di loro conformità (e della conformità dei processi messi in atto dal fabbricante) tesa a determinare se siano soddisfatti i requisiti essenziali di cibersicurezza di cui all'allegato I del regolamento.

Il principio generale della libera circolazione dei prodotti con elementi digitali che siano conformi al regolamento, di cui all'art. 4, par. 1, del regolamento, costituisce poi il terzo elemento[38].

Infine, l'atto di armonizzazione in parola presenta una procedura di salvaguardia volta a consentire la possibilità di contestare la conformità dei prodotti con elementi digitali rientranti nell'ambito di applicazione del regolamento. Come previsto all'art. 114, par. 10, TFUE, e come noto, le misure di armonizzazione adottate sul fondamento giuridico dell'art. 114 possono infatti comportare, «nei casi opportuni, una clausola di salvaguardia che autorizza gli Stati membri ad adottare, per uno o più dei motivi di carattere non economico di cui all'articolo 36, misure provvisorie soggette ad una procedura di controllo dell'Unione». L'art. 57 del regolamento sulla ciberresilienza consente così alle autorità di vigilanza del mercato degli Stati membri di chiedere a un operatore economico di adottare tutte le misure del caso (dalla limitazione al divieto) qualora ritenga che un prodotto con elementi digitali (e i processi messi in atto dal fabbricante) presenti «un rischio di cibersicurezza significativo e comporti[no] inoltre un rischio per a) la salute e la sicurezza delle persone; b) la conformità agli obblighi previsti dal diritto dell'Unione o dal diritto nazionale a tutela dei diritti fondamentali; c) la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte di soggetti essenziali del tipo di cui […] alla direttiva 2022/2555; o d) altri aspetti della tutela dell'interesse pubblico». Si tratta di misure provvisorie, da comunicare agli altri Stati membri e alla Commissione, della cui legittimità, soprattutto in termini di effettiva giustificazione, quest'ultima è tenuta a giudicare per confermare oppure no tali misure[39].

---

e switch, prodotti per case intelligenti con funzionalità di sicurezza, tra cui serrature intelligenti, telecamere di sicurezza, sistemi di monitoraggio dei neonati e sistemi di allarme, giocattoli connessi a Internet disciplinati dalla direttiva 2009/48/CE del Parlamento europeo e del Consiglio (1) che presentano funzionalità sociali interattive (in grado ad esempio di parlare o filmare) o di geolocalizzazione. Fra i prodotti di cui alla classe II, ancora a titolo esemplificativo, vi sono firewall, sistemi di rilevamento e prevenzione delle intrusioni, microprocessori a prova di manomissione, microcontrollori a prova di manomissione.

Per i cosiddetti «prodotti con elementi digitali critici», invece, l'art. 8 del regolamento subordina la loro libera circolazione nel mercato interno all'ottenimento di un certificato europeo di cibersicurezza a un livello di affidabilità almeno «sostanziale» nell'ambito del sistema europeo di certificazione della cibersicurezza ai sensi del cosiddetto regolamento sulla cibersicurezza (regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) 526/2013, in *GUUE* L 151 del 7.6.2019, p. 15 ss.).

[38] L'art. 4 permette agli Stati membri, in via di eccezione, di consentire la presentazione e l'uso di un prodotto con elementi digitali non conforme al regolamento «in occasione di fiere, mostre e dimostrazioni o eventi analoghi […] a condizione che il prodotto presenti un'indicazione visibile che specifichi chiaramente che esso non è conforme al presente regolamento e che non deve essere messo a disposizione sul mercato finché non lo sarà» (art. 4, par. 2). Allo stesso modo, ma con riferimento a un software non finito che sia non conforme al regolamento, l'art. 4, par. 3, prevede che esso possa essere messo a disposizione sul mercato «a condizione che [esso] sia reso disponibile solo per un periodo limitato necessario ai fini di prova e con un'indicazione visibile che specifichi chiaramente che esso non è conforme al presente regolamento e che non sarà disponibile sul mercato per fini diversi dalla prova».

[39] Alla luce della qualificazione del regolamento sulla ciberresilienza fra gli atti di armonizzazione *ex* art. 114 TFUE, è da ritenere che su specifici aspetti della disciplina che esso detta, e l'adozione di misure provvisorie nel quadro della clausola di salvaguardia può ben costituire un esempio particolarmente significativo, rilevanti debbano considerarsi le pronunce della Corte di giustizia dell'Unione pur se riferite a regolamenti o direttive diverse dal regolamento in parola. Rispetto, appunto, alla clausola di salvaguardia e alle criticità che la sua applicazione può comportare, ad esempio con riguardo al *quantum* di discrezionalità di cui goda la Commissione nella valutazione circa la legittimità delle misure provvisoriamente adottate dalle autorità nazionali e, dunque, alla legittimità delle misure di esecuzione da questa assunte, si veda, fra le pronunce più recenti e riferite alla direttiva

Poste tali premesse, appaiono innegabili due (interlocutorie) conclusioni. Da un lato, come si è appena tentato di illustrare, il regolamento sulla cibersolidarietà costituisce a buon diritto un tipico atto di armonizzazione, volto a rendere possibile il raggiungimento degli obiettivi, *ex* art. 26, par. 1, TFUE, dell'instaurazione e del funzionamento del mercato interno, occupandosi di come consentire la libera circolazione di peculiari merci, i prodotti con elementi digitali. Dall'altro lato, per addivenire a tali obiettivi, il legislatore di diritto derivato dell'Unione approva una disciplina esplicitamente improntata alla considerazione e al rispetto di interessi generali anche "altri" rispetto a quelli propriamente collegati al processo di integrazione economica e di fusione dei mercati nazionali. Quanto l'esigenza di assicurare, per il tramite di disposizioni di armonizzazione delle pertinenti disposizioni degli Stati membri, anche i valori della sicurezza e della salute dei consumatori e (addirittura, verrebbe da dire) della democrazia[40] deve ritenersi legittima, ovverosia conforme ai Trattati istitutivi e, in ultima istanza, al principio, di sicuro rango costituzionale, di attribuzione delle competenze?

4. Il regolamento sulla cibersolidarietà, un atto di politica industriale dell'Unione.

Venendo ora a toccare qualche profilo del regolamento sulla cibersolidarietà, mette conto innanzitutto ricordare come esso, già nel titolo, dichiari di mirare a rafforzare la solidarietà e la capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e di risposta agli stessi.

Sebbene non costituisca, come anticipato, un atto di armonizzazione, tale regolamento assume senz'altro un ruolo centrale nel quadro legislativo dell'Unione in tema di cibersicurezza e risulta intimamente connesso agli altri atti che compongono questo complesso intreccio normativo. Fra le sue basi giuridiche figura, infatti, l'art. 173, par. 3, TFUE, disposizione che, da sola, esaurisce il titolo XVII della parte terza del TFUE, dedicato alla politica industriale dell'Unione; ambito, come noto, nel quale l'Unione dispone di una competenza alquanto limitata, potendo soltanto, ai sensi dell'art. 6 TFUE, «svolgere azioni intese a sostenere, coordinare o completare l'azione degli Stati membri»[41]. Coerentemente, tale art. 173, par. 3, TFUE, premesso che l'Unione contribuisce, insieme agli Stati membri, alla realizzazione dell'obiettivo di assicurare la competitività dell'industria dell'Unione attraverso politiche e azioni che essa attua anche ai sensi di altre disposizioni dei Trattati[42], abilita i colegislatori dell'Unione ad adottare, al fine di raggiungere il medesimo obiettivo, misure specifiche «destinate a sostenere le azioni svolte negli Stati membri» e a esclusione di qualsiasi armonizzazione delle loro disposizioni legislative e regolamentari.

