Lorenzo Ricci

Il Comitato interistituzionale per la cibersicurezza e la direzione strategica del CERT-EU: verso una 'regolazione strategica' della cibersicurezza?

Abstract: L'articolo si apre con l'esame del Comitato interistituzionale per la sicurezza informatica (IICB). Il Regolamento (UE) 2023/2841, oltre ad assegnare maggiori compiti e un ruolo più ampio al CERT-EU, attribuisce a questo organo il duplice compito di monitorare e sostenere l'attuazione del regolamento citato, da parte degli attori dell'UE, nonché di supervisionare l'attuazione delle priorità e degli obiettivi generali del CERT-EU, con la possibilità di fornire una direzione strategica a questa entità. Si tratta, quindi, di riflettere sull'organizzazione e sulle funzioni attribuite a questo board, nel tentativo di evidenziare il ruolo che si intende attribuirgli e, soprattutto, i poteri normativi che lo caratterizzano, nella direzione di configurare un modello omogeneo ed efficace di regolamentazione della cybersecurity.

Keywords: ICBB; CERT-EU; Coordinamento; Direzione strategica; Regolazione strategica.

1. Premessa

Il regolamento (UE) 2023/2841 ha istituito il Comitato interistituzionale per la cibersicurezza (IICB), al duplice scopo di controllare e sostenere l'attuazione del presente regolamento da parte dei soggetti dell'UE, nonché di vigilare in relazione alla realizzazione delle priorità e degli obiettivi generali del CERT-EU, con la possibilità di imprimere a tale centro una direzione di tipo strategico. Sotto questo profilo, il regolamento in questione ha inoltre attribuito maggiori compiti nonché un più ampio ruolo al CERT-EU.

Pertanto, si tenterà anzitutto di riflettere sull'organizzazione e sulle funzioni che sono attribuite a questo Comitato[1], per cercare di chiarire il ruolo che si è inteso attribuirgli e, in special modo, i poteri di regolazione che lo caratterizzano, nella direzione di configurare un sistema omogeneo ed efficace di cibersicurezza a livello europeo.

1 Più in generale, sul ruolo dei Comitati a livello europeo, per tutti, cfr. Savino 2005.

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760164

Nello specifico, dopo aver effettuato la ricostruzione dell'assetto organizzativo, si pone come necessario metterne in luce le relative relazioni intersoggettive, sia per quanto attiene a quelle di tipo organizzativo che a quelle concernenti i profili funzionali; invero, tale Comitato è destinato ad intrattenere 'intensi' rapporti con il CERT-EU. Inoltre, vengono in rilievo anche le relazioni con l'ENISA[2], nella direzione di un assetto destinato ad essere caratterizzato da una rilevante presenza di questi tre 'soggetti'.

Infine, suscita notevole interesse esaminare gli strumenti e le modalità attraverso le quali il Comitato è destinato ad operare. È quindi opportuno porre l'accento sul potere riconosciuto a tale 'organismo' circa la facoltà di adottare una strategia, su base pluriennale, al fine di innalzare il livello di cibersicurezza nei soggetti appartenenti all'UE. Da questo punto di vista – come si vedrà meglio più avanti – il Comitato valuta periodicamente tale strategia e, in ogni caso, è comunque tenuto a farlo ogni cinque anni, potendo altresì – ove lo dovesse reputare necessario – procedere ad una sua modifica.

Si è dinanzi ad un potere che assume particolare significato in ragione delle sue potenzialità circa la (possibile) configurazione di una regolazione strategica del CERT-EU e, di conseguenza, della cibersicurezza nel suo complesso.

La domanda di ricerca, invero, ha come obiettivo, in ultima analisi, proprio quello di tentare di riflettere attorno all'interrogativo concernente la possibilità per cui, attraverso il Comitato e i poteri di direzione nei confronti del CERT-EU che gli sono attribuiti, sulla base anche della strategia europea in materia, si vada verso una regolazione strategica della cibersicurezza, anche per il tramite di un maggior coordinamento (e, dunque, di una più efficace cooperazione) fra i vari soggetti che, a diverso titolo, sono chiamati alla regolazione di tale fenomeno[3].

L'ipotesi di partenza, infatti, è che la cibersicurezza richieda una regolazione pubblica[4] in grado di essere flessibile per meglio adattarsi ai repentini mutamenti che interessano il mondo delle tecnologie e, quindi, ai relativi attacchi informatici. La giustificazione ultima di questo modello di regolazione non può che rinvenirsi nella protezione dei diritti che da tali attacchi rischiano di essere lesi, quegli stessi diritti che, in ragione del carattere personalista[5] tanto dell'ordinamento europeo quanto delle costituzioni (di quasi tutti) i paesi che ne fanno parte, a partire da quella italiana, devono inevitabilmente rappresentare il punto di partenza di ogni riflessione in ambito giuridico.

2 Più in generale, sul ruolo delle Agenzie nell'organizzazione delle amministrazioni europee (e la loro articolazione in forma 'reticolare') cfr., per tutti, Chiti, 2002; Chiti 2009.

3 Sul punto, di recente, cfr. Camisa, Simoncini 2024.

4 In proposito, di recente, Lalli 2024. Nella prospettiva della co-regolazione, che si può considerare come una forma di regolazione intermedia tra quella privata (autoregolazione) e quella pubblica (eteroregolazione) e che sembra essere il modello regolatorio su cui si fondano sia il *Digital Markets Act* che il *Digital Services Act*, cfr. Simoncini 2022. Sul punto cfr. anche Iannuzzi 2023.

5 Cfr. Caterina 2023.

2. Composizione, funzionamento e ruolo del IICB

Per quanto attiene alla composizione del IICB, senza elencare tutte le quindici istituzioni europee che ne fanno parte[6], il regolamento prevede che, oltre alla totalità degli organi dell'UE[7], per quanto concerne i soggetti più direttamente interessati alla cibersicurezza, vi sia un rappresentante del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca, uno dell'ENISA e, infine, un rappresentante del Garante europeo della protezione dei dati (GEPD). Inoltre, sono previsti tre rappresentanti designati dalla rete delle agenzie dell'Unione (EUAN) su proposta del suo comitato consultivo TIC per difendere gli interessi degli organi e degli organismi dell'Unione che gestiscono il proprio ambiente TIC, ovviamente diversi dai soggetti espressamente elencati che hanno già, appunto, un proprio rappresentante[8]. Di conseguenza, il Comitato può contare sui quindici rappresentanti di cui sopra, ai quali si aggiungono i tre designati dall'EUAN, per un totale di diciotto membri.

Si stabilisce che ciascun componente possa farsi assistere da un supplente e che, in aggiunta ai diciotto membri, le istituzioni europee – oltre al proprio rappresentante – possano vedere invitati, da parte del presidente del Comitato, ulteriori rappresentanti allo scopo di assistere alle riunioni dello stesso Comitato, senza tuttavia che sia loro riconosciuto il diritto di voto[9]. Il Comitato è tenuto ad adottare un proprio regolamento interno[10] e a designare tra i suoi membri – conformemente allo stesso regolamento – un presidente, il cui mandato ha durata triennale[11]. Il Comitato è, inoltre, chiamato a riunirsi almeno tre volte l'anno, riunione che avviene o su iniziativa del suo presidente, o su richiesta del CERT-EU o, infine, a seguito della richiesta di uno dei componenti[12].

Per quanto riguarda, invece, il profilo relativo al diritto di voto, è previsto che ciascun membro sia titolare di un voto e che le decisioni siano adottate a maggioranza semplice, con l'eccezione di quei casi in presenza dei quali il regolamento disponga diversamente.

interessante sottolineare che il presidente non è titolare, generalmente, del diritto di voto, diritto che, tuttavia, sorge in capo ad egli allorché si presenti una situazione di parità (di voti). In questo modo, si riconosce al presidente la facoltà di esprimere quello che è, a tutti gli effetti, il voto decisivo per uscire dall'eventuale stato di impasse ed arrivare così ad una scelta[13].

6 Cfr. art. 10, par. 3, lett. *a*).

7 E cioè: Parlamento europeo, Consiglio europeo, Consiglio dell'Unione europea (o Consiglio, se si preferisce), Commissione europea, Corte di Giustizia europea, Corte dei Conti europea e Banca centrale europea.

