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

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0253 • articolo sottoposto a peer review • pubblicato in anteprima il 10 dic. 2025

Pier Giorgio Chiara, Geordie Morciano
Alessandro Vannini, Raffaella Brighi, Marco Prandini

Un approccio pratico di '*legal design*': la Guida al regolamento UE Cyber Resilience Act. Metodo, obiettivi ed impatti

Questo articolo illustra il lavoro multidisciplinare alla base della '*Guida al regolamento UE Cyber Resilience Act: un approccio di legal design*', soprattutto, dando rilevanza al metodo, nonché agli obiettivi e agli impatti attesi. La Guida intende chiarire l'applicazione del Regolamento UE 2024/2847 (Cyber Resilience Act, CRA). Al fine di ridurre l'alta complessità tecnico-giuridica del CRA, la guida adotta un approccio innovativo che combina i principi del *legal design* con competenze tecniche, informatiche e giuridiche, in materia di cybersicurezza. Le disposizioni e i meccanismi complessi del CRA sono tradotti in processi più accessibili a coloro che dovranno applicarli, riducendo pertanto il rischio di errate interpretazioni nelle fasi di pianificazione della conformità e di attuazione.

Legal design – Cybersicurezza – Cyber Resilience Act – Diritto Ue – Ricerca multidisciplinare

A practical legal design approach: the Guide to the EU Regulation Cyber Resilience Act. Methodology, goals and impacts

This article outlines the multidisciplinary work behind the '*Guide to the EU Cyber Resilience Act: a legal-design approach*' project, with a particular emphasis on its methodology, objectives, and expected impacts. The Guide aims to clarify the application of EU Regulation 2024/2847 (Cyber Resilience Act, CRA). To lower the high technical-legal complexity of the CRA, the Guide employs an innovative approach that integrates legal design principles with technical expertise, encompassing both IT and legal aspects, in the cybersecurity field. The CRA's complex provisions and mechanisms are translated into processes that are more accessible to those required to implement them, thereby reducing the risk of misinterpretation during compliance planning and implementation phases.

Legal design – Cybersecurity – Cyber Resilience Act – EU law – Multidisciplinary research

P.G. Chiara e R. Brighi afferiscono al Dipartimento di Scienze Giuridiche, mentre A. Vannini e M. Prandini afferiscono al Dipartimento di Informatica - Scienza e Ingegneria dell'Università di Bologna. G. Morciano è legal innovation specialist

A P.G. Chiara sono da attribuirsi le sezioni 1 e 3. La sezione 2 è da attribuirsi congiuntamente a P.G. Chiara, G. Morciano e A. Vannini

Questo contributo è stato sostenuto dal Progetto SERICS (PE00000014), finanziato dall'Unione Europea - NextGenerationEU attraverso il MUR nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3

1. Introduzione

Il presente lavoro illustra gli obiettivi, la metodologia e la struttura della Guida dedicata al Regolamento (UE) 2024/2847, che introduce requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (Cyber Resilience Act, CRA)[1]. L'iniziativa nasce con l'intento di chiarire il funzionamento del Regolamento e di tradurre requisiti normativi e tecnici complessi in misure organizzative e operative concrete, fornendo quindi indicazioni chiare e attuabili ai soggetti coinvolti nella sua applicazione, tra cui operatori economici (fabbricanti, importatori, distributori, rappresentanti autorizzati e gestori di software open source), consulenti legali ed esperti tecnici di cybersicurezza. In questa prospettiva, la Guida si configura non solo come un riferimento giuridico, ma come uno strumento pratico per la pianificazione della conformità, il coordinamento tra i diversi attori coinvolti dalle attività di compliance (internamente ed esternamente ad un'azienda) e la riduzione del rischio di errore interpretativo durante la fase di implementazione.

La Guida si distingue per l'adozione di un approccio metodologico innovativo, fondato sull'integrazione di principi di legal design e competenze tecniche, vale a dire, giuridiche e informatiche, di cybersicurezza. Il legal design contiene nel suo spettro competenze trasversali di matrice giuridica, linguistica e di design, le cui tecniche, sinergicamente applicate, permettono di rimodellare testualmente e graficamente il precetto normativo, lasciandone invariata la corretta connotazione giuridica[2]. Il punto focale di tale disciplina, e delle tecniche ad essa sottese, corrisponde ai bisogni e alle esigenze pratiche degli utenti finali specificamente identificati per il progetto di specie. Tale architettura progettuale consente, così, di semplificare e rendere fruibili contenuti normativi complessi. In particolare, colmare la lacuna epistemica tra i "classici" utenti del diritto (avvocati, giudici e autorità) e tutti gli altri utenti (cittadini, consumatori, imprese)[3].

La Guida è frutto di una collaborazione multidisciplinare tra l'area giuridica, con esperienza in diritto europeo della cybersicurezza, l'area ingegneristica, con specifiche competenze in *Operational Technology* (OT) *security*, ed infine uno specialista in tecniche di legal design. In tale contesto, è stato adottato il design thinking quale metodo operativo di riferimento, calibrandone le fasi canoniche (dall'analisi dei bisogni all'ideazione, prototipazione e validazione) agli obiettivi e alle tempistiche del progetto[4]. Tale impostazione metodologica ha consentito di realizzare un processo autenticamente multidisciplinare, nel quale

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). Per un'analisi critica del regolamento, si permetta il rinvio a Chiara 2025.
2. Hagan 2020; Koulu–Pohle 2024; Rossi–Ducato–Haapio–Passera 2019.
3. Legal Design Alliance 2018.
4. Ducato–trowel 2021.

la dimensione giuridica, tecnica e comunicativa si integrano in modo coerente e complementare.

Oltre al suo valore operativo, la Guida svolge un ruolo di ponte concettuale tra domini tradizionalmente separati (giuridico, tecnico e gestionale), promuovendo una visione integrata della cybersicurezza e della resilienza, e una cultura comune della conformità tra i molteplici attori coinvolti.

Conformandosi a questi principi, la Guida mira ad essere tuttavia strumento utile per i diretti utilizzatori del Regolamento, nel caso di specie di stampo prevalentemente tecnico, e in questo senso, dunque, anche per gli utenti "classici" del diritto, in virtù della specificità del CRA data non solo dalla complessa commistione tra l'elemento tecnico e giuridico, ma anche dall'ibridizzazione di diversi approcci regolatori (sezione 2). L'accesso ad un testo giuridico in modo chiaro è una componente essenziale di una compliance e governance efficace della cybersicurezza. Non è un caso che per rispondere alle esigenze dei professionisti a sostegno dell'attuazione del CRA, l'articolo 10 del regolamento richieda agli Stati membri di promuovere misure e strategie volte a sviluppare competenze di cybersicurezza anche attraverso la creazione di strumenti organizzativi e tecnologici. Guardando invece all'esperienza in settori più maturi, importanti esperimenti di legal design sono stati condotti in un ambito "vicino" alla cybersicurezza[5], vale a dire la protezione dei dati personali, segnatamente nell'applicazione del GDPR[6], ed in particolare dell'articolo 12.

Per garantire al contempo rigore giuridico e accuratezza tecnica, l'analisi del regolamento è stata arricchita da contributi tecnici in materia di cybersicurezza, rendendo il documento accessibile a un pubblico interdisciplinare. Il risultato è un'interpretazione operativa che mira a ridurre l'alta complessità tecnico-giuridica del Cyber Resilience Act, utile a orientare la progettazione e l'adeguamento dei processi aziendali in diversi contesti reali.