Ancora una volta, l'attenzione principale è rivolta all'enorme rilevanza e alle importanti conseguenze di un incidente di cibersicurezza, evidenziate l'assoluta centralità dell'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza da esse «in tutti i settori di attività

2006/42/CE relativa alle macchine, Tribunale UE, 8 settembre 2021, causa T-152/19, *Brunswick Bowling Products c. Commissione*, ECLI:EU:T:2021:539, punto 66 ss.

[40] Si rinvia, ancora, al considerando 1 del regolamento sulla ciberresilienza, cit.

[41] Ulteriore base giuridica è l'art. 322, par. 1, lett. a), TFUE, secondo cui «il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione della Corte dei conti, adottano mediante regolamenti […] le regole finanziarie che stabiliscono in particolare le modalità relative alla formazione e all'esecuzione del bilancio, al rendiconto e alla verifica dei conti».

[42] Vale la pena ricordare come l'art. 173, par. 1, TFUE indirizzi l'azione dell'Unione e degli Stati membri «ad accelerare l'adattamento dell'industria alle trasformazioni strutturali, a promuovere un ambiente favorevole all'iniziativa ed allo sviluppo delle imprese di tutta l'Unione, segnatamente delle piccole e medie imprese, a promuovere un ambiente favorevole alla cooperazione tra imprese, a favorire un migliore sfruttamento del potenziale industriale delle politiche d'innovazione, di ricerca e di sviluppo tecnologico»; tutto ciò in un contesto espressamente individuato come quello di «un sistema di mercati aperti e concorrenziali».

economica e della società, date l'interconnessione e l'interdipendenza crescenti delle pubbliche amministrazioni, delle imprese e dei cittadini degli Stati membri a livello transettoriale e transfrontaliero»[43]. Come per la direttiva NIS 2, si rinviene, dunque, una chiara presa d'atto, l'ennesima dunque, della vulnerabilità del mercato e, più in generale, della stessa società dell'Unione rispetto a tali incidenti e alle gravi minacce che essi arrecano nei confronti del funzionamento delle reti e dei sistemi informativi.

Ora, tuttavia, la prospettiva appare differente. Conformemente alla diversa base giuridica adottata e, dunque, alla collocazione del regolamento in parola nel contesto della politica industriale dell'Unione, a fronte di tali considerazioni la preoccupazione dei colegislatori dell'Unione è quella, appunto, di «rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitale e sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale»[44] e, ancor più specificamente, di evidenziare la necessità di «investire in infrastrutture e servizi e creare capacità per sviluppare competenze in materia di cibersicurezza che permettano di velocizzare il rilevamento delle minacce e degli incidenti informatici e di assicurare una risposta più rapida»[45].

Non si tratta, per la verità, di prese di posizione inedite. In modo del tutto simile, pur nel differente contesto, appena presentato, del regolamento sulla ciberresilienza, Parlamento europeo e Consiglio avevano sottolineato l'estrema rilevanza di disporre, tanto a livello degli Stati membri quanto dell'Unione, di competenze adeguate in materia di cibersicurezza, richiamando vari documenti di ordine programmatico e politico come, ad esempio, la Comunicazione della Commissione del 18 aprile 2023, «Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE», e le conclusioni del Consiglio del 22 maggio 2023, sulla politica di ciberdifesa dell'UE. In quell'occasione, la necessità di disporre di tali competenze veniva presentata come una delle condizioni per poter garantire la piena efficacia al regolamento, identificato esplicitamente, quale elemento negativo e di sicuro ostacolo a tale obiettivo, il divario di competenze in materia di cibersicurezza all'interno dell'Unione, sia nel settore pubblico che in quello privato, così come di risorse adeguate a disposizione delle autorità nazionali di vigilanza del mercato e degli organismi di valutazione della conformità degli Stati membri.

Del resto, inoltre, sul punto il regolamento sulla cibersolidarietà riproduce, tuttavia amplificandoli, per così dire, i *desiderata* espressi dalla Commissione e indirizzati agli Stati membri nella raccomandazione 2017/1584 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala[46]. In tale raccomandazione, adottata anche all'esplicito fine di colmare le lacune che la direttiva NIS presentava rispetto all'assenza di un quadro di cooperazione dell'Unione in casi di incidenti e crisi di cibersicurezza su vasta scala[47], erano già ben presenti, infatti, le medesime valutazioni alla base del regolamento sulla cibersolidarietà[48]; così come l'enfasi posta sulla «fiducia dei

[43] Regolamento sulla cibersolidarietà, cit., considerando 1.
[44] Regolamento sulla cibersolidarietà, cit., considerando 3.
[45] *Ibidem*.
[46] Raccomandazione (UE) 2017/1584 della Commissione del 13 settembre 2017 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala, in *GUUE* L 239 del 19.9.2017, p. 36 ss.
[47] Raccomandazione (UE) 2017/1584, cit., considerando 8.
[48] In questo senso, si veda, ad esempio, il considerando 5, secondo cui «una risposta efficace agli incidenti e alle crisi di cibersicurezza su vasta scala a livello dell'UE richiede una cooperazione rapida ed efficace tra tutti i portatori di interesse e dipende dalla preparazione e dalle capacità dei singoli Stati membri, come pure da un'azione comune coordinata sostenuta dalle capacità dell'Unione. Per rispondere in modo tempestivo ed efficace agli incidenti sono pertanto necessari procedure e meccanismi di cooperazione stabiliti in precedenza e, per quanto possibile, ben collaudati che definiscano con chiarezza i ruoli e le responsabilità dei principali attori a livello nazionale e di Unione».

cittadini e delle imprese europei nei servizi digitali [ritenuta] essenziale per un mercato unico digitale fiorente»[49]. Se, dunque, considerazioni in larga parte sovrapponibili sono alla base dei due atti, appare del tutto evidente come la sostituzione di una raccomandazione della Commissione con un regolamento di Parlamento europeo e Consiglio dimostri in modo inequivoco un chiaro e rilevante salto di qualità nell'intervento dell'Unione che, certamente e prima di tutto, con tale atto vincola se stessa e, nel debito rispetto delle competenze delle varie parti in gioco, vincola altresì gli Stati membri per perseguire con maggiore forza l'obiettivo rafforzare le capacità comuni dell'Unione in materia di rilevamento, conoscenza e reazione alle minacce informatiche.