8 Art. 10, par. 3, lett. *b*).

9 Art. 10, par. 4.

10 Art. 10, par. 6.

11 Art. 10, par. 7.

12 Art. 10, par. 8.

13 Art. 10, par. 9.

In relazione alla procedura deliberativa, si stabilisce che essa si svolga sulla base di una procedura semplificata e che la decisione finale, in assenza di obiezioni da parte di uno dei membri, sia considerata approvata entro il termine fissato dal presidente del Comitato[14].

Con riferimento, poi, ai rappresentanti nominati dall'EUAN, il regolamento stabilisce che essi trasmettano le decisioni assunte in seno al Comitato ai membri dello stesso EUAN e che a ciascuno di loro sia riconosciuta la facoltà di sottoporre ai membri nominati per far parte del Comitato o, addirittura, al presidente stesso di quest'ultimo, qualsiasi tipo di decisione che si ritenga debba essere posta all'attenzione del Comitato[15].

Un potere del Comitato che potrebbe assumere particolare rilievo è quello che consiste nella facoltà, espressamente attribuitagli, di istituire un comitato esecutivo con il compito di farsi assistere, potendo prevedere nei suoi confronti una delega sia di compiti che di poteri[16].

Rispetto invece al resoconto – e quindi al relativo conseguente controllo – dell'attività svolta dal Comitato, il legislatore ha disposto che quest'ultimo, entro l'8 gennaio 2025 e, successivamente, con cadenza annuale, presenti tanto al Parlamento quanto al Consiglio una relazione illustrativa dei progressi compiuti in punto di attuazione del presente regolamento; inoltre, si stabilisce che tale relazione debba precisare la tipologia di cooperazione intrattenuta dal CERT-EU "con i suoi omologhi degli Stati membri in ciascuno Stato membro". La relazione così definita – si legge – "costituisce un contributo alla relazione sullo stato della cibersicurezza nell'Unione adottata a norma dell'articolo 18 della direttiva (UE) 2022/2555"[17].

Esaminata la composizione dell'istituito Comitato, preme soffermare ora l'attenzione sul profilo attinente ai compiti che il legislatore europeo ha inteso attribuirgli. Coerentemente alla previsione del duplice compito – già ricordato – consistente, da un lato, nel controllare e sostenere l'attuazione del presente regolamento da parte dei soggetti dell'UE e, dall'altro, nel vigilare sull'attuazione delle priorità, nonché degli obiettivi di tipo generale da parte del CERT-EU, e imprimere a quest'ultimo una direzione definita espressamente come 'strategica', si prevede – per quello che qui più interessa e, dunque, con particolare riguardo al CERT-EU – anzitutto che esso fornisca orientamenti al direttore del CERT-EU e che, con riferimento al compito di vigilare e sostenere l'attuazione del regolamento, sostenga i soggetti dell'UE nel compito nient'affatto agevole ma, ciò nonostante, fondamentale, in relazione all'opera di rafforzamento del loro livello di cibersicurezza[18], anche, se del caso, mediante la facoltà di richiedere relazioni *ad hoc* ai soggetti dell'UE e

14 Art. 10, par. 11.
15 Art. 10, par. 12.
16 Art. 10, par. 13.
17 Art. 10, par. 14.
18 Sulla qualificazione della 'robustezza dei sistemi informatici' come interesse pubblico, cfr. Brighi, Chiara 2021: 26-27.

allo stesso CERT-EU. Inoltre, il regolamento attribuisce a tale Comitato, previa discussione strategica, il potere di adottare una strategia, su base pluriennale, che abbia quale fine ultimo quello di innalzare il livello di cibersicurezza nei soggetti dell'UE, e ciò – come già anticipato – mediante una valutazione periodica di tale strategia, essendo comunque in ogni caso tenuta ad analizzarla ogni cinque anni, potendo sempre, ove lo dovesse reputare necessario, procedere ad una sua modifica.

Quest'ultimo compito, unitamente ai poteri di direzione strategica di cui il Comitato è titolare, rappresenta un aspetto fondamentale per affrontare il profilo – come si tenterà di spiegare più avanti – relativo all'ipotesi di una regolazione di tipo strategico della cibersicurezza.

Un altro compito rilevante che il legislatore ha attribuito al Comitato è quello concernente il potere di approvare, sulla base di una proposta avanzata dal presidente del CERT-EU, il programma di lavoro annuale di quest'ultimo, controllandone la relativa attuazione. Allo stesso modo, rivestono importanza i poteri di approvazione – sempre sulla base del medesimo meccanismo da ultimo descritto – della pianificazione finanziaria annuale delle entrate e delle spese (comprese quelle in materia di personale), per le attività proprie del CERT-EU, nonché della relazione annuale elaborata dal presidente del CERT-EU avente ad oggetto sia le attività di quest'ultimo che la relativa gestione dei fondi.

Infine, preme evidenziare altri tre poteri che, per quanto non direttamente collegati con il CERT-EU, presentano profili di sicuro interesse ai fini del presente scritto.

Invero, la facoltà riconosciuta al Comitato circa l'istituzione di gruppi di consulenza tecnica con l'obiettivo di farsi assistere nello svolgimento della propria attività, approvando il loro operato, oltre a designarne i relativi presidenti, rappresenta un potere di peculiare importanza poiché consente al Comitato di dotarsi delle necessarie specifiche conoscenze (in punto di cibersicurezza) che sono fondamentali affinché possa svolgere efficacemente i propri compiti. Il secondo potere attiene, invece, alla valutazione dei documenti e delle relazioni presentate dai soggetti dell'UE sulla base di quanto previsto dal presente regolamento come, per esempio, quelle concernenti le c.d. 'valutazioni di maturità' della cibersicurezza. Infine, il Comitato istituisce un piano relativo alla gestione delle crisi informatiche con la duplice finalità di sostenere – anzitutto sotto il profilo operativo – la gestione coordinata degli incidenti più gravi che possono colpire i soggetti dell'UE, da una parte, e, dall'altra, di contribuire al regolare scambio delle informazioni necessarie, avuto particolare riguardo all'impatto nonché all'entità di siffatti incidenti, oltre che ai possibili modi per (quantomeno) attenuarne i relativi effetti.

3. I nuovi compiti del CERT-EU e l'importanza della cooperazione

Il regolamento (UE) 2023/2841, oltre a dettare misure per un livello più elevato di cibersicurezza nei soggetti dell'UE e a prevedere l'istituzione del IICB, amplia i

compiti del CERT-EU[19]. Invero, dopo averne mutato la denominazione[20], si stabiliscono disposizioni precise circa la sua organizzazione nonché il relativo funzionamento e, più in generale, in merito alla sua operatività.

Si afferma anzitutto che la missione del CERT-EU consiste nel contribuire alla sicurezza dell'ambiente TIC (che non sia riservato) di tutti i soggetti dell'UE e ciò avviene fornendo loro un'attività di consulenza in materia di cibersicurezza che si manifesta anche mediante un aiuto rispetto alla prevenzione ed al rilevamento degli incidenti, aiuto che consiste anche ovviamente nell'affrontare (o comunque attenuare) siffatti incidenti. Il CERT-EU, per questi soggetti, secondo il legislatore europeo, deve assumere il ruolo di una piattaforma in grado di scambiare le informazioni sulla cibersicurezza ed assicurare il coordinamento della risposta in caso di incidenti[21].

Per fare ciò il CERT-EU raccoglie, gestisce, analizza e condivide informazioni con i soggetti dell'UE in relazione alle minacce informatiche, le vulnerabilità e gli incidenti che riguardano le infrastrutture TIC. Inoltre, svolge un'azione di coordinamento delle risposte agli incidenti a livello tanto interistituzionale quanto a livello di soggetti dell'UE, e ciò anche attraverso un'attività che sia in grado di fornire e/o coordinare un'assistenza operativa di tipo specialistico[22].

Il legislatore detta poi i compiti del CERT-EU necessari per assistere i soggetti dell'UE[23] nonché le modalità attraverso le quali contribuire all'attuazione del presente regolamento.