Come anticipato, il presente contributo illustra la metodologia innovativa adottata per l'elaborazione della Guida, la cui originalità risiede non soltanto nell'aver utilizzato il *design thinking*[7] quale struttura portante dell'intero processo operativo, ma anche nell'impiego mirato di tecniche di design capaci di "scomporre" la complessità del Regolamento e di "ricomporla" in un ordine concettuale chiaro, coerente e logicamente fruibile. Muovendo dalle cinque fasi del *design thinking*, le sezioni che seguono ne ripercorrono l'applicazione al progetto, illustrando per ciascuna fase le strategie e gli strumenti adottati e mettendo in evidenza il loro contributo alla costruzione di un modello interpretativo e operativo del Cyber Resilience Act.

In questa introduzione si riportano sinteticamente le cinque fasi che hanno scandito il processo. La prima fase, "Ricerca" (sezione 2.1), ha avuto l'obiettivo di comprendere i bisogni e le esigenze degli utilizzatori finali della Guida, al fine di raccogliere *insight* qualitativi e quantitativi utili all'impostazione del progetto. In linea con un approccio di co-design collaborativo, è stata definita una strategia di ricerca basata su interviste strutturate, strumenti che hanno consentito di delineare in modo realistico le aspettative, le criticità operative e le competenze degli utenti potenziali. Sulla base dei dati raccolti, infatti, il team ha delineato i profili rappresentativi dei potenziali destinatari che, nelle diverse tipologie professionali, si troveranno a utilizzare la Guida nella pratica quotidiana. La seconda fase, "Definizione & Ideazione" (sezione 2.2), è stata concepita come un unico step da un punto di vista metodologico, e ha tradotto gli insight emersi nella fase "Ricerca" in soluzioni progettuali concrete. Attraverso tecniche di *whiteboarding*, *information mapping* e *co-design* collaborativo, sono stati rielaborati i contenuti del Regolamento, organizzandoli in un'architettura chiara, coerente e facilmente fruibile. La terza fase è stata invece dedicata alla "Prototipazione" (sezione 2.3) della soluzione scelta, che ha assunto la forma di un documento interattivo a contenuto visivo e testuale, coerente con la logica della conformità alla normativa. Le disposizioni del regolamento, nonché i requisiti essenziali di natura tecnico-informatica, sono stati rielaborati e sintetizzati in schemi e percorsi visuali che consentissero una

5. Mantelero–Vaciago–Esposito–Monte 2020.
6. Si veda, *ex multis*, Rossi–Palmirani 2020; Rundle 2006; Garante per la Protezione dei Dati Personali 2025.
7. Lewrick–Link–Leifer 2018; Lewrick–Link–Leifer 2020. Si veda anche Ducato–Strowel 2021.

comprensione immediata e funzionale dei relativi obblighi. Successivamente, nella quarta fase, "User test" (sezione 2.4), sono stati coinvolti nuovi soggetti dai diversi *background* (es., consulenti tecnici; giuristi; informatici; responsabili aziendali) al fine di testare il prototipo e valutare l'efficacia comunicativa e la fruibilità operativa. I feedback raccolti, sia sul piano percettivo-visivo, sia concettuale-logico, hanno consentito di apportare le necessarie modifiche e ottimizzazioni in vista del rilascio definitivo della Guida. Infine, nella quinta fase, "Miglioramento & Lancio" (sezione 2.5), sono state apportate le modifiche necessarie alla luce dei feedback emersi nella fase precedente e quindi è stato organizzato il rilascio della Guida.

La Guida è stata progettata e sviluppata nell'ambito del progetto "EcoCyber – Risk Management for Future Cyber-Physical Ecosystems", realizzato all'interno della Partnership Estesa SERICS (PE00000014), che è un'iniziativa nazionale del Piano Nazionale di Ripresa e Resilienza (PNRR) del MUR, finanziata dall'Unione Europea – Next Generation EU. Il progetto EcoCyber è dedicato allo sviluppo di soluzioni e metodi tecnici e giuridici innovativi per sfruttare le opportunità offerte dai sistemi cyber-fisici, affrontando al contempo le sfide connesse (ad esempio, minacce e vulnerabilità informatiche). In particolare, questo lavoro è stato condotto dai team di ricerca di due Work Package di EcoCyber: WP 2 – Soluzioni per la progettazione e il collaudo di componenti smart sicuri e WP 4 – Regole per la società del futuro, integrando così gli aspetti tecnici e legali nel summenzionato approccio multidisciplinare[8].

2. Realizzazione della Guida

I motivi per i quali si è deciso di concentrare la Guida sul regolamento Cyber Resilience Act sono duplici. Al fine di risolvere la frammentazione del quadro normativo europeo in materia di cybersicurezza in relazione alla generalità dei prodotti hardware e software[9], il regolamento introdurrà una nuova serie di requisiti tecnici "di cybersicurezza di base" ed obblighi giuridici ad un ampio novero di soggetti privati che intendono immettere sul mercato unico "prodotti con elementi digitali"[10]. Connesso a ciò, l'intrinseca combinazione di elementi tecnici e giuridici, propria della legislazione armonizzata in materia di sicurezza dei prodotti[11], rende il CRA un atto giuridico ad alta complessità[12].

Combinando due approcci regolatori distinti, quello della sicurezza dei prodotti e quello basato sul rischio, il CRA introduce requisiti essenziali di cybersicurezza vincolanti per l'immissione sul mercato di prodotti con elementi digitali, un aspetto finora disciplinato solo attraverso pratiche volontarie di settore o accordi contrattuali tra operatori economici. I requisiti essenziali sono prescrizioni di alto livello; con il cd. "Nuovo

8. Coordinati rispettivamente dai professori Marco Prandini (DISI-Unibo) e Raffaella Brighi (DSG-Unibo).
9. Il quadro giuridico dell'Ue in materia di cybersicurezza antecedente al CRA si concentrava infatti su settori specifici o categorie di prodotti delimitate, lasciando pertanto scoperta una vasta parte del mercato digitale. Se il Regolamento (UE) 2019/881 (Cybersecurity Act) ha introdotto un sistema di certificazione per prodotti, servizi e processi ICT, caratterizzato pertanto dalla volontarietà, i soli requisiti obbligatori in materia di cybersicurezza per prodotti con elementi digitali erano frammentati tra diversi atti giuridici, in base al settore o alla categoria di prodotto. Ad esempio, la direttiva 2014/53/UE (direttiva sulle apparecchiature radio), anche e soprattutto attraverso il regolamento delegato (UE) 2022/30, impone requisiti di cybersicurezza limitati ai prodotti elettrici o elettronici che emettono e/o ricevono intenzionalmente onde radio, lasciando pertanto fuori dall'ambito di applicazione tutti i prodotti connessi per altro mezzo che non fossero le onde radio. Ancora, il regolamento (UE) 2017/745 stabilisce *inter alia* requisiti di cybersicurezza per i soli dispositivi medicali.
10. L'ambito di applicazione oggettivo del CRA include i prodotti con elementi 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 (art. 2, para. 1), dove per "prodotto con elementi digitali" si intende qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immessi sul mercato separatamente (art. 3, punto 1).
11. Commissione europea 2022.
12. Teichmann–Sergi 2025, p. 7.