Per raggiungere il proprio scopo, il regolamento sulla cibersolidarietà individua come prioritarie l'istituzione di una rete paneuropea di poli informatici (il sistema europeo di allerta per la cibersicurezza), di un meccanismo per le emergenze di cibersicurezza e di un meccanismo europeo di riesame degli incidenti di cibersicurezza; di team nazionali di risposta agli incidenti di sicurezza informatica, sempre nel rispetto delle competenze degli Stati membri e senza pregiudizio per le attribuzioni e le funzioni dei soggetti istituiti in attuazione delle direttive NIS, primi fra tutti i CSIRT,[50]. Coerentemente con la propria natura, giustificandosi così il rinvio alla sua seconda base giuridica, l'art. 322, par. 1, lett. a), TFUE[51], per conseguire tali obiettivi il regolamento prevede la modifica di alcuni settori del regolamento (UE) 2021/694, istitutivo del programma Europa digitale[52], aggiungendo nuovi obiettivi operativi relativi al sistema europeo di allerta per la cibersicurezza e al meccanismo per le emergenze di cibersicurezza nell'ambito dell'obiettivo specifico 3 di tale programma.

5. L'applicazione del regolamento sulla cibersolidarietà fra competenze "comunitarie" e PESC.

Concentrando ora l'attenzione su un punto ben limitato, pare utile evidenziare come, rinviando agli obiettivi posti dalla Commissione e dall'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza nella Comunicazione congiunta, del 10 novembre 2022, sulla politica di ciberdifesa dell'Unione, il considerando 6 ponga l'accento, fra gli altri, sull'obiettivo di «sostenere la costituzione graduale di una riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia». Il considerando 8 accumuna il sistema europeo di allerta per la cibersicurezza e tale riserva per cibersicurezza, ai quali vengono attribuite rilevantissimi funzioni di supporto agli Stati membri, il primo, agli Stati membri e alle istituzioni/organi/organismi dell'Unione, la seconda, per anticipare le minacce informatiche e proteggersi da esse (il sistema europeo di allerta), così come per rispondere agli incidenti di cibersicurezza significativi e su vasta scala (o equivalenti) e ad attenuarne l'effetto (la riserva per la cibersicurezza).

---

[49] Raccomandazione (UE) 2017/1584, cit., considerando 22.

[50] Vale la pena di evidenziare come il considerando 7 del regolamento sulla cibersolidarietà stabilisca espressamente che tutte le azioni descritte dovrebbero realizzarsi in piena conformità alle disposizioni del TFUE in tema di aiuti di Stato alle imprese. Non potrebbe, del resto, essere altrimenti, posto che, in linea del tutto generale, l'art. 173, par. 3, comma 2, TFUE dispone, per quanto qui più ci riguarda, che il titolo XVII della parte terza del TFUE – come più sopra ricordato, costituito dal solo art. 173 TFUE – «non costituisce una base per l'introduzione da parte dell'Unione di qualsivoglia misura che possa generare distorsioni di concorrenza» e che, come ricordato più *supra*, alla nota 43, le azioni di attuazione di tale politica di Unione e Stati membri devono realizzarsi «nell'ambito di un sistema di mercati aperti e concorrenziali» *ex* art. 173, par. 1, comma 2. Per considerazioni generali in tema di rapporto fra politica industriale e politica di concorrenza dell'Unione europea, F. ROSSI DAL POZZO (a cura di), *Politiche di concorrenza e politica industriale, sinergia o conflitto?*, *Eurojus* – Fascicolo speciale, 2023.

[51] Si rinvia alla nota 42.

[52] Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240, in *GUUE* L 166 dell'11.5.2021, p. 1 ss.

Entrambi tali strumenti, ed è questo il profilo che qui più mi interessa sottolineare, si aprono al coinvolgimento e alla partecipazione di Paesi terzi o di soggetti giuridici ivi stabiliti. Si sarebbe portati ad affermare che, date le caratteristiche del fenomeno, per definizione "transfrontaliero" quanto ai suoi effetti, ma con una transfrontalierità che, ovviamente, non può arrestarsi alle frontiere dell'Unione, l'evocata "apertura" verso l'esterno dell'Unione non possa che essere obbligata; fatalmente, si direbbe, occorre che l'Unione cooperi con istituzioni internazionali e con Paesi terzi al fine di meglio rafforzare la propria risposta alle minacce e agli incidenti informatici. Se una tale premessa appare pacifica, le modalità concrete con le quali attuare tale cooperazione e, dunque, la disciplina delle stesse, non appaiono per nulla di agevole individuazione; ovvero, in altri termini, risulta altrettanto pacifico quanti e quanto rilevanti rischi esse possano comportare. Per questo il considerando 9 qualifica espressamente le istituzioni internazionali e i Paesi terzi di cui sopra come partner «di fiducia che condividono gli stessi principi» e, specificamente rispetto ai secondi, tali devono essere intesi «i paesi che condividono i principi che hanno informato la creazione dell'Unione, vale a dire la democrazia, lo Stato di diritto, l'universalità e indivisibilità dei diritti umani e delle libertà fondamentali, il rispetto della dignità umana, i principi di uguaglianza e solidarietà e il rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale, e che non pregiudicano gli interessi essenziali dell'Unione o dei suoi Stati membri in materia di sicurezza»[53].

Occorre perciò, come consuetudine, trovare il giusto bilanciamento fra interessi contrapposti e se già il regolamento istitutivo del programma Europa digitale contemplava tale apertura verso l'esterno, il regolamento sulla cibersolidarietà interviene, modificando il regolamento precedente, per garantire ancora meglio che tale apertura sia concretamente realizzabile nel rispetto di alcuni fondamentali interessi generali, fra tutti la sicurezza e il rispetto dei valori *ex* art. 2 TUE. Così, ad esempio, è ancora il considerando 8 a stabilire che, tenuto conto delle differenti e specifiche funzioni attribuite al sistema europeo di allerta per la cibersicurezza e alla riserva dell'Unione per la cibersicurezza, la partecipazione a essi dei soggetti giuridici stabiliti nell'Unione ma controllati da Paesi terzi debba essere consentita «nel caso in cui vi sia un rischio reale che gli strumenti, le infrastrutture e i servizi necessari e sufficienti, o le tecnologie, le competenze e le capacità necessarie e sufficienti, non siano disponibili nell'Unione e i vantaggi derivanti dall'inclusione di tali soggetti siano superiori ai rischi per la sicurezza». Similmente, sempre con riguardo alla piena operatività ed efficacia del sistema europeo di allerta per la cibersicurezza e della riserva dell'Unione, parrebbe opportuno, «a condizione che siano soddisfatte determinate condizioni di disponibilità e sicurezza, che le gare d'appalto per tali infrastrutture, strumenti e servizi potrebbero essere aperte a soggetti giuridici controllati da paesi terzi, a condizione che siano rispettati i requisiti di sicurezza»[54]. Ai fini di una tale verifica, e in modo ancora più specifico, i colegislatori dell'Unione propongono di tenere in considerazione «diversi elementi, quali la struttura societaria e il processo decisionale di un soggetto, la sicurezza dei dati e delle informazioni classificate o sensibili e la garanzia che i risultati dell'azione non siano soggetti a controlli o restrizioni da parte di paesi terzi non ammissibili»[55].