Con riferimento ai primi, fra i tanti – per quello che qui più interessa – merita richiamare i servizi CSIRT standard che offre ai soggetti dell'UE mediante un pacchetto di servizi di cibersicurezza che sono espressamente descritti nel proprio catalogo di servizi (c.d. 'servizi base')[24], così come rilevante è il potere di richiamare l'attenzione del IICB rispetto a qualsiasi tipo di problema concernente l'attuazione del presente regolamento e degli indirizzi, delle raccomandazioni e degli inviti a intervenire[25]. Anche la possibilità di una stretta cooperazione con l'ENISA sulla base delle informazioni raccolte di cui sopra[26] costituisce un potere rilevante che va nella direzione, giustappunto, di un maggiore coordinamento nel 'governo'

19 La stessa Commissione europea, attraverso un comunicato, ha affermato che il regolamento (UE) 2023/2841 prevede un mandato ampliato del CERT-EU sul presupposto per cui si tratti di un polo di scambio di informazioni nonché coordinamento della risposta agli incidenti, un organo, cioè, con funzioni consultive istituito a livello centrale e fornitore di servizi.

20 La nuova denominazione, secondo quanto previsto dal punto 19 dei *Considerando*, dovrebbe essere "Servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione"; tuttavia, allo scopo di facilitarne il riconoscimento, sembra destinata a mantenere l'attuale acronimo.

21 Art. 13, par. 1.

22 Art. 13, par. 2.

23 Si tratta di compiti espressamente previsti all'art. 13, par. 3.

24 Art. 13, par. 3, lett. *b*).

25 Art. 13, par. 3, lett. *d*).

26 Art. 13, par. 3, lett. *e*).

della cibersicurezza[27] che, in questo caso, passa attraverso una inevitabile serrata interlocuzione con il soggetto che, a livello europeo, è preordinato a configurare le condizioni per un elevato livello comune di cibersicurezza. Inoltre, il CERT-EU ha il compito fondamentale di coordinare la gestione degli incidenti ritenuti gravi[28].

Per quanto concerne il profilo della cooperazione, si specifica che il CERT-EU può cooperare con le competenti autorità di cibersicurezza all'interno dell'UE (e dei suoi Stati membri) anche negli ambiti relativi: *i*) alla preparazione, al coordinamento (in caso di incidente), allo scambio di informazioni e risposta alle crisi che si sono verificate a livello tecnico rispetto a casi che hanno coinvolto soggetti dell'UE; *ii*) alla cooperazione operativa per quanto concerne la rete CSIRT (compresa l'assistenza reciproca); *iii*) all'*intelligence* che riguarda le minacce informatiche, fra le quali il legislatore fa rientrare anche la c.d. 'consapevolezza situazionale'; *iv*) a qualsiasi aspetto che richieda le competenze di tipo tecnico in materia di cibersicurezza proprie dello stesso CERT-EU[29]. Inoltre, quest'ultimo, nell'ambito delle sue competenze, intraprende una cooperazione (espressamente definita dal legislatore come "strutturata") con l'ENISA allo scopo di sviluppare capacità, una cooperazione di tipo operativo nonché analisi strategiche di lungo periodo rispetto alle minacce informatiche (secondo quanto disposto dal regolamento (UE) 2019/881). Il CERT-EU può altresì contare su una cooperazione, e conseguente scambio di informazioni, con il Centro per la lotta alla criminalità informatica di Europol[30].

Un ulteriore profilo, che si interseca con l'aspetto relativo alla cooperazione, attiene ai poteri riconosciuti al CERT-EU al fine di concorrere all'attuazione del regolamento (UE) 2023/2848. Il legislatore europeo attribuisce a tale organismo il potere di predisporre inviti ad intervenire il cui contenuto ha ad oggetto la descrizione delle misure di sicurezza urgenti che i soggetti dell'UE sono chiamati ad adottare nel termine prestabilito[31]. Inoltre, il CERT-EU può avanzare proposte al IICB per indirizzi destinati o a tutti i soggetti dell'UE ovvero solamente ad una parte di essi[32], nonché raccomandazioni – sempre rispetto al Comitato appena richiamato – da effettuare nei confronti di singoli soggetti dell'UE[33].

Prima di passare al profilo delle relazioni intersoggettive merita rapidamente analizzare il contenuto di tali indirizzi e regolamenti per mettere così in luce la tipologia di apporto che può derivare dal CERT-EU nell'opera di attuazione del presente regolamento. Il contenuto di questi atti, secondo quanto disposto, può prevedere, fra l'altro, metodologie comuni nonché un modello in grado

27 Sul punto, di recente, cfr. Moroni 2024; Giupponi 2024.

28 Art. 13, par. 3, lett. *f*).

29 Art. 13, par. 4, lett. *a*), *b*), *c*) e *d*).

30 Art. 13, par. 5. Sulla criminalità informatica, per un inquadramento generale, cfr. Pietropaoli 2022.

31 Art. 14, par. 1, lett. *a*), con l'aggiunta della previsione per cui il soggetto dell'UE interessato – dopo aver ricevuto l'invito ad adottare le misure di sicurezza urgenti ritenute necessarie – è tenuto tempestivamente ad informare il CERT-EU su come ha applicato le misure di sicurezza suggerite.

32 Art. 14, par. 1, lett. *b*).

33 Art. 14, par. 1, lett. *c*).

di valutare la maturità della cibersicurezza dei soggetti dell'UE[34], così come le modalità (o, comunque, i miglioramenti) che concernono la gestione dei rischi per la cibersicurezza e le relative misure di gestione dei rischi ad essa connessi[35]. Inoltre, tali indirizzi e raccomandazioni possono indicare anche le modalità afferenti alle valutazioni circa il livello di maturità della cibersicurezza[36] e gli accordi di condivisione delle informazioni sulla cibersicurezza[37], previsti dall'art. 20 del presente regolamento.

Per quanto riguarda più nel dettaglio l'aspetto relativo alla cooperazione, il regolamento (UE) 2023/2848 detta una serie di disposizioni aventi ad oggetto, da un lato, il profilo della cooperazione tra il CERT-EU e gli omologhi degli Stati membri e, dall'altro, la cooperazione fra il CERT-EU e gli omologhi diversi ed ulteriori dagli Stati membri.

Rispetto al primo versante, il CERT-EU è tenuto a cooperare e scambiare informazioni, senza ingiustificato ritardo, con gli omologhi degli Stati, giustappunto; più precisamente, il legislatore stabilisce che tale cooperazione e scambio di informazioni avvenga con gli CSRIT[38], ovvero, se necessario, con le autorità competenti e i c.d. 'punti di contatto unici'[39]. L'oggetto di ciò è rappresentato da incidenti, minacce informatiche, vulnerabilità, quasi incidenti, oltre che dalle possibili contromisure e le c.d. '*best practices*' e, più in generale, tutte le questioni ritenute pertinenti per migliorare la protezione degli ambienti TIC di tutti i soggetti dell'UE, e ciò anche per mezzo della rete CSIRT[40], istituita – lo si ricorda – al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri (c.d. 'rete dei CSIRT nazionali')[41].

Coerentemente con tale previsione si prevede poi che il CERT-EU comunichi tempestivamente agli omologhi pertinenti dello Stato in questione[42] l'incidente significativo di cui è venuto a conoscenza[43].

34 Art. 14, par. 2, lett. *a*).

35 Art. 14, par. 2, lett. *b*).

36 Art. 14, par. 2, lett. *c*). A tali valutazioni il regolamento (UE) 2023/2840 dedica un apposito articolo (7).

37 Art. 14, par. 2, lett. *f*).

38 Il riferimento è ai Team di risposta agli incidenti di sicurezza informatica (CSIRT) istituiti a norma dell'art. 10 della direttiva (UE) 2022/2555.

39 Punto di contatto che, secondo quanto disposto dall'art. 8 della direttiva (UE) 2022/2555, svolge una funzione di collegamento al fine di garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con quelle pertinenti degli altri Stati membri e, ove ritenuto opportuno, anche con la Commissione e l'ENISA; inoltre, al punto di contatto è attribuito il compito di garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro. Si ricorda, altresì, che tale disposizione prevede anche che, allorché uno Stato abbia designato solamente una autorità competente responsabile della cibersicurezza e dei relativi compiti di vigilanza, quella stessa autorità assuma pure il ruolo di punto di contatto (par. 3).