Approccio" del 1985, confermato dal "Nuovo Quadro Legislativo" del 2008, i requisiti essenziali sono dettagliati dalle norme armonizzate europee, vale a dire standard tecnici elaborati dagli organismi di normazione europei (CEN, CENELEC, ETSI) dietro mandato della Commissione ed adottati da quest'ultima[13].

I requisiti essenziali, unitamente a diversi obblighi degli operatori economici rilevanti lungo l'intera catena di valore dei prodotti (fabbricanti, ma anche distributori, importatori, rappresentanti autorizzati), si estendono per l'intero ciclo di vita del prodotto, imponendo misure di sicurezza by design e by default, gestione delle vulnerabilità, aggiornamenti, e documentazione tecnica continua. Secondo l'approccio *risk-based*, invece, i prodotti sono classificati in base al livello di rischio di cybersicurezza, con la conseguenza di avere procedure di valutazione della conformità differenziate a seconda del grado di rischio (dall'autovalutazione al controllo da parte di organismi notificati). L'interazione tra questi due modelli genera un sistema complesso, in cui le imprese devono integrare competenze normative e tecniche per interpretare correttamente obblighi variabili e nuovi, gestire rischi dinamici e garantire la conformità durante tutta la vita del prodotto.

Avendo scelto di adottare la tecnica del legal design per rendere più agevole l'interpretazione non solo delle disposizioni giuridiche, ma anche, e soprattutto, dei meccanismi tecnico-giuridici del regolamento, con l'obiettivo di supportare gli operatori nei processi di conformità, la prima questione di design affrontata è stata come rappresentare graficamente in modo chiaro e intuitivo tali contenuti, mantenendo al tempo stesso il rigore e la precisione del testo normativo[14]. Infatti, per quanto l'idealtipo di destinatario della Guida sia un tecnico professionista, sia nell'ambito legale che in quello informatico, l'intento che ha animato la traduzione e riformulazione del regolamento in componenti visive e grafiche è stato quello di rendere più chiara la lettura e la comprensione del testo giuridico anche all'utilizzatore che non dispone necessariamente degli strumenti ermeneutici del tecnico.

Nel contesto della progettazione dell'informazione, e quindi della grafica e delle interfacce, il problema della comunicazione mediata assume un rilievo peculiare allorché le azioni poste in essere dall'utente, sulla base della propria interpretazione dell'artefatto, possano produrre effetti giuridicamente rilevanti[15]. La mediazione visiva non si limita a svolgere una funzione estetica o divulgativa, ma incide direttamente sui processi cognitivi e decisionali che presiedono alla comprensione e all'applicazione della norma. La questione si pone dunque in termini di responsabilità progettuale: il design dell'informazione giuridica deve garantire, oltre alla chiarezza comunicativa, anche la fedeltà concettuale e sistematica rispetto al contenuto normativo di riferimento[16].

Al tempo stesso, è opportuno precisare che la Guida non si configura come un processo di "iconizzazione" di disposizioni giuridiche, operazione che potrebbe introdurre criticità in ordine alla qualità e all'affidabilità della rappresentazione normativa, bensì come una traslazione grafica strutturata e analitica del testo giuridico. Tale impostazione metodologica mira a preservare, da un lato, la coerenza semantica e sistematica della disposizione e, dall'altro, ad evitare un'eccessiva semplificazione che possa compromettere l'accuratezza interpretativa del dato normativo. In questo senso, la rappresentazione visuale non sostituisce la norma, ma ne costituisce una diversa forma di accesso e comprensione, fondata su criteri di rigore, trasparenza e conformità giuridica.

2.1. Ricerca

Dopo aver delineato l'oggetto e gli obiettivi del progetto, nella prima fase, ancora in uno stadio preliminare, abbiamo individuato chi fossero i soggetti maggiormente interessati alla Guida. I destinatari primari sono stati individuati tra le aziende rientranti nell'ambito di applicazione del regolamento. Destinatari secondari della Guida sono stati identificati negli esperti del diritto (es., avvocati) ed

13. Kamara 2025.
14. Rossi–Haapio 2019. Si veda anche Ducato–Strowel 2021.
15. Rossi–Palmirani 2020.
16. Perondi 2024.

informatici che avrebbero dovuto studiare il regolamento per supportare le attività di conformità degli operatori economici destinatari degli obblighi del CRA. L'obiettivo di questa prima attività era pertanto comprendere l'approccio specifico dei diversi soggetti aziendali coinvolti nella compliance normativa, le principali criticità riscontrate di fronte a nuove normative e i bisogni informativi che sono emersi nella specifica fase di adeguamento al CRA[17].

Dopo aver definito un numero congruo di partecipanti (5 aziende e/o professionisti operanti sul territorio nazionale), abbiamo somministrato loro un'intervista strutturata, composta da 21 domande, divise in 6 sezioni con allegata l'informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 GDPR. Nelle prime due sezioni le domande hanno preso in esame, da una parte, il contesto specifico dell'intervistato[18] e, dall'altra, le modalità con le quali gli intervistati approfondiscono una normativa[19]. La terza sezione ha poi definito il perimetro delle attività progettuali indagando il grado di conoscenza e approfondimento del CRA[20]. In questo contesto, la quarta sezione ha verticalizzato il focus sulla complessità delle attività interpretative e su determinati casi-limite[21]. La quinta sezione, invece, ha preso in esame la relazione tra il CRA e le altre normative di settore[22]. La sesta sezione si è infine concentrata sui risultati attesi da parte dei partecipanti all'intervista dal progetto "Guida

17. Così Hagan 2020, p. 8-9: "the goal is to find people in the context of the system [nel nostro caso, il CRA, ndr.] who are trying to use the system through its technologies, rules, interfaces, language, and services and then to gather information from them by triggering a reflective process that can expose what their deeper needs and aspirations are".
18. È stato chiesto quale fosse il ruolo attuale e in che modo l'intervistato, unitamente al team di appartenenza, fosse coinvolto nella normativa in azienda; quali fossero i team o singoli professionisti all'interno dell'azienda che si occupano a vario titolo delle attività di progettazione, sviluppo e conformità del prodotto rispetto alla normativa e con i quali l'intervistato si interfaccia ogniqualvolta si debba applicare un nuovo perimetro normativo; una descrizione, per punti o fasi, del flusso di consegne/lavoro tra i team di lavoro coinvolti nelle attività di compliance normativa.
19. È stato chiesto quali fossero le principali fonti utilizzate per l'interpretazione delle disposizioni normative; come queste fossero state reperite e quali fossero state giudicate le più complete e funzionali. Inoltre, è stato chiesto quali fossero i criteri per la selezione di professionalità per la soluzione di dubbi interpretativi.
20. È stato chiesto agli intervistati se avessero già approfondito il CRA in vista della sua applicazione; se, oltre al testo del regolamento, avessero consultato materiali di supporto per comprenderlo meglio (es., sintesi, schede pratiche, guide, ecc.), e, in caso di risposta affermativa, quali avessero trovato più chiari e utili. Infine, è stato chiesto agli intervistati di riordinare alcuni elementi centrali della normativa (es., data di entrata in applicazione; ambito di applicazione; obblighi per i soggetti; procedure documentali; casi limite ed esempi pratici; glossario tecnico e definizioni chiave; procedure di valutazione della conformità; sanzioni) in base all'ordine di priorità data all'elemento normativo-informazionale, immaginando di consultare una "guida al CRA".
21. È stato chiesto agli intervistati quali parti del CRA ritenessero più complesse da interpretare o applicare (ad es., definizioni, ambito di applicazione, criteri per "prodotto con elementi digitali"); se avessero già effettuato una valutazione per identificare quali, tra i loro prodotti, rientrassero nello *scope* del regolamento e se, contestualmente, fossero emersi casi-limite in cui non fosse chiaro se un prodotto con elementi digitali fosse soggetto al CRA. Connesso a ciò, è stato chiesto agli intervistati quali figure e ruoli, all'interno del contesto aziendale, fossero coinvolte nella decisione finale sul fatto che un prodotto debba essere conforme al regolamento. Sotto altro profilo, gli intervistati hanno indicato quali aspetti del regolamento generassero le maggiori difficoltà operative per le organizzazioni di riferimento (es., produzione della SBOM; gestione degli aggiornamenti di sicurezza; gestione delle vulnerabilità; ecc.).
22. È stato chiesto agli intervistati se, rispetto alla documentazione tecnica richiesta già da altre normative applicabili (es. direttiva RED, direttiva NIS2, AI Act, ecc.), avessero chiaro come integrare i requisiti del CRA e se, in questo contesto, ritenessero che il CRA si sovrapponga o entri in conflitto con altre normative applicabili ai prodotti forniti oppure se, di contro, rilevassero sinergie sfruttabili.