Il regolamento contempla poi anche quella che potrebbe definirsi una seconda forma di "apertura" verso l'esterno, ovverosia l'ammissione al sostegno alla riserva per la cibersicurezza concessa anche ai Paesi terzi associati al Programma Europa digitale. In linea generale, e dato per soddisfatto il requisito preliminare secondo cui una tale ammissione sia possibile unicamente laddove lo specifico accordo con cui un Paese terzo è associato al Programma preveda specificamente questo sostegno, Parlamento europeo e Consiglio ritengono che uno scenario siffatto possa darsi se, da un lato,

[53] Regolamento sulla cibersolidarietà, cit., considerando 9.
[54] *Ibidem*.
[55] *Ibidem*.

i soggetti per i quali il Paese terzo domanda il sostegno siano attivi in settori critici o ad alta criticità, dall'altro lato, laddove gli incidenti individuati determinino «perturbazioni operative significative o potrebbero avere effetti di ricaduta nell'Unione»[56]. Tali Paesi terzi, inoltre e più specificamente, sarebbero chiamati, sottoposti a tal fine a una valutazione periodica da parte della Commissione ai sensi dell'art. 19, par. 3, al rispetto di ulteriori tre criteri, l'ultimo dei quali appare, qui, particolarmente significativo[57]. La lett. c) di tale disposizione impone infatti che «il sostegno fornito [sia] coerente con la politica dell'Unione nei confronti del paese e con le sue relazioni generali con il paese, e se [sia] coerente con altre politiche dell'Unione in materia di sicurezza». Al fine di rendere possibile una tale valutazione, il regolamento prevede che la Commissione si consulti con l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza.

L'apertura ai Paesi terzi mette perciò in gioco, in maniera tanto evidente quanto inevitabile, procedure e valutazioni che, fossimo ancora sotto il regime precedente alla revisione dei Trattati attuata con il Trattato di Lisbona, collocheremmo a cavallo fra due pilastri dell'Unione, il primo, costituito dalle Comunità (dunque dalle politiche, esercitate, seppure in maniera non del tutto uniforme, con il cosiddetto metodo comunitario, del mercato interno, dell'agricoltura, dello spazio di libertà, sicurezza e giustizia, dei trasporti, dell'occupazione, dell'ambiente e via dicendo), e il secondo, rappresentato dalla politica estera e di sicurezza comune (nella cui preparazione e attuazione risulta(va) predominante un metodo intergovernativo)[58]. In effetti, facendo ora astrazione del dato formale e collocando (anche) il regolamento sulla cibersolidarietà nel contesto del quadro giuridico che, in materia di cibersicurezza, l'Unione ha adottato in vista dell'instaurazione dell'efficace funzionamento del mercato interno, emerge in maniera molto chiara come la prospettiva interna e quella esterna all'Unione non possano che essere intimamente connesse e debbano, a motivo di ciò, fondarsi su principi il più possibile comuni e condivisi. Così, come del resto già messo in luce anche con riferimento agli altri interventi di armonizzazione – questi ultimi sì, formalmente ascrivibili alla competenza dell'Unione in materia di mercato interno – , la prospettiva plurivaloriale appare ben presente al legislatore dell'Unione.

Il rispetto di determinati valori e principi, dunque la condivisione di essi fra l'Unione e il Paese terzo di volta in volta in considerazione, non può non scandire la corretta attuazione degli obblighi previsti dal regolamento sulla cibersolidarietà e, per tale via, sancire oppure no la sua stessa piena efficacia. Se, come ricordato, tali principi e valori sono, come è pacifico che sia in tema di cibersicurezza, connessi agli interessi essenziali dell'Unione in tema di sicurezza, dal loro rispetto non può, evidentemente, prescindersi. In proposito, il considerando 53, del resto, è cristallino quando ricorda che «la fornitura di sostegno ai paesi terzi associati al programma Europa digitale può incidere sulle relazioni con i paesi terzi e sulla politica di sicurezza dell'Unione, anche nel contesto della politica estera e di sicurezza comune e della politica di sicurezza e di difesa comune».

Ne derivano, allora, importanti implicazioni di ordine istituzionale e, in concreto, molto pratico sulla gestione del regolamento sulla cibersolidarietà; ancora potendosi richiamare quell'immagine, sbiadita forse ma pur sempre ancora molto efficace laddove si ponga mente al fatto che l'eliminazione dei pilastri è stata realizzata in maniera compiuta soltanto sotto un profilo formale attraverso il Trattato

---

[56] Regolamento sulla cibersolidarietà, cit., considerando 52.

[57] I primi due criteri, *ex* art. 19, par. 3, lett. a) e b), prescrivono che il Paese debba «rispettare le condizioni dell'accordo […] nella misura in cui esse si riferiscono alla partecipazione alla riserva dell'UE per la cibersicurezza» e che abbia «adottato misure adeguate per prepararsi a incidenti di cibersicurezza significativi o agli incidenti di cibersicurezza equivalenti a incidenti su vasta scala». In altri termini, è cioè necessario che il Paese *de quo* rispetti pienamente i termini pertinenti dell'accordo e abbia mostrato di disporre di un quadro di misure in ogni caso rispondenti ai normali standard di diligenza richiesti, «data la natura complementare della riserva dell'UE per la cibersicurezza» (così il considerando 52 del regolamento).

[58] In tema, per tutti, U. VILLANI, *Metodo comunitario e metodo intergovernativo nell'attuale fase dell'Unione europea*, in *Studi sull'Integrazione Europea*, 2019, pp. 259-270.

di Lisbona, dell'intersezione, per così dire, fra primo e secondo pilastro dell'Unione. Si è già fatto riferimento all'obbligo per la Commissione, *ex* art. 19, par. 3, di consultare l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza; se essa ritiene che un paese terzo associato al programma Europa digitale soddisfi tutte le condizioni richieste presenta al Consiglio una proposta di adozione di un atto di esecuzione per autorizzare la fornitura di sostegno a titolo della riserva dell'UE per la cibersicurezza nei confronti di tale paese. In modo ben più significativo, tuttavia, occorre evidenziare come il medesimo art. 19 attribuisca direttamente al Consiglio, in circostanze, beninteso e certamente, eccezionali, la competenza per modificare o abrogare, di propria iniziativa, uno di tali atti di esecuzione. Qualora, infatti, il Consiglio «ritenga che vi sia stato un cambiamento significativo per quanto riguarda il criterio di cui al paragrafo 3, primo comma, lettera c)»[59], il regolamento ritiene necessaria un'azione urgente da parte dell'Unione, tale da non consentire alla Commissione di esercitare la sua ordinaria competenza di esecuzione, non potendosi attendere lo svolgimento di valutazioni approfondite e in anticipo da parte di quest'ultima istituzione. È d'uopo ricordare come le condizioni per poter soddisfare il suddetto criterio, il terzo nell'ordine previsto dall'art. 19, par. 3, siano quelle, più propriamente "politiche", pacificamente delineatesi nel contesto della competenza dell'Unione in materia di politica estera e di sicurezza comune. Se è pur vero, dunque, che la scelta operata dal regolamento sulla cibersolidarietà non possa essere ritenuta, *ex se*, illegittima rispetto al quadro delle competenze delle singole istituzioni come previsto dai Trattati istitutivi – la dottrina ricorda che il Consiglio «concentra una serie di attribuzioni e funzioni che lo caratterizzano come titolare al tempo stesso del potere legislativo e di quello esecutivo»[60] – pare ben più significativo notare come tale scelta debba dirsi, in un certo senso, imposta dalla consapevolezza che, in linea generale, a definire e attuare la politica estera e di sicurezza comune sia, *ex* art. 24, comma 2, TUE il Consiglio (insieme al Consiglio europeo), una volta accertato, come si è fatto fin qui, che l'applicazione del regolamento sulla cibersolidarietà, ai fini di garantirne davvero l'efficacia, non possa, appunto, essere confinata all'interno di un'unica politica (industriale? mercato interno?) dell'Unione.