40 Art. 17, par. 1.

41 Il riferimento è all'art. 15 della direttiva (UE) 2022/2555 rubricato Rete CSIRT.

42 Ossia lo Stato nel cui territorio si è verificato l'incidente significativo.

43 Art. 17, par. 2.

Il legislatore europeo attribuisce al CERT-EU il potere di scambiare, "senza indebito ritardo" – così si legge – specifiche informazioni circa gli incidenti con i soggetti omologhi degli Stati membri allo scopo di facilitare il rilevamento delle minacce informatiche o degli incidenti analoghi e, più in generale, per poter fornire il proprio contributo rispetto all'analisi di quel determinato incidente, senza che sia necessario ricevere preventivamente la relativa autorizzazione da parte del soggetto dell'UE interessato. Per quanto concerne, invece, lo scambio di informazioni specifiche che abbiano ad oggetto la rivelazione dell'identità del bersaglio dell'incidente di cibersicurezza, il CERT-EU lo può fare solo a determinate condizioni, tipizzate dal legislatore: *i*) il soggetto dell'UE interessato deve rilasciare il proprio consenso; *ii*) il soggetto dell'UE interessato (cioè oggetto dell'incidente) non vi acconsente ma, tuttavia, la diffusione della sua identità avrebbe quale effetto quello di aumentare la probabilità di evitare o, comunque, attenuare ulteriori incidenti altrove[44]; *iii*) il soggetto dell'UE interessato dall'incidente ha già pubblicizzato il proprio coinvolgimento[45].

In relazione al profilo della cooperazione con gli altri omologhi, il legislatore specifica anzitutto che tale cooperazione con questi soggetti possa avvenire, purché essi rispettino i requisiti dell'UE in materia di cibersicurezza, precisando altresì che vi rientrano anche gli omologhi di specifici settori.

L'oggetto della cooperazione, in questi casi, attiene agli strumenti e ai metodi (come, per esempio, le tecniche, le tattiche, le procedure e le *best practices*) nonché alle minacce informatiche ed alle vulnerabilità. È richiesta l'approvazione preventiva da parte del IICB per poter procedere a qualsiasi tipo di cooperazione con i soggetti previsti e tale approvazione deve avvenire caso per caso. Una volta istituita questa cooperazione, il CERT-EU è tenuto ad informare gli omologhi dello Stato membro nel cui territorio si trova il soggetto con cui si è intrapresa siffatta cooperazione. Si stabilisce, inoltre, che tale cooperazione possa eventualmente inverarsi anche mediante accordi di riservatezza nella forma dei contratti e/o degli accordi amministrativi[46].

È importante sottolineare come ulteriori forme di cooperazione possano essere intrattenute, da parte del CERT-EU, con una serie di partner come, ad esempio, i soggetti commerciali (compresi quelli che appartengono a specifici settori), le or-

44 Il legislatore stabilisce, in questo caso, che le decisioni di scambiare informazioni siano avallate dal direttore del CERT-EU, descrivendone poi l'intera procedura.

45 Art. 17, par. 3.

46 Secondo quanto disposto dall'art. 18, par. 1, tali accordi di riservatezza non debbono essere preventivamente approvati ad opera del Comitato interistituzionale, pur dovendo, tuttavia, avvisare il suo presidente. Se dovesse ricorrere una situazione di imminente ed urgente necessità di scambiare informazioni circa la cibersicurezza nell'interesse dei soggetti dell'UE (o anche di altri soggetti), è possibile procedere a tale scambio purché questo avvenga con un soggetto dotato di competenze, capacità e conoscenze specifiche ritenute necessarie per far fronte a tale situazione di urgenza e ciò può verificarsi anche qualora il CERT-EU non abbia stipulato un accordo di riservatezza con tale soggetto; in questi casi, però, è richiesto al CERT-EU di procedere ad una comunicazione immediata al presidente del Comitato e di tenere informato lo stesso Comitato mediante relazioni e/o riunioni periodiche.

ganizzazioni internazionali, nonché enti nazionali di Stati non appartenenti all'UE o, addirittura, singoli esperti. Tale cooperazione, prevede il legislatore, è funzionale alla raccolta di informazioni riguardo a minacce informatiche (siano esse generali, siano esse specifiche), quasi incidenti, vulnerabilità e possibili contromisure. Se si ritiene opportuna una cooperazione di più ampia portata con tali soggetti è necessario che il CERT-EU chieda, caso per caso, un'approvazione preventiva al Comitato interistituzionale[47]. Inoltre, il CERT-EU, una volta ricevuto il consenso da parte del soggetto dell'UE interessato dall'incidente, e a condizione che sussista un accordo di non divulgazione con il soggetto omologo o con il partner interessato[48], può fornire ad essi le informazioni relative allo specifico incidente, e ciò con la sola giustificazione di contribuire alla sua analisi[49].

Un ultimo profilo su cui preme soffermare l'attenzione è quello concernente gli accordi di condivisione delle informazioni sulla cibersicurezza. Invero, com'è evidente, si tratta di un aspetto di particolare rilevanza – da salutare con favore al netto di una parziale 'timidezza' del legislatore, come si dirà – che va nella direzione di un rafforzamento del livello di cibersicurezza nei soggetti dell'UE, aumentando in questo modo la capacità di risposta dell'UE dinanzi agli attacchi informatici.

Il legislatore dispone, infatti, che i soggetti dell'UE, su base volontaria, possano notificare e fornire informazioni al CERT-EU in merito agli incidenti, alle minacce informatiche, ai quasi incidenti ed alle vulnerabilità che li interessano. Il CERT-EU è, a sua volta, tenuto a garantire la disponibilità di efficaci mezzi di comunicazione, dotati di un livello di tracciabilità, riservatezza e affidabilità elevati, proprio per rendere più agevole lo scambio e, soprattutto, la condivisione delle informazioni con i soggetti sopra menzionati. Si detta poi una specificazione nient'affatto irrilevante che incide sull'operatività dello stesso CERT-EU; infatti, si prevede che quest'ultimo, nel trattare le notifiche pervenutegli, possa dare priorità a quelle obbligatorie, prendendo successivamente in considerazione le notifiche volontarie. In relazione a quest'ultima tipologia di notifica, il legislatore afferma che – salvo ovviamente il caso delle notifiche derivanti dal controllo del IICB circa l'osservanza del presente regolamento[50] – esse non debbono comportare, per il soggetto che le effettua, nessun tipo di obbligo ulteriore rispetto a quelli a cui è già sottoposto abitualmente[51].

Inoltre, si riconosce al CERT-EU il potere di chiedere ai soggetti dell'UE le informazioni "tratte dai loro rispettivi inventari dei sistemi TIC", incluse quelle relative alle minacce informatiche, ai quasi incidenti, alle vulnerabilità, nonché quelle attinenti ai c.d. 'indicatori di compromissione', agli allarmi di cibersicurezza ed alle raccomandazioni che riguardano la configurazione stessa degli strumenti di cibersicurezza, per poterne così rilevare gli incidenti. Il soggetto che riceve la domanda

47 Art. 18, par. 2.
48 Il riferimento è ai soggetti di cui ai paragrafi 1 e 2 dell'art. 18.
49 Art. 18, par. 3.
50 Il riferimento è all'art. 10.
51 Art. 20, par. 1.

di trasmissione delle informazioni è tenuto ad inviarla senza ritardo, così come gli è richiesto di procedere ad ogni loro eventuale successivo aggiornamento[52].

Si tratta, com'è agevole intuire (e come chiarisce, del resto, il legislatore), di un potere che, in ultima analisi, è imprescindibile per il CERT-EU affinché sia in grado di realizzare i compiti che gli sono stati espressamente attribuiti mediante il regolamento in esame.

Anche le informazioni specifiche circa un determinato incidente che rivelano l'identità stessa del soggetto dell'UE coinvolto nell'incidente possono essere oggetto di scambio, purché sussista il consenso di quest'ultimo; il quale può pure rifiutarsi di prestare il proprio consenso, essendo tuttavia tenuto in tal caso a spiegare al CERT-EU le ragioni alla base del suo diniego[53].

Si stabilisce poi, da un lato, che i soggetti dell'UE condividano sia con il Parlamento europeo che con il Consiglio, su loro richiesta, le informazioni riguardanti il completamento dei piani di cibersicurezza[54], quegli stessi piani rispetto ai quali il presente regolamento dedica un'apposita disposizione e, dall'altro, similmente, che il CERT-EU ovvero il IICB (a seconda dei casi), condividano – sempre con i due organi appena menzionati e sempre previa richiesta – indirizzi, raccomandazioni ed inviti ad agire[55].