al CRA"[23]. Una domanda di chiusura della *survey*[24] ha chiesto agli intervistati se non avessimo incluso tra le domande degli elementi che, secondo loro, sarebbero stati utili per capire meglio i problemi applicativi del CRA nei loro contesti aziendali.

Dall'indagine è emerso che tutti gli intervistati hanno già intrapreso le attività di approfondimento sul CRA, sebbene con diversi gradi di dettaglio. Rispetto alle fonti utilizzate, prevalgono i materiali ufficiali (es., testo del regolamento sulla Gazzetta Ufficiale dell'Ue) e solo secondariamente workshop, webinar e sintesi di consulenti esperti. Con riferimento a questi materiali di supporto, un partecipante segnala la scarsa applicabilità di tali risorse, giudicate "troppo poco chiare" e "lontane dalla realtà operativa".

Quando invitati a ordinare le sezioni di una potenziale guida al CRA secondo priorità di consultazione, i partecipanti convergono su una struttura orientata agli aspetti pratici e applicativi. Le aree ritenute più rilevanti sono: (i) data di entrata in vigore e tempistiche di applicazione; (ii) obblighi per i soggetti coinvolti; (iii) procedure documentali e operative; (iv) ambito di applicazione del regolamento. Seguono, in ordine decrescente, le sezioni relative alle procedure di valutazione, ai casi-limite ed esempi pratici, e solo successivamente alle definizioni o ai glossari tecnici.

In ordine invece alle principali difficoltà di interpretazione, alcuni degli intervistati ritengono che l'ambito di applicazione, nonché i criteri di classificazione dei prodotti siano troppo ambigui; ulteriore criticità emersa è la gestione di componenti di terze parti, soprattutto nei casi in cui non sia possibile ottenere collaborazione dai fornitori, nonché la traduzione delle prescrizioni normative in soluzioni tecniche praticabili nei diversi contesti (software, macchinari industriali, sistemi IoT). A livello operativo, le problematiche più ricorrenti si concentrano sulla gestione degli aggiornamenti di sicurezza e sul monitoraggio delle vulnerabilità e degli incidenti, seguiti dalla gestione documentale e dall'eventuale produzione della *Software Bill of Materials* (SBOM)[25].

Per quanto concerne invece lo stato di implementazione del CRA, tre organizzazioni hanno già completato una valutazione interna per determinare i prodotti soggetti al regolamento; i cd. "casi-limite" (difficoltà nel determinare l'applicabilità del regolamento ad un dato prodotto con elementi digitali) sono al momento poco frequenti. In questo contesto, le figure coinvolte nelle decisioni legate alla compliance variano sensibilmente tra le organizzazioni: in alcuni casi la responsabilità è affidata all'ufficio legale o alla direzione, in altri al CTO, ai referenti di progetto o a consulenti esterni.

Sul piano normativo, emerge una percezione diffusa di una parziale sovrapposizione con la direttiva NIS2, ma non di conflitto. Alcuni partecipanti segnalano possibili sinergie operative, in particolare nella gestione degli accessi e dei log. Solo due organizzazioni dichiarano di avere già chiaro come integrare i requisiti del CRA con quelli di normative esistenti (es., direttiva sulle apparecchiature radio [RED][26], AI Act, MDR), mentre le altre sono ancora in fase di analisi.

Infine, tutti i partecipanti concordano sull'utilità di una *guida operativa* che semplifichi il CRA attraverso schemi, elementi grafici e strumenti pratici. Gli strumenti ritenuti più utili, in ordine di priorità, sono: (i) flowchart decisionali per determinare l'ambito di applicazione e le classi di rischio; (ii) checklist operative per verificare la conformità dei prodotti e dei processi; (iii) template documentali

23. È stato chiesto agli intervistati se potesse essere utile per le attività di compliance un documento-guida che diminuisse la complessità del regolamento anche attraverso l'introduzione di elementi grafici-schematici e come loro immaginassero tale output (es., flowchart decisionali; tabelle di confronto; checklist operative; template di documenti; glossario visuale; struttura logica e ragionata degli articoli del regolamento; ecc.). In conclusione, gli intervistati hanno dovuto indicare eventuali esempi di guide simili che avessero trovato particolarmente utili.

24. Lewrick–Link–Leifer 2018; Lewrick–Link–Leifer 2020.

25. Si veda, ad esempio, nel contesto nazionale, l'adozione del framework CycloneDX, versione 1.6, attraverso le linee guida pubblicate da ACN a fine ottobre 2025, nel contesto dell'applicazione dei criteri di premialità di cui all'articolo 14 della legge n. 90/2024. Il DPCM 30 aprile 2025, in attuazione dell'articolo 14 della legge 90/2024, prevede all'articolo 4 l'applicazione dei sopra citati criteri di premialità, "previa analisi dell'elenco di tutti i componenti di fabbricazione del prodotto o delle infrastrutture impiegate per erogare un servizio" (*bill of materials*).

26. Sulla relazione tra cybersicurezza e direttiva RED, si permetta di rimandare a Chiara 2022.

per la dichiarazione di conformità e la reportistica; (iv) esempi di casi-limite e tabelle di confronto tra normative; (v) struttura logica e ragionata del CRA per orientarne la lettura.

Nessuno dei partecipanti ha citato strumenti esistenti ritenuti chiari o completi, confermando una lacuna di risorse di riferimento a livello europeo e nazionale.