6. Considerazioni conclusive.

L'analisi di taluni e specifici profili del regolamento sulla ciberresilienza e del regolamento sulla cibersolidarietà consente di formulare qualche riflessione conclusiva di tenore generale rispetto al quadro normativo adottato dall'Unione in materia di cibersicurezza. Ciò che pare emergere in modo molto evidente è che tale quadro permette di apprezzare in modo chiarissimo il grado di complessità cui, sotto molteplici profili, è giunto oggi, in generale, l'intero processo di integrazione europea, costituendone una rappresentazione esemplificativa altamente efficace.

In particolare, un tale scenario induce a interrogarsi in merito alla legittimità di un intervento di armonizzazione adottato in vista del soddisfacimento di più (e fra di loro differenti) valori ma esclusivamente fondato sull'unica base giuridica dell'art. 114 TFUE e, dunque, su di un'unica competenza, quella riferibile all'instaurazione e al funzionamento del mercato interno, dell'Unione. D'altra parte, occorre anche domandarsi se sia necessaria e, ancora, se sia legittima alla luce del quadro delle competenze attribuite su cui l'Unione si fonda, l'evidenziata sorta di mobilità, quanto, di nuovo, agli ambiti di materia presenti nei Trattati istitutivi, degli effetti derivanti dall'applicazione di un singolo atto. Detto altrimenti, è legittimo che un regolamento adottato, essenzialmente, nell'ambito della politica industriale dell'Unione (pur se, peraltro, ritenuto necessario per completare un quadro normativo che si

[59] Così l'art. 19, par. 5, comma 2, del regolamento sulla cibersolidarietà, cit.
[60] In questi termini, R. ADAM, A. TIZZANO, *Lineamenti di diritto dell'Unione europea*, Giappichelli, Torino, 2022, p. 70.

fonda su una politica dell'Unione ancora differente) perché possa pienamente produrre i propri effetti debba "coinvolgere" politiche differenti, chiamando eventualmente in causa anche istituzioni a prima vista estranee a tale regolamento?

Quanto al primo quesito, esso mette in discussione, in sostanza, l'idoneità di un'unica base giuridica di diritto primario a perseguire, simultaneamente, più valori e interessi generali di ordine differente; un'idea, dunque, di pluralismo valoriale a partire, tuttavia, da un'unica base giuridica e quindi all'interno di una sola specifica politica dell'Unione.

In merito, si è fatto riferimento a una sorta di *climax* cui, pur se con intensità differenti, non si sottrae nessuno degli atti presentati. Con specifico riguardo alla direttiva NIS 2 e al regolamento sulla cibersolidarietà, ad esempio, entrambi i considerando 2 di tali atti illustrano in modo chiaro quali interessi generali possano essere colpiti da una minaccia o da un incidente informatico: vengono in considerazione ostacoli, prima di tutto, all'esercizio dell'attività economica nel mercato interno, quindi all'erogazione di pubblici servizi; vengono poi messe in luce, quali conseguenze di tali ostacoli, perdite finanziarie e perdite di fiducia degli utenti, gravi danni alle economie e alle società dell'Unione che, a loro volta, si concretizzano anche in gravi danni alle economie e ai sistemi democratici dell'Unione. La progressione è evidente. Che il legislatore di diritto derivato dell'Unione sia sempre più impegnato, in tempi recenti, in un'operazione di "rilettura" della base giuridica, in particolare proprio con riferimento all'art. 114 TFUE, è ben messo in evidenza da quella dottrina che, pur dichiarandosi non sorpresa di una tale evoluzione, si domanda tuttavia fino a che punto essa possa avvenire «a diritto (primario) costante senza che venga a determinarsi una violazione del principio costituzionale di attribuzione delle competenze»[61].

Occorre ritenere che senz'altro, alla luce dell'attuale quadro di riferimento, costituito dal diritto primario e dalla giurisprudenza interpretativa della Corte di giustizia che si è formata su di esso, tali atti debbano ritenersi del tutto legittimi. Di più, potrebbe anche ricordarsi come un tale fenomeno non rappresenti davvero un'assoluta novità nel panorama degli atti di diritto derivato dell'Unione (meglio, delle allora Comunità economiche) volti all'instaurazione e al funzionamento del mercato (già) comune. In questo senso, particolarmente significativa appare la direttiva 65/65/CEE[62] – della quale proprio quest'anno ricorrono i 60 anni dall'approvazione – che può ben definirsi il primo atto di armonizzazione in tema di circolazione dei medicinali nelle Comunità. Tale direttiva aveva quale base giuridica l'art. 100 del Trattato CEE (nella sostanza l'attuale, e ormai del tutto residuale, art. 115 TFUE) ovverosia l'allora unico fondamento normativo esistente in tema di armonizzazione per la realizzazione del mercato comune. Siffatta disposizione, come noto, prevedeva che, all'unanimità e su proposta della Commissione, il Consiglio potesse stabilire «direttive volte al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che [avessero] un'incidenza diretta sull'instaurazione o sul funzionamento del mercato comune»; eventualmente consultati l'Assemblea (l'attuale Parlamento europeo) e il Comitato economico e sociale sulle direttive «la cui esecuzione [avrebbe importato], in uno o più Stati membri, una modificazione nelle disposizioni legislative». A giustificare, esattamente come allo stato attuale, l'adozione di una direttiva di armonizzazione le disparità esistenti fra le disposizioni nazionali, qui relative ai medicinali, giudicate idonee a «ostacolare

[61] In questi termini, con considerazioni riferite specificamente al cosiddetto *Digital Services Act* ma che ben possono essere traslate nel contesto che qui ci occupa, trovandosi pur sempre all'interno, proprio per il discorso svolto fin qui sulle basi giuridiche dei provvedimenti di armonizzazione presentati, del mercato unico digitale dell'Unione, F. CASOLARI, *Il* Digital Services Act *e la costituzionalizzazione dello spazio digitale europeo*, in *Giurispr. It.*, 2024, pp. 462-465, a p. 465.

[62] Direttiva del Consiglio, del 26 gennaio 1965, per il ravvicinamento delle disposizioni legislative, regolamentari ed amministrative relative alle specialità medicinali, in *GUCE* L 369 del 9.2.1965, p. 65 ss.

gli scambi delle specialità medicinali in seno alla Comunità»[63] e aventi perciò «un'incidenza diretta sull'instaurazione e sul funzionamento del mercato comune»[64]. Se, dunque, la necessità di eliminare gli ostacoli determinati dalle evocate differenze di disciplina fra gli Stati membri legittimava l'impiego dell'art. 100 CEE quale base giuridica della direttiva *de qua*, nel dettare i requisiti armonizzati di qualità, sicurezza ed efficacia dei medicinali a uso umano il Consiglio (allora unico legislatore di diritto derivato comunitario) aveva tuttavia espressamente dichiarato di avere, come unico ed essenziale obiettivo, quello di garantire la tutela della sanità pubblica[65]. Tutto ciò, come ben noto, in assenza, nei Trattati istitutivi, di qualsiasi idonea base giuridica o di politiche comunitarie espressamente volte alla protezione di tale fondamentale interesse generale "non economico" nell'adozione di normative armonizzate sulla libera circolazione delle merci (beninteso, nel caso, di ben peculiari merci).