4. (*Segue*). Le relazioni intersoggettive e l'esigenza di coordinamento

Il profilo relativo al coordinamento riveste notevole importanza poiché – come noto, ed in parte visto – molteplici sono i soggetti a livello europeo (e, quindi, a livello nazionale) chiamati, a vario titolo, a concorrere a quello che si può qui definire nei termini di 'governo della cibersicurezza'. Pertanto, appare necessario riflettere circa le relazioni che sussistono fra tali soggetti e su come si possa assicurare il coordinamento fra di loro, strumentale a configurare un sistema realmente in grado di regolare la cibersicurezza ed aumentarne il relativo livello nei soggetti dell'UE, che si rende tanto più necessario proporzionalmente all'aumentare sia degli attacchi informatici che del loro grado di raffinatezza.

Ai presenti fini interessa, in particolare, tentare di delineare le relazioni che sussistono fra il IICB, il CERT-EU e l'ENISA. Da questo punto di vista, si può prendere in considerazione il coordinamento (e conseguente cooperazione) che il legislatore europeo, con il presente regolamento, ha inteso prevedere rispetto alla risposta in caso di incidenti.

Il CERT-EU, infatti, svolgendo una funzione analoga a quella di una piattaforma creata per lo scambio di informazioni in materia di cibersicurezza e susseguente coordinamento della risposta allorché si verifichi un incidente, è tenuto a rendere più agevole la circolazione delle informazioni attinenti agli incidenti, alle minacce

52 Art. 20, par. 2.
53 Art. 20, par. 3.
54 Art. 20, par. 4.
55 Art. 20, par. 5.

informatiche, alle vulnerabilità e ai quasi incidenti. Questa circolazione – si legge – deve avvenire fra i soggetti dell'UE nonché con i soggetti omologhi degli Stati membri dell'UE (quelli previsti dall'art. 17 per intendersi) e gli altri soggetti omologhi (quelli di cui all'art. 18)[56].

Il CERT-EU può facilitare tale coordinamento fra i soggetti dell'UE in materia di risposta agli incidenti anche per mezzo di una stretta cooperazione con l'ENISA e, per fare ciò, può ricorrere ad una serie di 'strumenti' come, a titolo di esempio, il sostegno reciproco mediante la condivisione delle informazioni ritenute pertinenti per i soggetti dell'UE ovvero attraverso la fornitura di assistenza[57]. Sempre potendo ricorrere ad una stretta cooperazione con l'ENISA, il CERT-EU sostiene i soggetti dell'UE con riferimento alla 'consapevolezza situazionale' degli incidenti, delle minacce, delle vulnerabilità e dei quasi incidenti. Inoltre, il CERT-EU condivide gli sviluppi che si sono prodotti nel settore della cibersicurezza[58].

Nell'attività di coordinamento di tali incidenti un ruolo importante è attribuito anche al IICB perché è a questi che spetta il compito – sulla base di una proposta del CERT-EU – di adottare gli atti e gli indirizzi sul coordinamento della risposta in caso di incidenti, oltre che sulla cooperazione allorché si verifichino incidenti più gravi. Il CERT-EU, inoltre, è tenuto a fornire una consulenza rispetto a come debba essere segnalato l'incidente alle autorità competenti, segnalazione che deve avvenire senza ritardo e che è la conseguenza di un incidente rispetto al quale sussiste un sospetto circa la sua rilevanza ai termini della legge penale[59].

Ancora più evidente è la cooperazione fra i tre soggetti in questione se si esamina la disposizione inerente la gestione degli incidenti più gravi. Invero, in questo caso, si ha una più stretta relazione fra il IICB da un lato e il CERT-EU e l'ENISA dall'altro; il primo, come già anticipato, ha il potere di istituire un piano di gestione delle crisi informatiche per far fronte agli incidenti e ciò avviene in stretta cooperazione – così si legge – con il CERT-EU e l'ENISA[60]. Anche in tali casi il soggetto deputato al coordinamento è sempre il CERT-EU, il quale è chiamato altresì ad assistere proprio il IICB nel coordinamento di quegli stessi piani a cui si è appena fatto riferimento[61].

Più in generale, si può osservare come il Comitato, nei confronti del CERT-EU – lo si vedrà meglio più avanti – abbia un potere sia di vigilanza, dato che ne controlla costantemente l'attuazione delle priorità e degli obiettivi, che di natura direttiva, potendo infatti imprimere a quest'ultimo – lo si è già anticipato – una "direzione strategica". Il Comitato è, dunque, titolare di un rilevante potere di coordinamento del CERT-EU che si esplica anche mediante la facoltà di fornire orientamenti al suo direttore. Con riferimento, invece, ai rapporti con l'ENISA, il Comitato può farsi sostenere da essa nell'opera di scambiare le *best practices* nonché le informa-

56 Art. 22, par. 1.
57 Art. 22, par. 2.
58 Art. 22, par. 3.
59 Art. 22, par. 4.
60 Art. 23, par. 1.
61 Art. 23, par. 3.

zioni relative all'attuazione del regolamento (UE) 2023/2848. Inoltre, come visto, l'ENISA è rappresentata in seno al Comitato e ciò proprio in ragione del suo ruolo quale centro di competenza in materia di cibersicurezza e del sostegno che, più in generale, tale autorità fornisce ai soggetti dell'UE.

Sussistono poi rapporti diretti fra CERT-EU e ENISA. Il primo, infatti, dovrebbe avvalersi delle competenze dell'ENISA sulla base di quella cooperazione strutturata sancita espressamente dal regolamento (UE) 2019/881, dove, per converso, si prevede che quest'ultima si avvalga delle competenze, sia tecniche che operative, disponibili del CERT-EU, attraverso, appunto, tale cooperazione strutturata, cooperazione che potrebbe fondarsi sulle competenze proprie dell'ENISA, con la possibilità (anche) di ricorrere ad accordi fra i due soggetti allo scopo di definire l'attuazione in concreto di questa forma di cooperazione ed evitare così la duplicazione delle relative attività[62].

Il regolamento (UE) 2023/2841 ricorda, infatti, la possibilità di definire accordi fra tali due soggetti, sottolineando, in particolare, la cooperazione che il CERT-EU potrebbe instaurare con l'ENISA in punto di analisi delle minacce, condividendo con quest'ultima (con cadenza periodica) la sua relazione avente ad oggetto la panoramica in tema di minacce[63].

Emerge, dunque, in maniera piuttosto evidente, l'esigenza di coordinamento[64] fra questi tre soggetti che, a vario titolo, concorrono al governo della cibersicurezza ed alla loro regolazione, nella direzione del rafforzamento del livello complessivo di cibersicurezza nei soggetti dell'UE.

Il IICB si inserisce in un assetto che già vedeva la presenza sia del CERT-EU che dell'ENISA e, proprio in virtù della sua organizzazione che è preordinata a rappresentare tutti i soggetti dell'UE in qualche misura interessati alla (e dalla) cibersicurezza, rafforza tale assetto mediante la capacità di coordinamento che le è propria.

Si potrebbe, pertanto, configurare una sorta di 'triade' nel governo e quindi nella regolazione della cibersicurezza, dove, accanto all'ENISA e al CERT-EU, si affianca ora il Comitato[65]. L'ENISA continua a svolgere il suo ruolo tradizionale di soggetto che, anzitutto, è chiamato a "conseguire un elevato livello comune di cibersicurezza in tutta l'UE, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'UE nel miglioramento della cibersicurezza". Il CERT-EU, anche in ragione dei maggiori compiti e del rafforzamento organizzativo recentemente operato dal legislatore europeo, costituisce – per così dire – il 'braccio armato' sia dell'ENISA che del Comitato, svolgendo un ruolo prevalentemente operativo, fondamentale al contrasto e, prima ancora, alla prevenzione degli attacchi informatici.