2.2. Definizione & Ideazione

La mancanza di linee guida operative, che adottino un linguaggio semplice, di un regolamento ad alta complessità tecnico-giuridica come il CRA è una delle principali problematiche evidenziate dagli operatori economici emerse nell'analisi empirica. Pertanto, per produrre la Guida al CRA, la seconda fase progettuale è coincisa con la delimitazione dell'obiettivo progettuale. In particolare, sono stati individuati non solo i nuclei concettuali centrali del Regolamento, ma anche i meccanismi tecnici e gli istituti giuridici più "critici", al fine di chiarire la struttura tecnica-organizzativa del CRA, percepita, soprattutto in specifici articoli, come troppo intricata. In particolare, le norme afferenti a un medesimo tema risultano spesso distribuite in più punti del Regolamento, ovvero tra i paragrafi di un singolo articolo e attraverso i continui rinvii ai diversi articoli e allegati. In questo modo, specifiche informazioni e procedure, seppure concettualmente e operativamente connesse, risultano distanti nella struttura formale, sfuggendo così a una chiara visione d'insieme.

Tale attività si è concentrata sui primi tre capi del regolamento, insieme alle regole sulle sanzioni contenute nel capo VII, in quanto definiscono i requisiti e gli obblighi che incidono direttamente sul modo in cui il regolamento deve essere compreso e attuato dagli operatori economici. Pertanto, l'attività di mappatura non ha ricompreso il capo IV del CRA, che introduce regole per le autorità nazionali responsabili degli organismi di valutazione della conformità (organismi notificati), e non quindi requisiti ed obblighi direttamente rivolti agli operatori destinatari della Guida.

Il testo del Regolamento, una volta rielaborato, è stato oggetto di una mappatura[27] su whiteboard, vale a dire di una scomposizione, o vero e proprio "spacchettamento", in macrosezioni, all'interno delle quali gli articoli afferenti a uno stesso sub-argomento sono stati organizzati in flussi caratterizzati da un preciso ordine e consequenzialità logica (Figura 1[28]), evidenziando non solo la struttura concettuale, ma anche le dinamiche semantiche del testo normativo.

Si è infatti lavorato su un duplice piano: da un lato, la razionalizzazione logica dei contenuti, finalizzata a rendere chiara la relazione tra norme, allegati e rimandi interni; dall'altro, una analisi linguistico-giuridica puntuale, che ha consentito di individuare e valorizzare tutti gli elementi lessicali con funzione condizionale o limitativa (ad esempio, *where*, *only when*, *provided that*, *may*, *shall be*) e di riconoscerne il peso specifico, in termini giuridici, ponendoli nella stessa mappa come punti di attenzione e "nodi semantici" di ulteriori diramazioni di flussi (Figura 2).

Al contempo, sono state ideate potenziali soluzioni visuali di raggruppamento dei contenuti e sono state identificate le corrispondenti etichette tematiche. In parallelo, sono stati tracciati tutti i rimandi e le connessioni trasversali tra gli articoli e gli allegati, propedeutici alla costruzione di un prototipo che garantisse una fluida navigazione e una comprensione sistemica dell'intero Regolamento.

In questa fase si è quindi materialmente definita la struttura portante del successivo prototipo, una "visione satellitare" del Regolamento finalizzata a garantire, a diverse altezze, coerenza testuale e architettonica. Macroscopicamente, dunque, si è perseguita l'ambizione di restituire linearità e chiarezza, al fine di predisporre un format che risultasse quanto più possibile coerente, accessibile e rispondente alle diverse esigenze di fruizione.

Ad esempio, l'articolo 13 rappresenta una delle disposizioni più dense, complesse e centrali dell'intero Regolamento. Nei suoi 25 paragrafi, infatti, racchiude e dettaglia gli obblighi che i fabbricanti (utenti primari di progetto) devono adempiere per garantire la conformità dei propri prodotti ai sensi

27. Lewrick–Link–Leifer 2018; Lewrick–Link–Leifer 2020.

28. Le figure nel contributo hanno scopo puramente esplicativo della metodologia adottata. Per approfondimenti relativi ai contenuti si rimanda alla consultazione della Guida, scaricabile in PDF dal sito https://site.unibo.it/cybersecurity-legal-lab.

del Regolamento. Tale norma risulta di difficile lettura in diversi punti, sia per la complessità lessicale e sintattica del testo normativo, sia per la distribuzione frammentata al suo interno e negli allegati.

Al fine di ridurre la complessità dell'articolo 13, il lavoro si è pertanto concentrato sul "riordinare" i diversi obblighi dei fabbricanti secondo un criterio logico-procedurale, costruito riflettendo in modo funzionale il ciclo di attività e adempimenti che l'operatore è tenuto a rispettare. In particolare, gli obblighi sono stati suddivisi nelle tre fasi caratteristiche del processo della conformità nell'ambito della legislazione armonizzata: (i) pianificazione, design, sviluppo, produzione; (ii) messa a disposizione sul mercato; (iii) periodo di assistenza. È stato inoltre aggiunto un livello ulteriore, trasversale alle tre fasi, contenente gli obblighi che i fabbricanti devono osservare in tutte e tre le fasi precedenti, quindi costantemente durante l'intero ciclo di vita del prodotto.

Come illustrato nella Figura 3, tutti i 25 paragrafi dell'articolo sono stati inizialmente "scorporati" e trasposti in un elenco consequenziale verticale (in verde), consentendo una lettura analitica e ordinata del testo normativo. Questa prima fase di scomposizione ha permesso di accompagnare la segmentazione con una parallela analisi del linguaggio giuridico, evidenziando ridondanze, ripetizioni e rimandi interni che ostacolavano la chiarezza. Successivamente, si è proceduto a un'opera di riorganizzazione in forma visiva (Figura 4): i paragrafi dell'articolo sono stati etichettati in base al tema specifico di riferimento (es., obblighi documentali, gestione delle vulnerabilità, periodo di supporto, informazioni da notificare alle autorità, informazioni da notificare agli utenti) e collocati all'interno di uno schema grafico che riproduce le tre fasi del ciclo di vita dei prodotti con elementi digitali. In tal modo, ciascun obbligo è stato "posizionato" nella fase procedurale in cui il fabbricante è tenuto ad adempiervi, rendendo immediatamente percepibile la sequenza logica e temporale delle attività richieste. Nella parte superiore dello schema, invece, è stata aggiunta una porzione di tabella dedicata ai paragrafi i cui obblighi devono essere adempiuti dai fabbricanti in modo continuativo durante tutto il ciclo di vita del prodotto (in azzurro).

In tal modo, l'approccio di legal design, coadiuvato dalla competenza tecnico-giuridica, ha permesso non solo di implementare una rappresentazione visiva chiara e immediatamente leggibile dell'articolo, ma anche di trasformare il testo normativo in uno strumento operativo, sempre tecnicamente corretto, capace di rappresentare il flusso degli adempimenti in modo coerente con la sequenza reale delle attività che i fabbricanti sono chiamati a svolgere.

Come ricordato supra, il CRA stabilisce dei requisiti essenziali di cybersicurezza, i quali coprono le tematiche di sicurezza del prodotto e i processi di gestione delle vulnerabilità. Tali requisiti devono essere implementati dai soggetti ricadenti nell'ambito di applicazione del CRA al fine di garantire un adeguato livello di cybersecurity per i prodotti con elementi digitali che essi sviluppano.