Ma al di là del dato, per così dire, aneddotico che può soltanto indurre a ritenere che non si sia davvero di fronte a fenomeni nuovi – e, anzi, per quel che si dirà subito, posto il ben differente quadro "costituzionale" di riferimento rispetto a quello attuale, quelle misure di armonizzazione avrebbero dovuto destare preoccupazioni senz'altro più forti e forse anche più giustificate rispetto a quelle cui possono dar luogo gli atti di armonizzazione presentati – , vi sono due ordini di ragioni, fra loro intimamente connesse, che militano per la piena legittimità dei regolamenti in parola.

La prima ragione potrebbe andare sotto il nome della "funzionalità", facendosi cioè appello a una caratteristica precipua dell'ordinamento dell'Unione e prima ancora, e forse in modo ancora più evidente, dell'ordinamento delle Comunità. Tali ordinamenti, innegabilmente, costituiscono sistemi giuridici che, di per sé, presentano fin dall'inizio un rilevantissimo carattere funzionale al perseguimento di obiettivi determinati; vale a dire di quelli, evidentemente, indicati nei loro Trattati istitutivi[66]. Se è ben vero che di tale funzionalità si fa, per prima, interprete e forse anche paladina strenua la Corte di giustizia[67], è altrettanto vero che questa funzionalità debba dirsi insita già negli stessi Trattati istitutivi. Ne costituisce un evidente esempio, ancora, l'art. 100 del Trattato CEE che, si potrebbe dire, a fronte di coordinate piuttosto vaghe consente, come appena visto, l'adozione di atti di armonizzazione per assicurare a sua volta del tutto "generiche" libertà economiche di circolazione. Tale disposizione si presta, perciò, senza dubbio a un'interpretazione evolutiva e funzionale al raggiungimento di obiettivi, come detto, a loro volta individuati in modo non del tutto preciso (o, se si preferisce, dal contenuto notevolmente ampio) dai Trattati istitutivi. Del resto, a compensare questa vaghezza e, anche, a confermare indirettamente simile ricostruzione, si pone la previsione di un voto all'unanimità in seno al Consiglio. Se è vero, cioè, che attraverso tale norma la Comunità avrebbe potuto legiferare pur in assenza di specifica competenza (basi giuridiche e/o politiche espressamente previste dai Trattati, cioè, maggiormente rispondenti agli obiettivi dichiarati degli atti di armonizzazione via via adottati), ciò non sarebbe stato possibile se non con il consenso unanime di tutti i suoi Stati membri, attraverso un voto del Consiglio.

Soprattutto, venendo alla seconda ragione, la richiamata evoluzione in senso strumentale dell'ordinamento dell'Unione e che ha permesso, ad esempio, l'adozione della direttiva 65/65/CEE, è stata poi "costituzionalizzata", essendo stata recepita nei Trattati istitutivi con le varie e successive revisioni che li hanno via via interessati. Sono, così, state concepite nuove basi giuridiche, ovvero è stato reso più semplice, dal punto di vista procedurale, l'impiego di quelle esistenti; sono state previste nuove

[63] Direttiva 65/65/CEE, cit., considerando 3.
[64] *Ibidem*.
[65] Direttiva 65/65/CEE, cit., considerando 1.
[66] Per analoghe considerazioni, pur se espressamente riferite alle peculiari specificità dell'attività interpretativa del diritto dell'Unione ad opera della Corte di giustizia, si vedano P. MENGOZZI, C. MORVIDUCCI, *Isitituzioni di diritto dell'Unione europea*, Lavis, 2014, a p. 252.
[67] In merito, *ex multis*, R. ADAM, A. TIZZANO, *Lineamenti*, cit., p. 222.

competenze e, dunque, nuove politiche, attribuite, sia pure tendenzialmente in via concorrente, alla Comunità/Unione; hanno fatto la propria comparsa nei Trattati, più recentemente, disposizioni di carattere orizzontale idonee a ricevere applicazione all'interno di differenti politiche dell'Unione. Non può, dunque, ritenersi illegittimo un intervento di armonizzazione che realizzi obiettivi ben più "alti" del (mero) completamento del mercato interno soltanto per via del fatto che esso si basi esclusivamente (o principalmente) sull'art. 114 TFUE. Sarebbe forse più opportuno dire che, allo stato attuale del processo di integrazione, e coerentemente con le prese di posizione espresse dalla Corte di giustizia[68], il legislatore di diritto derivato dell'Unione – sempre più simile a un legislatore nazionale – debba sì ancora trovare la base giuridica adeguata a fondare la propria competenza ad adottare atti. Continua, in tale scenario, del resto a essere in gioco la questione, di rilievo assolutamente costituzionale, del rapporto dell'Unione con i suoi Stati; questione che, formalmente e nel quadro del sistema giurisdizionale dell'Unione e delle competenze della Corte di giustizia, si risolve nel giudizio sulla legittimità dell'intervento legislativo stesso dell'Unione. Tuttavia, il "come" poi orientare quell'intervento, ovverosia determinare il merito delle scelte e, in ancora più semplificati termini, il contenuto della disciplina concretamente applicabile, attuando un delicato bilanciamento fra interessi generali contrapposti, non può che essere determinato (anche) da altre disposizioni di rango primario che, a differenza del passato, sono ora sicuramente presenti nei Trattati e dalle quali non può, dunque, per nulla prescindersi.

In questo senso, dunque, può emergere l'idea che il legislatore di diritto derivato europeo possa apparire sempre più simile a un legislatore nazionale, della cui competenza non può ragionevolmente dubitarsi rispetto a nessuna materia in cui intenda intervenire e che, perciò, viene apprezzato e sottoposto a valutazione proprio in virtù di come attua quell'evocato bilanciamento fra valori ed esigenze generali fra di loro in conflitto. Se l'art. 114 TFUE può fungere, in modo tutto sommato piuttosto agevole, da così ampia base giuridica, l'illusione ottica che ne deriva è, per l'appunto, perfino quella di "dimenticarsi" di essere al cospetto di un ordinamento giuridico di un soggetto diverso dallo Stato[69], al fine di domandarsi se esso disponga oppure no di una competenza legislativa armonizzatrice, per ritenere invece assorbente l'apprezzamento (che si presenterebbe come) successivo, quello volto ad appurare come gli interessi generali vengono fra loro ordinati.