Il Comitato, in tutto ciò, rappresenta uno strumento di particolare importanza poiché mira a definire un livello (elevato) di cibersicurezza comune tra i sogget-

62 Punto 33 dei *Considerando* del regolamento (UE) 2019/881.

63 Punto 32 dei *Considerando*.

64 Sull'importanza del coordinamento quale metodo "aperto" fra il piano europeo e quello nazionale cfr. Del Gatto 2012.

65 Si potrebbe parlare, da questo punto di vista, di una sorta di "arcipelago amministrativo".

ti dell'UE, sul presupposto per cui, avendo il regolamento anche l'obiettivo di rafforzare il livello complessivo di cibersicurezza dell'UE – coerentemente con quanto già previsto dalla direttiva (UE) 2022/2555 –, tale rafforzamento debba riguardare tutti i soggetti dell'UE in maniera uniforme ed indiscriminata. Invero – come ricorda lo stesso legislatore – gli ambienti TIC di quest'ultimi sono fortemente interdipendenti fra loro[66], cosicché qualsiasi attacco ad un soggetto potrebbe avere effetti assai dannosi anche su uno o più degli altri soggetti appartenenti all'UE.

In altre parole, il rafforzamento del livello di cibersicurezza dei soggetti all'interno dell'UE deve riguardarli tutti, altrimenti rischia di essere un'operazione vana, fine a sé stessa, che dinanzi ad un attacco informatico di vaste dimensioni e raffinata sofisticatezza potrebbe mandare in tilt l'intero sistema (informatico) europeo e pregiudicare così i diritti da esso dipendenti.

5. La direzione strategica del CERT-EU ed un nuovo potenziale modello regolatorio all'orizzonte

Il potere del Comitato di vigilare in relazione alla realizzazione delle priorità nonché degli obiettivi generali del 'CERT-EU', con la possibilità di imprimere a tale centro una direzione di tipo strategico, offre interessanti spunti per riflettere sul modello regolatorio della cibersicurezza che va delineandosi[67]. Invero, avuto particolare riguardo alla possibilità di imprimere al CERT-EU una direzione di tipo strategico, sembra aprirsi la strada per un modello di regolazione della cibersicurezza che si può definire nei termini di 'regolazione strategica'. Come noto, infatti, nel 2020 è stata adottata la strategia sulla cibersicurezza[68], con l'obiettivo di configurare una rete internet globale ed aperta, contraddistinta da linee guida per poter affrontare i rischi sia per la sicurezza che per i diritti e le libertà fondamentali dei cittadini dell'UE. La strategia definisce, quindi, in quale modo l'UE proteggerà i suoi cittadini, le imprese e le istituzioni dalle minacce informatiche, come promuoverà la cooperazione internazionale e, infine, secondo quali azioni contribuirà a garantire una rete internet globale ed aperta.

In questa sede non interessa analizzare la strategia in sé quanto, diversamente, mettere in luce come essa possa costituire il substrato per configurare il modello di regolazione di tipo strategico. Tale strategia, lo si ricorda, si colloca in quel variegato panorama di documenti europei – composto dal documento "Plasmare il futuro

66 Utilizzano, infatti, flussi di dati integrati e, inoltre, sono accomunati dalla circostanza di essere caratterizzati da una stretta collaborazione fra i loro utenti.

67 Sul punto, con specifico riguardo alla regolazione delle piattaforme digitali, dove si effettuano osservazioni (circa i diversi modelli regolatori) in grado di offrire spunti utili per la configurazione del modello regolatorio della cibersicurezza, secondo una prospettiva che muove dal presupposto della necessità di considerare l'intero sistema digitale come l'oggetto (e, quindi, l'ambito) dei nuovi modelli di regolazione delle piattaforme, cfr. Santaniello 2021.

68 JOIN (2020) 18 final.

digitale dell'Europa"[69], dal piano per la ripresa europea della Commissione[70], dalla strategia per l'Unione della sicurezza 2020-2025[71] e, infine, dalla strategia globale per la politica estera e di sicurezza dell'Unione europea – e mira ad esserne, come si legge, "una componente chiave".

Il Comitato, si è detto, imprime al CERT-EU una direzione strategica attraverso i compiti che gli sono espressamente assegnati dal legislatore. Di particolare rilievo sotto questo profilo sono, fra gli altri, il potere di fornire orientamenti al direttore del CERT-EU e il potere di approvare il suo programma di lavoro annuale, controllandone la relativa attuazione. Il Comitato, lo si ricorda, adotta una strategia pluriennale al fine di innalzare il livello di cibersicurezza nei soggetti dell'UE, a cui si accompagna una sua valutazione periodica e, soprattutto, la possibilità di procedere ad una sua modifica.

Si tratta, pertanto, di una regolazione che sembra essere una 'regolazione strategica', vale a dire una regolazione che si fonda anzitutto su una strategia, senza per questo essere però caratterizzata da misure specifiche individuate *ex ante* dal legislatore. Non è la regolazione tradizionale conosciuta dal diritto amministrativo in passato e, più in generale, dal diritto della regolazione, quella cioè che si basava su strumenti di c.d. '*command and control*', dove non c'era una strategia alla base e le misure della regolazione erano specificamente (e preventivamente) previste dal legislatore.

L'obiettivo della regolazione di questo tipo consiste nell'attuazione della strategia: è questa che fissa il macro-obiettivo (che, in tal caso, è, appunto, quello di innalzare il livello di cibersicurezza nei soggetti dell'UE) e la regolazione è lo strumento che serve per attuarlo in concreto. Si è in presenza di una regolazione flessibile poiché è la stessa strategia che si può aggiornare periodicamente e, di conseguenza, è una regolazione caratterizzata da un possibile mutamento in punto di strumenti di cui servirsi per conseguire l'obiettivo finale (questo, in teoria, non flessibile); essi, infatti – lo si ripete –, non sono predeterminati dal legislatore.

Tale modello regolatorio ha degli elementi in comune con la c.d. 'regolazione persuasiva', la quale, non a caso, "si definisce in relazione agli obiettivi piuttosto che agli strumenti"[72]. Invero, è l'obiettivo stabilito dalla strategia che contraddistingue e caratterizza la regolazione flessibile. La regolazione persuasiva è, del resto, una regolazione flessibile, una regolazione che – come è stato osservato – "può consentire una maggiore rapidità nell'adattamento alle acquisizioni della scienza"[73].

Ciò detto, la regolazione strategica non è necessariamente – e non deve essere – una regolazione per così dire '*soft*', 'debole', potendo, al contrario, essere una regolazione 'forte'. La sua 'forza' (nel senso di vincolatezza) dipende sia dal tasso di ambizione degli obiettivi posti che dai termini prefissati entro i quali conseguire siffatti obiettivi, oltre che, ovviamente, dagli strumenti utilizzati.

69 COM(2020) 67 final.
70 COM(2020) 98 final.
71 COM(2020) 605 final.
72 Cafaggi, 2022: 494.
73 Cafaggi, 2022: 521.

Tale modello di regolazione è – e non potrebbe essere altrimenti – multilivello e deve necessariamente superare l'attuale situazione caratterizzata da un eccesso di norme, la cui causa è da rinvenire (anche) in quel fenomeno che assume il nome di 'normazione policentrica'. All'opposto, le norme devono essere quelle strettamente necessarie al raggiungimento dell'obiettivo fissato dal legislatore nelle varie strategie. L'orizzonte della regolazione multilivello è indispensabile in ragione della rilevanza globale del fenomeno della cibersicurezza e, perciò, è essenziale il coinvolgimento del livello sovra-europeo. Per quanto riguarda invece il discorso circa l'esigenza di superare l'eccesso di norme, ciò dipende dal continuo e rapido mutamento delle tecnologie e, quindi, degli attacchi informatici; un numero elevato di norme mal si presterebbe alla prevenzione ed al contrasto di tali attacchi, anche perché la promulgazione di esse richiede un lasso di tempo, a partire dalla loro formulazione[74], che difficilmente consentirebbe la prevenzione dei rischi informatici, oltre che per il fatto che, comunque, un eccesso di norme crea, come noto, confusione, anche rispetto a quale norma dover applicare e a come poi 'coordinarle' fra di loro.

Tutto ciò ha delle implicazioni evidenti sulle amministrazioni[75], destinate a vedere aumentare la loro discrezionalità; l'attività delle amministrazioni, infatti – non eccessivamente imbrigliate nelle maglie del legislatore –, può consentire quella 'capacità adattiva' al mutamento delle tecnologie e degli attacchi informatici; certo, ciò presuppone, comunque, il rispetto del principio di legalità e, di conseguenza, il mantenimento di quel legame con l'apparato politico, necessario ai fini della loro legittimazione (democratica). Inoltre, è essenziale che tali amministrazioni siano titolari delle competenze tecniche richieste (nonché degli strumenti) per poter predisporre una regolazione efficace, e cioè tempestiva e tecnica.