Dal punto di vista tecnico ed ingegneristico, il progetto si è confrontato con la necessità di rendere maggiormente chiari e dettagliati i ventuno requisiti essenziali di cybersecurity del CRA, necessariamente formulati in modo generico e poco operativo, e che non hanno ancora ricevuto un'adeguata implementazione tecnica attraverso il previsto rilascio delle norme tecniche armonizzate. A tal fine, è stata effettuata un'attività di mappatura degli standard tecnici esistenti, a livello internazionale ed europeo, al fine di valutare la copertura da loro offerta ai requisiti del CRA, facilitando così le procedure di conformità al regolamento, nelle more delle norme tecniche armonizzate. Il punto di partenza di questa ricerca è stato un report dell'ENISA (Agenzia europea per la Cybersicurezza) del 2024[29]. Per ogni requisito, il report ENISA proponeva alcuni standard rilevanti, evidenziandone eventuali gap e limitazioni. Inoltre, definiva un set di sotto-requisiti per ognuno dei requisiti essenziali del CRA, finalizzati a dettagliarne ed espanderne le richieste in termini di specifiche di cybersicurezza.

Da una parte, l'attività progettuale ha analizzato ulteriori standard e sistemi di certificazione non ricoperti dalla mappatura ENISA; dall'altra, si è dettagliato il grado dell'indagine in un quadro analitico multilivello. Infatti, la realizzazione della componente tecnica della Guida è stata concepita come un processo sistematico, finalizzato a fornire