Sono quindi quelle disposizioni di carattere orizzontale, disseminate qua e là nei Trattati istitutivi, ad assumere assoluto rilievo. Fra di esse, in primo luogo, rileva ovviamente il paragrafo 3 dello stesso art. 114 TFUE, ai sensi del quale, come noto, nelle sue proposte di atti di armonizzazione in materia di sanità, sicurezza, protezione dell'ambiente e protezione dei consumatori, la Commissione è tenuta a basarsi «su un livello di protezione elevato, tenuto conto, in particolare, degli eventuali sviluppi fondati su riscontri scientifici»; obiettivo cui pure Parlamento europeo e Consiglio devono ritenersi espressamente vincolati. In linea, fatalmente, del tutto generale, l'art. 2 TUE pone poi la cornice di valori comuni entro cui il legislatore di diritto derivato dell'Unione è chiamato a muoversi, come emerge in maniera evidente proprio dai primi considerando degli atti che formano il quadro legislativo europeo in materia di cibersicurezza. Similmente, ma con una portata fatalmente ben diversa, la Carta dei diritti fondamentali dell'Unione costituisce imprescindibile vincolo di legittimità per ogni atto legislativo

---

[68] Si vedano, *ex multis*, Corte di giustizia, 4 maggio 2016, causa C-358/14, *Polonia c. Parlamento europeo e Consiglio dell'Unione*, ECLI:EU:C:2016:323, punti 34-36 e giurisprudenza ivi citata; Corte di giustizia, gr. sez., 8 dicembre 2020, causa C-626/18, *Polonia c. Parlamento europeo e Consiglio dell'Unione*, ECLI:EU:C:2020:1000; punti 46-53; Corte di giustizia, gr. sez., 8 dicembre 2020, causa C-620/18, *Ungheria c. Parlamento europeo e Consiglio dell'Unione*, ECLI:EU:C:2020:1001, punti 41-48.

[69] In merito, per considerazioni anche più generali, G. TESAURO, *Una nuova revisione dei Trattati dell'Unione per conservare i valori del passato*, in *I Post di AISDUE, aisdue.eu*, 18 giugno 2021, p. 4 ss. Si rinvia, altresì, a R. ADAM, A. TIZZANO, *Lineamenti*, cit., p. 10 ss.

dell'Unione, disponendo essa, anche qui come noto, *ex* art. 6, par. 1, TUE dello «stesso valore giuridico dei trattati»[70]. Rilevanti sono anche le coordinate, anch'esse generali, poste dall'art. 3, par. 3, TUE tese a delineare, in via certamente lata, la nozione di mercato interno. L'obiettivo dell'Unione non è, cioè, solo quello di instaurare un mercato interno "qualsiasi", bensì un mercato interno nel quale numerosi valori e interessi generali devono essere tenuti in considerazione e, dunque, messi in equilibrio con le libertà di circolazione. Vengono così in gioco, fra gli altri, principi davvero fondamentali e caratterizzanti il processo di integrazione europea quali lo sviluppo sostenibile, la piena occupazione e il progresso sociale, la lotta alle discriminazioni, la parità fra donne e uomini, l'elevato livello di tutela e di miglioramento della qualità dell'ambiente, oltre che, naturalmente, l'economia sociale di mercato fortemente competitiva.

Vera e propria clausola orizzontale deve ritenersi, soprattutto, l'art. 9 TFUE che potrebbe ben qualificarsi come un tentativo di concretizzare alcuni almeno di tali ultimi e generali valori. Tale disposizione, infatti, collocata fra quelle di applicazione generale di cui al Titolo II del TFUE (dunque nel Titolo che immediatamente precede quelli riferiti alle singole politiche) afferma che «nella definizione e nell'attuazione delle sue politiche e azioni, l'Unione tiene conto delle esigenze connesse con la promozione di un elevato livello di occupazione, la garanzia di un'adeguata protezione sociale, la lotta contro l'esclusione sociale e un elevato livello di istruzione, formazione e tutela della salute umana»[71].

Rispetto al secondo quesito e, dunque, alla possibilità di ritenere legittimo un intervento dell'Unione quando la sua attuazione concreta renda necessario "allontanarsi" dalla specifica politica dell'Unione nel quale esso sia stato adottato e ciò, in particolare, qualora una tale attuazione metta in gioco, come per il regolamento sulla cibersolidarietà, istituzioni e procedure che coinvolgano più pilastri dell'ex Unione di Maastricht, le considerazioni da svolgere sono, nella sostanza, molto simili alle precedenti.

Non si può, cioè, che ritenere legittimo un simile intervento legislativo anche solo alla luce della circostanza per cui il legislatore dell'Unione non può più dirsi costretto all'interno di un'unica politica e, dunque, di un'unica competenza fra quelle previste dai Trattati istitutivi. Che tali sconfinamenti possano o meno avvenire, e con quale di volta in volta variabile intensità, dipende invero dal tipo di

---

[70] In proposito, la Carta dei diritti fondamentali sarebbe, inoltre, ovviamente vincolante anche per gli Stati membri. Con particolare riferimento agli atti di armonizzazione del mercato interno, il recepimento nazionale di procedure uniformi cui subordinare le libertà economiche di circolazione, come per gli atti summenzionati rispetto a specifiche merci, e, soprattutto, l'utilizzo di procedure di salvaguardia che consentono di derogare, seppure in via provvisoria e sotto il controllo della Commissione, al principio generale della libera circolazione che l'atto di armonizzazione prevede, costituiscono, infatti, misure di attuazione del diritto dell'Unione e, per tale via, rendono applicabile la Carta dei diritti (ai sensi del suo art. 51, par. 1) e scrutinabili rispetto a essa le condotte degli Stati membri.

[71] Vale la pena, almeno in nota, soltanto accennare a un'ulteriore considerazione. Se, come si è fin qui tentato di argomentare, il regolamento in parola costituisce a pieno titolo un atto di diritto derivato di armonizzazione delle disposizioni nazionali in vista dell'instaurazione del mercato interno, si sarebbe tentati di interrogarsi circa la sua rispondenza ai requisiti recentemente fissati dalla Commissione nella Comunicazione «The Single Market: our European home market in an uncertain world - A Strategy for making the Single Market simple, seamless and strong» del 21 maggio 2025; pur essendo tale regolamento precedente alla Comunicazione. Alla luce dei numerosi criteri fissati dalla Commissione, potrebbe ben dirsi, a prima vista, che il complicato quadro di relazioni che il regolamento sulla ciberresilienza è chiamato a intrattenere con numerosi ulteriori atti di diritto derivato già adottati rappresenti un chiaro (ma evidentemente necessario) elemento di debolezza quanto all'idea che, allo stato attuale, il mercato interno soffrirebbe proprio di un eccesso di disciplina a livello dell'Unione stessa (Comunicazione «The Single Market», cit., pp. 4-6). In linea ancor più generale, poi, occorre valutare se, effettivamente, la dichiarata attenzione più volte posta alle difficoltà che le microimprese e le PMI incontrano nell'applicazione del regolamento metta concretamente davvero al riparo tali operatori economici da costi e oneri eccessivi, così come ne preservi le potenzialità innovative (in merito, si rinvia, ad esempio, alle pp. 3, 7-8, 20 ss. della Comunicazione).

ambito del quale tale legislatore intenda occuparsi, evidentemente. A questo proposito, come chiaro, l'ambito della cibersicurezza non può che mettere in comunicazione differenti politiche e competenze, essendo di per sé destinato a implicare riflessioni e a toccare interessi generali di diverso tipo.

A confermare un tale assunto, basti solo accennare al fatto che la ciberdifesa (che, certo, è ambito non del tutto coincidente con la cibersicurezza costituendone tuttavia, per così dire, un approfondimento specifico e operativo[72]) è contemplata, all'interno della cooperazione strutturata permanente nel settore della difesa *ex* art. 42, par. 6, TUE, nel contesto della cosiddetta «PESCO» di cui alla decisione del Consiglio 2017/2315[73], con un progetto, cui l'Italia prende parte, volto allo sviluppo di una piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta agli incidenti informatici, al più ampio fine di intensificare la cooperazione in materia di ciberdifesa.