Si tratta di una regolazione che, non potendo prescindere anche dai soggetti privati[76], lascia inevitabilmente un margine di libertà a quest'ultimi, secondo un meccanismo che – come già sottolineato – non sembra essere del tipo *top down*, e, dunque, eteroimposto, ma congiunto, sulla base di un obiettivo comune che si tenta di raggiungere 'incentivando' l'adozione di una serie di misure poiché all'assunzione di esse consegue un vantaggio per tutti coloro i quali decidono di attuarle[77]. Un modello regolatorio che, per la verità – anche alla luce dell'ultima

74 Anche se, sotto questo profilo, la digitalizzazione dei relativi procedimenti legislativi potrebbe contribuire ad una riduzione dei tempi; sul punto, con riferimento al piano nazionale (ma le cui considerazioni possono estendersi anche al piano europeo), cfr. le osservazioni di Cavalli 2023; Ibrido 2022. In merito, avuto particolare riguardo agli algoritmi, in una prospettiva di ampio respiro tesa a riflettere sulle implicazioni che tutto ciò determina per il modello attuale – sempre più messo in discussione – di democrazia rappresentativa, Cardone 2022.

75 In proposito, con particolare riguardo alla cibersicurezza nelle amministrazioni digitali, cfr. Montessoro 2019.

76 Nella prospettiva della necessaria collaborazione fra 'pubblico' e 'privato' ai fini della gestione dei rischi informatici cfr. Previti 2022. Sulla necessità di rafforzare la collaborazione fra 'pubblico' e 'privato' cfr. anche Bruno 2020.

77 Non si tratta della regolazione per incentivi di tipo tradizionale; in tal caso, quello che si definisce 'incentivo' non è un vantaggio attribuito dal legislatore, esterno cioè alla sfera giu-

considerazione circa l'impossibilità di prescindere dai soggetti privati – non è estraneo all'ordinamento europeo, il quale, da anni, attribuisce centralità allo strumento della strategia, strumento che, più di recente, ha assunto un'importanza (e, soprattutto, un'attenzione) con la comunicazione nota come *Green deal* europeo[78]. Ecco, si tratta di una regolazione – quella strategica in materia di cibersicurezza – non così dissimile da quella propria del *Green Deal* europeo; anzi, sembrano sussistere una serie di punti di contatto fra le due, e ciò non deve destare stupore poiché entrambe si innestano in quel processo di transizione (ecologica e digitale)[79] che caratterizza la politica europea più recente e riprova del collegamento fra il *Green deal* e la cibersicurezza è rappresentato dal fatto che la strategia relativa a quest'ultima –coerentemente proprio con lo stesso *Green Deal* – secondo la Commissione europea è "essenziale per la transizione verso un'energia più pulita, attraverso reti transfrontaliere e contatori intelligenti, evitando inutili duplicazioni nell'archiviazione dei dati"[80].

La regolazione strategica, dunque, è una regolazione di tipo flessibile e ciò le consente di adattarsi perfettamente (quantomeno da un punto di vista teorico) alla cibersicurezza ed al suo oggetto, essendo coerente con i repentini mutamenti che interessano le nuove tecnologie, di cui deve inevitabilmente farsi carico la cibersicurezza e, con essa, il diritto che la intende regolare.

6. Osservazioni conclusive

La cibersicurezza, come noto, non è solamente una questione di 'difesa nazionale' ma anche e, soprattutto, una questione legata ai diritti, da intendere più precisamente nei termini di 'fruizione dei diritti fondamentali di ciascun individuo'. Pertanto, si pone l'esigenza di una sua solida regolazione pubblica[81] per far fronte ai rischi sempre più frequenti (la 'società del rischio') che caratterizzano ormai la

ridica del destinatario, ma, diversamente, coincide con il rafforzamento di un interesse di cui il destinatario della misura è titolare e che è, quindi, già nella sua sfera giuridica. Il legislatore non concede, pertanto, un incentivo, un vantaggio, ma – previa definizione dell'obiettivo finale da raggiungere – si limita ad individuare le modalità attraverso le quali i destinatari possono conseguire quel determinato obiettivo. Sul punto cfr. Valaguzza 2016. Per un inquadramento generale sul ruolo della regolazione nel campo del diritto amministrativo, per tutti, cfr. Stewart 2004.

78 Sul *Green Deal* europeo quale processo regolatorio, per primo, Chiti 2022.

79 Sulle c.d. 'transizioni gemelle', cfr. Camisa 2024; Franca, Porcari, Sulmicelli 2024.

80 JOIN (2020) 18 final, 4. Sui dati, di recente, nell'ambito di una prospettiva che muove da un mutamento di paradigma nella regolazione europea avente ad oggetto i dati, con spunti circa il riutilizzo degli stessi, cfr. Cremona 2023.

81 Sulle implicazioni per i poteri pubblici nell'epoca della rivoluzione digitale, caratterizzata dalla potente presenza di poteri privati, cfr. Mannoni, Stazi 2021. Con particolare riferimento ai poteri privati ed al relativo potere digitale cfr. Simoncini 2017; Betzu 2022; Ferrarese 2022; Cremona 2023; Pollicino 2023; Resta 2023; Cipolloni 2024. Sui poteri privati ed il nuovo modello regolatorio che sembra emergere alla luce, in particolare, di talune recenti normative adottate in ambito europeo (come, per esempio, il *Digital Markets Act* ed il *Digital Services Act*), cfr. Bruti Liberati 2023.

c.d. 'vita digitale'[82] di ogni essere umano, dove si assiste, per esempio, ad attacchi a sistemi[83] rendendoli inutilizzabili e, quindi, impedendo l'esercizio di funzioni pubbliche o l'erogazione di prestazioni circa servizi essenziali, con la conseguente lesione (o rischio di lesione) di quegli stessi diritti fondamentali[84] riconosciuti e garantiti dall'ordinamento europeo (e dalle relative costituzioni) che, ormai, costituiscono il 'punto logico di partenza' di ogni analisi correttamente impostata sulla cibersicurezza, e la regolazione (forse quella che si è qui definito come 'regolazione strategica') deve muoversi in questa direzione, sebbene il cammino sia ancora lungo e dai risultati in larga parte incerti.

Ciò che invece appare certo è che la riflessione sul punto – con riferimento dunque, in particolare, al IICB – passi inevitabilmente da una più solida cooperazione fra i vari organismi deputati alla regolamentazione[85] e ad alla regolazione del fenomeno della cibersicurezza allo scopo di concorrere unitamente, ed in ultima analisi, alla garanzia di quei diritti ad essa connessi ed il cui effettivo godimento rischia di essere sempre più posto in costante e forte discussione.

Infine, prima di concludere – pur essendo estraneo al presente contributo il profilo concernente direttamente il governo della cibersicurezza – sembra possibile osservare che l'istituzione del Comitato, unitamente ai nuovi poteri attribuiti al CERT-EU, sono destinati a segnare una parziale riconfigurazione dell'assetto di governo della cibersicurezza a livello europeo (e quindi, in parte, anche a livello nazionale)[86] secondo una direttrice che appare essere caratterizzata dall'idea di fondo di una regolazione più incisiva per far fronte ai mutamenti in atto, sempre più frequenti, che interessano le nuove tecnologie e, in particolare, gli attacchi informatici, i quali rappresentano sicuramente una delle minacce[87] più serie e pericolose con le quali le società del 'domani' saranno inevitabilmente chiamate a confrontarsi.

Al diritto[88] il compito di cercare di anticipare tali rischi e, contestualmente – per quello che qui più interessa –, di ordinare il complesso ed articolato fenomeno della cibersicurezza, sulla scia di quell'autorevole insegnamento (ancora estremamente attuale) del diritto come strumento ordinante la società[89], dove l'ordine si con-

82 Nell'ambito di quella che si definisce ormai come "società digitale"; sul punto cfr. le riflessioni di Longo 2023. Sulla "società digitale" cfr. anche di Carpegna Brivio 2024. Con particolare attenzione al profilo dei diritti Celotto 2023.

83 Sulla sicurezza delle infrastrutture informatiche, di recente, cfr. Serini 2023. Più in generale, sulla sicurezza nel ciberspazio, cfr. Ursi 2023, dove si avanza l'ipotesi della sicurezza cibernetica quale (nuova) funzione pubblica.