29. Joint Research Centre & ENISA 2024.

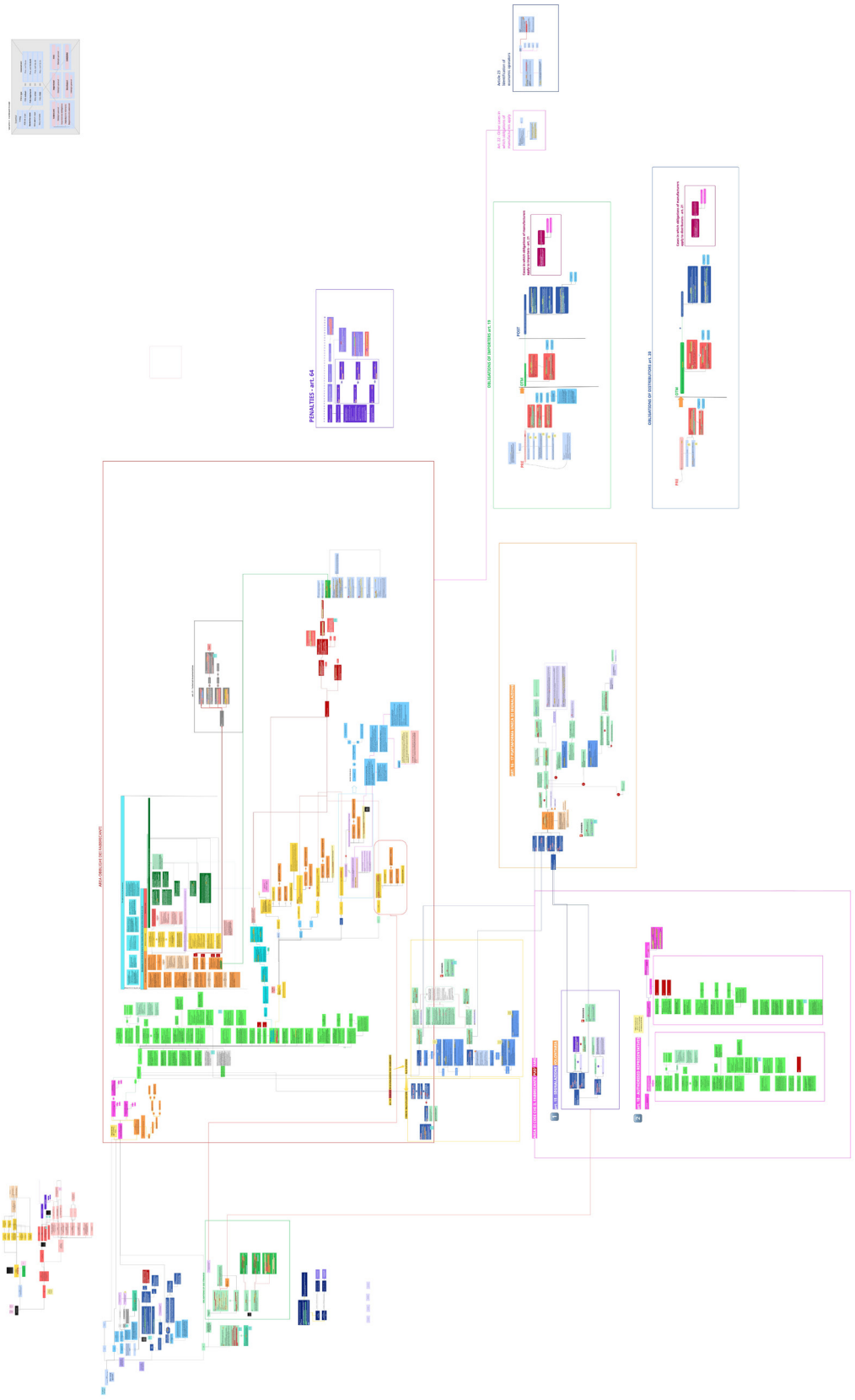

Fig. 1 — *Mappatura intera dei primi tre capi del Regolamento*

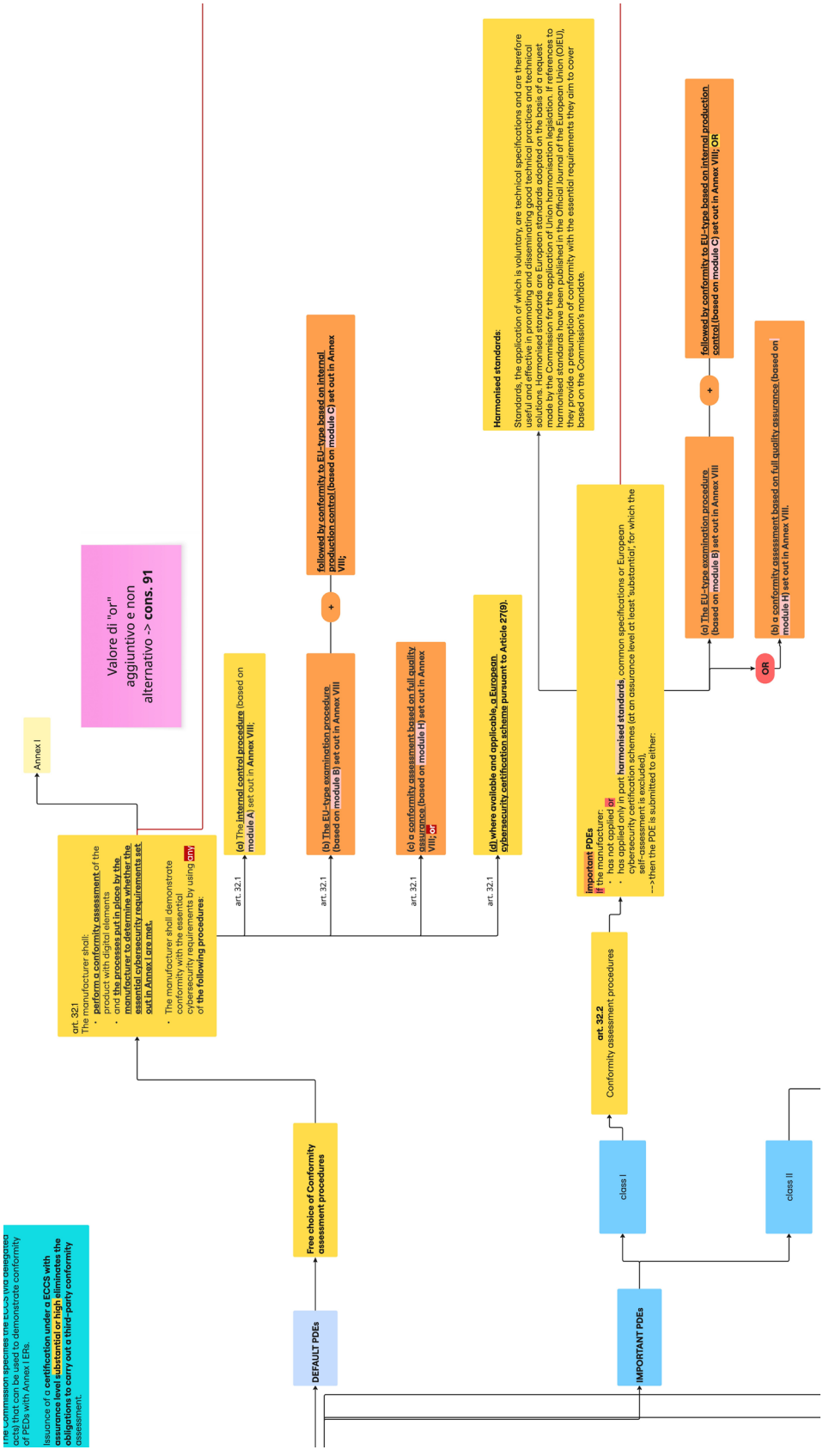

FIG. 2 — *Esempio di mappatura dei nodi semantici (Art. 32 – Procedure di valutazione della conformità)*