Vi è, tuttavia, di più. L'"interferenza" che, fatalmente, si verifica con l'ambito PESC consente, o per meglio dire impone, anche in questo caso in modo non dissimile da quanto più sopra evidenziato, di riferirsi a disposizioni orizzontali previste nei Trattati istitutivi. In questo senso, e con specifico riferimento proprio alle disposizioni in tema di PESC, rileva innanzitutto, fra le disposizioni generali sull'azione esterna dell'Unione, l'art. 21, par. 3, comma 2, TUE ai sensi del quale «l'Unione assicura la coerenza tra i vari settori dell'azione esterna e tra questi e le altre politiche. Il Consiglio e la Commissione, assistiti dall'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, garantiscono tale coerenza e cooperano a questo fine».

Ancora, con significativo riguardo alle disposizioni di applicazione generale dettate, ora, dal TFUE, occorre ricordare come l'art. 7 TFUE imponga all'Unione di «assicura[re] la coerenza tra le sue varie politiche e azioni, tenendo conto dell'insieme dei suoi obiettivi e conformandosi al principio di attribuzione delle competenze». Tali articoli, e il principio generale di coerenza che essi esprimono, devono perciò ritenersi idonei, anch'essi, a legittimare l'evocato sconfinamento fra politiche, impegnando le istituzioni a garantire che, fra tali politiche, si giunga a un efficace coordinamento.

In questo senso, in definitiva, se la questione, come ricorda la dottrina sopra richiamata, è "costituzionale", costituzionale è ormai anche la risposta da fornire a tale questione[74]. Proprio il rinvio all'art. 7 TFUE parrebbe confermare questa chiave di lettura, ormai imprescindibile. Allo stato attuale del processo di integrazione europea, l'ordinamento dell'Unione offre un consistente insieme di principi di rango "costituzionale" che dominano e scandiscono il suo operato; insieme di principi dal pieno rispetto dei quali dipende ogni valutazione di legittimità di tale operato. Per citarne soltanto alcuni: sussidiarietà, proporzionalità, leale cooperazione, equilibrio istituzionale, certezza del diritto e, ovviamente, il principio di attribuzione. Recente è, per ovvi motivi connessi al livello di approfondimento dell'integrazione raggiunto via via con i procedimenti di revisione dei Trattati istitutivi, la comparsa del principio di coerenza fra le differenti politiche dell'Unione.

Una valutazione in merito alla possibilità di rinvenire una gerarchia fra tali principi richiederebbe ben altro genere di approfondimento, forse perfino sproporzionato rispetto al circoscritto tema che si è qui tentato di affrontare. L'art. 7 TFUE, tuttavia, già consente di formulare un'ipotesi ricostruttiva ragionevolmente coerente, è da ritenere, con l'attuale fisionomia assunta dall'ordinamento dell'Unione, anche alla luce della pertinente giurisprudenza della Corte cui, *supra*, si è fatto

---

[72] In questo senso, *ex multis*, si rinvia alla Comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza «La politica di ciberdifesa dell'UE», del 10 novembre 2022, doc. JOIN(2022) 49 final, e alla cosiddetta «Bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali», approvata dal Consiglio il 21 marzo 2022.

[73] Decisione (PESC) 2017/2315 del Consiglio, dell'11 dicembre 2017, che istituisce la cooperazione strutturata permanente (PESCO) e fissa l'elenco degli Stati membri partecipanti, in *GUUE* L 331 del 14.12.2017, p. 57 ss.

[74] Si rinvia alla nota 62.

riferimento[75]. Il principio di attribuzione pare costituire, indubbiamente, il principio gerarchicamente più elevato posto che l'art. 7 TFUE, come appena ricordato, vi fa rinvio come sorta di insuperabile limite all'esplicarsi del principio di coerenza. È, tuttavia, forse giunto il momento di provare a conferire a tale principio di attribuzione un margine di elasticità che, a parere di chi scrive, sarebbe in fondo imposto dalla necessità di assicurare contestualmente il rispetto di più principi "costituzionali". Si potrebbe, cioè, ritenere che il principio di attribuzione possa ritenersi rispettato anche qualora, al fine di assicurare la piena efficacia di un atto di diritto derivato dell'Unione, sia necessario dare concreta applicazione a politiche (dunque a disposizioni attributive di competenza) differenti rispetto a quelle sulle quali, formalmente, tali atti sono stati adottati. Ciò, tuttavia, laddove appunto il principio di coerenza fra le varie politiche e azioni dell'Unione renda obiettivamente (il più possibile obiettivamente, almeno) necessario "coinvolgere" politiche e competenze "altre" rispetto a quelle espressamente già contemplate dall'atto stesso. Due condizioni, dunque, occorrerebbe fossero adeguatamente dimostrare dall'Unione ai suoi Stati membri: da un lato, e sotto un profilo più concreto, l'effettiva applicazione dell'atto dovrebbe reclamare, per così dire, come necessario presupposto della sua piena efficacia la considerazione di interessi generali tuttavia appannaggio di altre politiche; dall'altro lato, sotto un profilo più generale e astratto, il suo ambito di intervento si dovrebbe prestare a essere ricondotto a differenti competenze fra quelle attribuite dai Trattati all'Unione.

Degno di nota, e in via generale, vale a dire rispetto ad entrambi i contesti di criticità illustrati, infine, è sottolineare come le disposizioni di carattere orizzontale, includendo in tale categoria tanto le disposizioni più astratte (come l'art. 7 TFUE) quanto quelle dal contenuto apparentemente più concreto e definito (come l'art. 9 TFUE), siano il frutto dei più recenti procedimenti di revisione dei Trattati, dunque della unanime volontà degli Stati membri.

Se, in definitiva, nel (lungo) periodo precedente alla prima riforma dei Trattati attuata con l'Atto Unico Europeo, la tendenza a interpretare in maniera eccessivamente estensiva la nozione di «mercato comune» al fine di, nella sostanza, legiferare al di là delle competenze espressamente attribuite alle Comunità dai Trattati è interamente da addebitare alle sole istituzioni comunitarie – e certamente, come si è segnalato, non si dimentichi che questa è una considerazione formale posto che la base giuridica utilizzata in quegli anni imponeva un voto unanime in Consiglio, dunque l'accordo di tutti i ministri degli Stati membri – l'introduzione delle disposizioni orizzontali, che legittimano a livello dello stesso Trattato quella che può pur sempre apparire, a prima vista, come un'indebita estensione di competenze realizzata attraverso il ricorso all'art. 114 TFUE per attuare considerazioni riferite a interessi generali "altri" rispetto a quelli più direttamente e pacificamente collegati al mercato interno, è, appunto, avvenuta con procedimenti di revisione dei Trattati e, dunque, con il consenso unanime degli Stati membri, che hanno negoziato e firmato tali Trattati, e dei loro Parlamenti nazionali di norma chiamati a ratificarli; nella piena consapevolezza, perciò, di tutti coloro che, a vario titolo, a questi processi di revisione hanno preso parte.

[75] Si rinvia alla nota 69.