84 In proposito, di recente, cfr. Iannuzzi, Laviola 2023.

85 Una recente ricognizione dell'evoluzione della disciplina in materia di cibersicurezza è offerta da Longo 2024. Cfr. anche Brighi 2024; Contaldo, Mula 2020.

86 Con una serie di implicazioni rispetto all'Agenzia nazionale per la cybersecurity, sulla quale, fra i tanti, Forgione 2022.

87 Con specifico riferimento al versante dei reati informatici cfr. Pietropaoli 2022.

88 In particolare quello pubblico; sul futuro e le sfide del diritto pubblico cfr. Aa.Vv. 2024.

89 Il riferimento è, e non potrebbe essere altrimenti, al magistero di Paolo Grossi.

trappone (anteponendosi) al caos[90], che è il regno del più forte, il luogo ove, per definizione, non vi è spazio per i diritti, per quegli stessi diritti che, come si è detto, costituiscono ormai patrimonio essenziale ed insopprimibile della cibersicurezza.

Bibliografia

Aa.Vv. 2024, "Il futuro del diritto pubblico. Il tempo e le sfide", in *Diritto pubblico*, 1: 3-130.

Betzu M. 2022, *I baroni del digitale*, Napoli: Editoriale scientifica.

Brighi R., Chiara P.G. 2021, "La cybersicurezza come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea", in *Federalismi.it*, 21: 18-42.

Brighi R. 2024 [2021], "Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione", in T. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, Milano: Wolters Kluwer: 75-88.

Bruno B. 2020, "Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali", in *Federalismi.it*, 14: 11-45.

Bruti Liberati E. 2023, "Poteri privati e nuova regolazione pubblica", in *Diritto pubblico*, 1: 285-301.

Cafaggi L. 2022, "Proibire, permettere, persuadere. Appunti di viaggio nella regolazione contemporanea", in *Mercato concorrenza e regole*, 3: 491-522.

Camisa F. 2024, "Ambiente e tecnologia: l'interconnessione tra le 'transizioni gemelle'", in *Federalismi.it*, 14: 55-75.

Camisa F., Simoncini A. 2024, "Il fattore umano e la regolazione della cybersecurity", in *Mondo digitale*, marzo: 1-17.

Cardone A. 2022, "Algoritmi e ICT nel procedimento legislativo: quale sorta per la democrazia rappresentativa?", in *Osservatorio sulle fonti*, 2: 57-382.

Caterina E. 2023, *Personalismo vivente. Origini ed evoluzione dell'idea personalista dei diritti fondamentali*, Napoli: Editoriale Scientifica.

Cavalli L. 2023, "Le Camere nell'emergenza da Covid-19. Notazioni ricostruttive e spunti problematici", in *Federalismi.it*, 3: 212-227.

Celotto A. 2023, *"Sudditi". Diritti e cittadinanza nella società digitale,* Milano: Giuffrè.

Chiti E. 2022, "Managing the ecological transition of the EU: the European green deal as a regulatory process", in *Common Market Law Review*, 59: 19-48.

Chiti E. 2009, "An important part of the EU's institutional machinery: features, problems and perspectives of European Agencies", in *Common Market Law Review*, 46: 1395-1442.

Chiti E. 2002, *Le Agenzie europee. Unità e decentramento nelle amministrazioni comunitarie*, Padova: Cedam.

Cipolloni C. 2024, *Persona, poteri privati e Stato nella rivoluzione internettiana*, Torino: Giappichelli.

Contaldo A., Mula D. (a cura di) 2020, Cybersecurity law. *Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa: Pacini Giuridica.

90 Da intendere nel senso di 'anomia', non (come sovente accade) di 'anarchia'. Sull'anarchia della Rete cfr. Gatti 2019.

Cremona E. 2023, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli: Edizioni Scientifiche Italiane.
Cremona E. 2023, "Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso", in *Rivista italiana di informatica e diritto*, 2: 111-130.
Del Gatto S. 2012, *Il metodo aperto di coordinamento. Amministrazioni nazionali e amministrazione europea*, Napoli: Jovene.
di Carpegna Brivio E. 2024, *Pari dignità sociale e* Reputation scoring*. Per una lettura costituzionale della società digitale*, Torino: Giappichelli.
Ferrarese M.R. 2022, *Poteri nuovi. Privati, penetranti, opachi*, Bologna: Il Mulino.
Forgione I. 2022, "Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", in *Diritto amministrativo*, 4: 1113-1143.
Franca S., Porcari A., Sulmicelli S. (a cura di) 2024, *Le transizioni e il diritto. Atti delle giornate di studio 21-22 settembre 2023*, Napoli: Editoriale scientifica.
Gatti A. 2019, "Istituzioni e anarchia nella Rete. I paradigmi tradizionali della sovranità alla prova di Internet", in *Il diritto dell'informazione e dell'informatica*, 3: 711-743.
Giupponi T.F. 2024, "Il governo nazionale della cibersicurezza", in *Quaderni costituzionali*, 2: 277-304.
Iannuzzi A. 2023, "Paradigmi normativi per la disciplina della tecnologia: auto-regolazione, co-regolazione ed etero-regolazione", in *Bilancio, comunità, persona*, 2: 91-107.
Iannuzzi A., Laviola F. 2023, "I diritti fondamentali nella transizione digitale fra libertà e uguaglianza", in *Diritto costituzionale*, 1: 9-40.
Ibrido R. 2022, "Evoluzioni tecnologiche o involuzioni costituzionali? La 'reingegnerizzazione' del processo di decisione parlamentare", in *Osservatorio sulle fonti*, 2: 291-310.
Lalli A. (a cura di) 2024, *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, Torino: Giappichelli.
Longo E. 2024, "La disciplina della cybersecurity nell'Unione europea e in Italia", in F. Pizzetti, M. Orofino, A. Iannuzzi, S. Calzolaio, E. Longo (a cura di), *La regolazione europea della società digitale*, Torino: Giappichelli: 203-234.
Longo E. 2023, "La ricerca di un'antropologia costituzionale della società digitale", in *Rivista italiana di informatica e diritto*, 2: 147-160.
Mannoni S., Stazi G. 2021, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli: Editoriale scientifica.
Montessoro P.L. 2019, "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", in *Istituzioni del Federalismo*, 3: 783-800.
Moroni L. 2024, "La governance della cybersicurezza a livello interno ed europeo: un quadro intricato", in *Federalismi.it*, 14: 179-199.
Pietropaoli S. 2022, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino: Giappichelli.
Pollicino O. 2023, "Potere digitale", in *Potere e Costituzione*, diretto da M. Cartabia, M. Ruotolo, *I tematici dell'Enciclopedia del diritto*, V, Milano: Giuffrè: 410-445.
Previti L. 2022, "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", in *Federalismi.it*, 25: 65-93.
Resta G. 2023, "Poteri privati e regolazione", in *Potere e Costituzione*, diretto da M. Cartabia, M. Ruotolo, *I tematici dell'Enciclopedia del diritto*, V, Milano: Giuffrè: 1008-1032.
Santaniello M. 2021, "La regolazione delle piattaforme e il principio della sovranità digitale", in *Digital Politics*, 3: 579-600.
Savino M. 2005, *I Comitati dell'Unione europea. La collegialità amministrativa negli ordinamenti compositi*, Milano: Giuffrè.

Serini F. 2023, "La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana", in *Rivista italiana di informatica e diritto*, 2: 41-76.
Simoncini A. 2022, "La co-regolazione delle piattaforme digitali", in *Rivista trimestrale di diritto pubblico*, 4: 1031-1049.
Simoncini A. 2017, "Sovranità e potere nell'era digitale", in O. Pollicino, T. E. Frosini, E. Apa (a cura di), *Diritti e libertà in Internet*, Milano: Mondadori Education.
Stewart R.B. 2004, "Il diritto amministrativo nel XXI secolo", in *Rivista trimestrale di diritto pubblico*, 1: 1-29.
Ursi R. (a cura di) 2023, *La sicurezza nel cyberspazio*, Milano: FrancoAngeli.
Valaguzza S. 2016, "La regolazione strategica dell'Autorità Nazionale Anticorruzione", in *Rivista della regolazione dei mercati*, 1: 9-58.