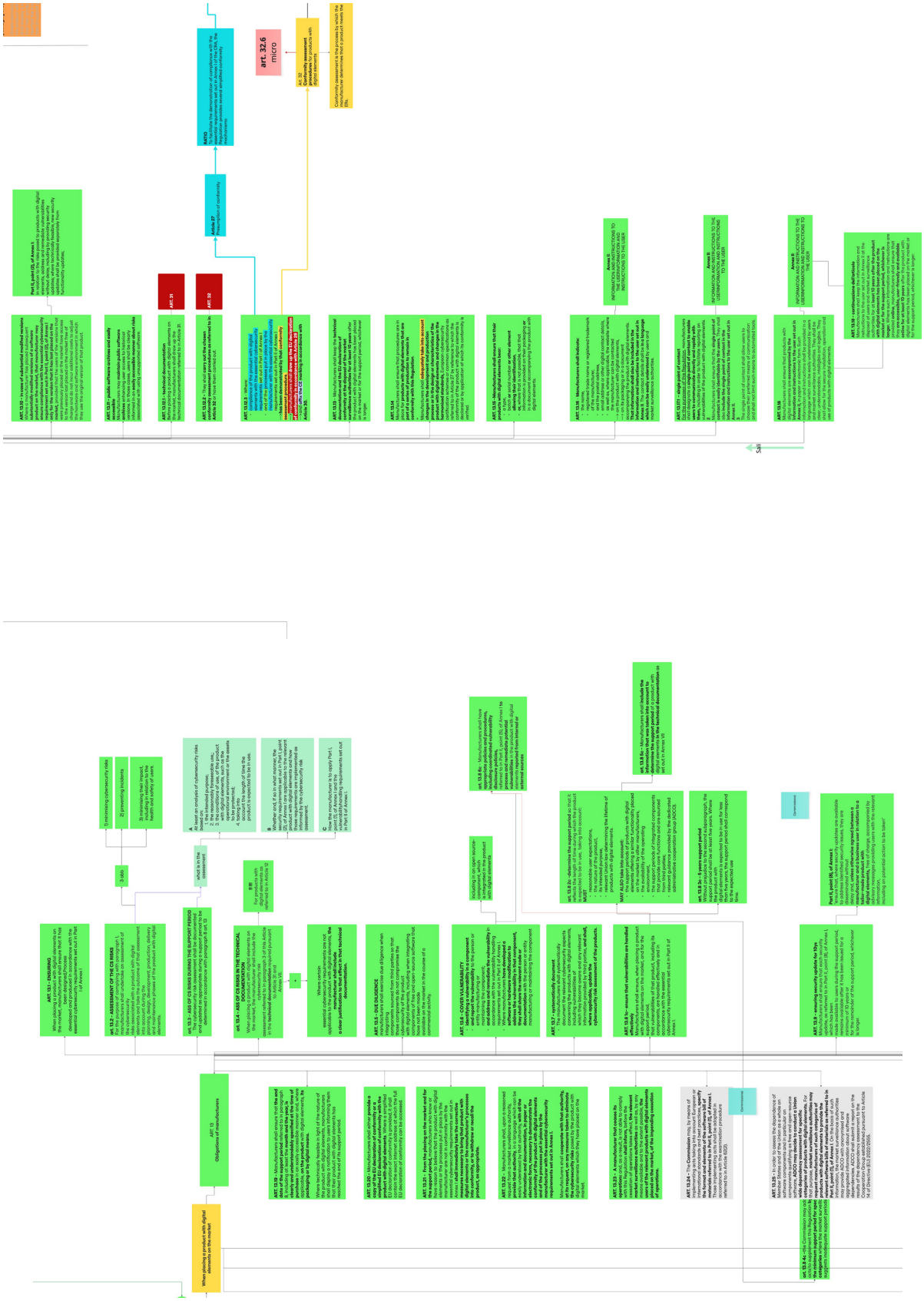

FIG. 3 — *Elenco consequenziale verticale di tutti i paragrafi dell'articolo 13*

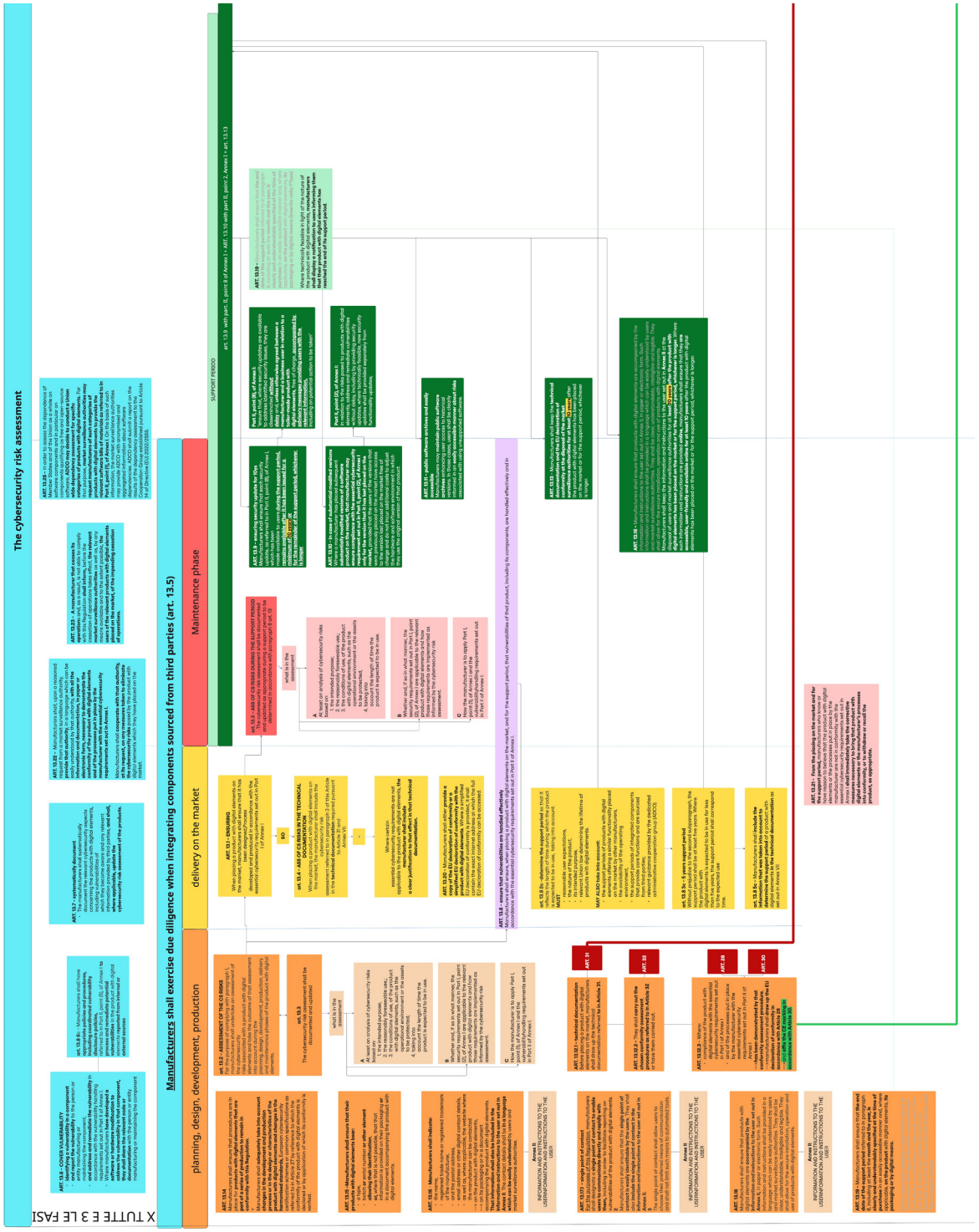

FIG. 4 — *Rappresentazione visiva, per fasi, dell'intero articolo 13*

una trasposizione operativa e strutturata dei requisiti del CRA in azioni concrete, tecnologie implementabili e riferimenti normativi ed istituzionali riconosciuti. L'obiettivo principale è stato quello di creare uno strumento di supporto pratico, ma al tempo stesso il più possibile rigoroso e completo, capace di tradurre la dimensione regolatoria del CRA in un insieme di attività tecniche e gestionali coerenti e immediatamente applicabili in contesti aziendali e industriali.

È necessario, tuttavia, notare che un corretto utilizzo della componente tecnica della Guida,

anche se completo ed esaustivo, non è da considerarsi come condizione sufficiente per raggiungere la conformità ai requisiti del CRA. Ai sensi dell'articolo 27 del Cyber Resilience Act, infatti, i prodotti con elementi digitali godono di una presunzione di conformità ai requisiti essenziali qualora rispettino gli standard armonizzati, le specifiche comuni adottate dalla Commissione attraverso atti di esecuzione, oppure siano certificati nell'ambito di schemi europei di certificazione della cybersicurezza. In attesa della pubblicazione di tali norme tecniche, i contenuti e le conclusioni presentati nel presente studio intendono contribuire al dibattito tecnico e scientifico che costituisce il fondamento del processo di standardizzazione e certificazione europea in materia di cybersicurezza.

In una prima fase, ogni requisito dell'Allegato I del CRA è stato analizzato e ampliato sulla base dei sotto-requisiti proposti da ENISA. Questo passaggio è stato fondamentale per garantire che la trattazione di ciascun requisito fosse completa, contestualizzata e coerente con le interpretazioni dell'Agenzia. A partire dai sotto-requisiti identificati, l'intero lavoro è stato organizzato secondo tre direttrici analitiche e complementari, che costituiscono la struttura portante della Guida dal punto di vista tecnico: 1. Attività & Principi; 2. Tecnologie & Strumenti; 3. Standard, linee-guida e migliori pratiche. Questa articolazione è stata progettata per rispondere alle diverse esigenze di chi, all'interno di un'organizzazione, si trova a dover implementare o supervisionare la conformità al CRA, dai profili manageriali ai tecnici operativi. La struttura tripartita della guida consente infatti di seguire un percorso logico e multilivello: il responsabile aziendale può individuare nella sezione "Attività e Principi" i processi necessari alla conformità; il team tecnico può approfondire la sezione "Tecnologie e Strumenti" per comprenderne le modalità di attuazione; infine, la sezione "Standard, linee-guida e migliori pratiche" permette di collocare le azioni intraprese all'interno di un quadro normativo di riferimento riconosciuto. In tal modo, la guida accompagna il lettore dal principio astratto (requisito essenziale) all'applicazione concreta, offrendo una visione completa e integrata dei requisiti del Cyber Resilience Act (Figura 5).

1) Attività e principi.

Relativamente alla prima direttrice, per ciascun requisito del CRA sono state individuate una serie di attività operative e di principi di sicurezza che un'organizzazione può mettere in atto per avvicinarsi alla soddisfazione dei vari requisiti. Ogni attività è formulata come un'azione operativa, ad esempio "Logging and Auditing" o "Authentication enforcement" o come principi di fondo, come il "Least Privilege", la "Defence-in-Depth" o il "Data Minimisation", fornendo una base teorica per la loro attuazione. Questa sezione consente quindi al lettore di identificare in modo immediato le azioni da intraprendere, costruendo una mappa chiara delle aree operative su cui intervenire per ciascun requisito normativo.

2) Tecnologie e strumenti.

La seconda direttrice, "Tecnologie e strumenti", traduce le attività precedenti in soluzioni pratiche e implementative. Per ogni attività individuata sono stati selezionati gruppi di tecnologie e strumenti da poter utilizzare al fine di implementare le attività proposte, fornendo anche esempi, ove possibile, di soluzioni open source. Questa scelta è motivata dal voler favorire la replicabilità e accessibilità delle soluzioni, dando modo al fruitore della guida di sperimentare strumenti spesso già ampiamente utilizzati, al fine di comprendere concretamente e tecnicamente le prescrizioni fornite dai requisiti del CRA. I gruppi di tecnologie sono organizzati per categoria funzionale (es. "Privileged Access Management solutions", "Host-based intrusion Detection systems", ecc.), in modo da consentire al lettore di poter individualmente approfondire le categorie ed individuare strumenti alternativi o complementari a seconda del proprio contesto operativo (IT, OT, IoT o embedded).

3) Standard, linee-guida e migliori pratiche.

La terza direttrice collega le due precedenti dimensioni operative al panorama normativo e regolamentare internazionale. Per ogni attività e requisito, la guida fornisce una selezione mirata di standard, framework e linee guida, scelte favorendo pubblicazioni di enti riconosciuti a livello internazionale ed europeo, quali ISO/IEC, NIST ed ENISA. Mentre il report ENISA fornisce principalmente riferimenti documentali relativi a noti standard pubblicati da ISO ed IEC, la Guida ha cercato di espandere questa sezione, includendo standard pubblicati da altri enti (es., NIST), oltre che citando migliori pratiche, linee-guida e framework in materia di cybersecurity (es., OWASP best

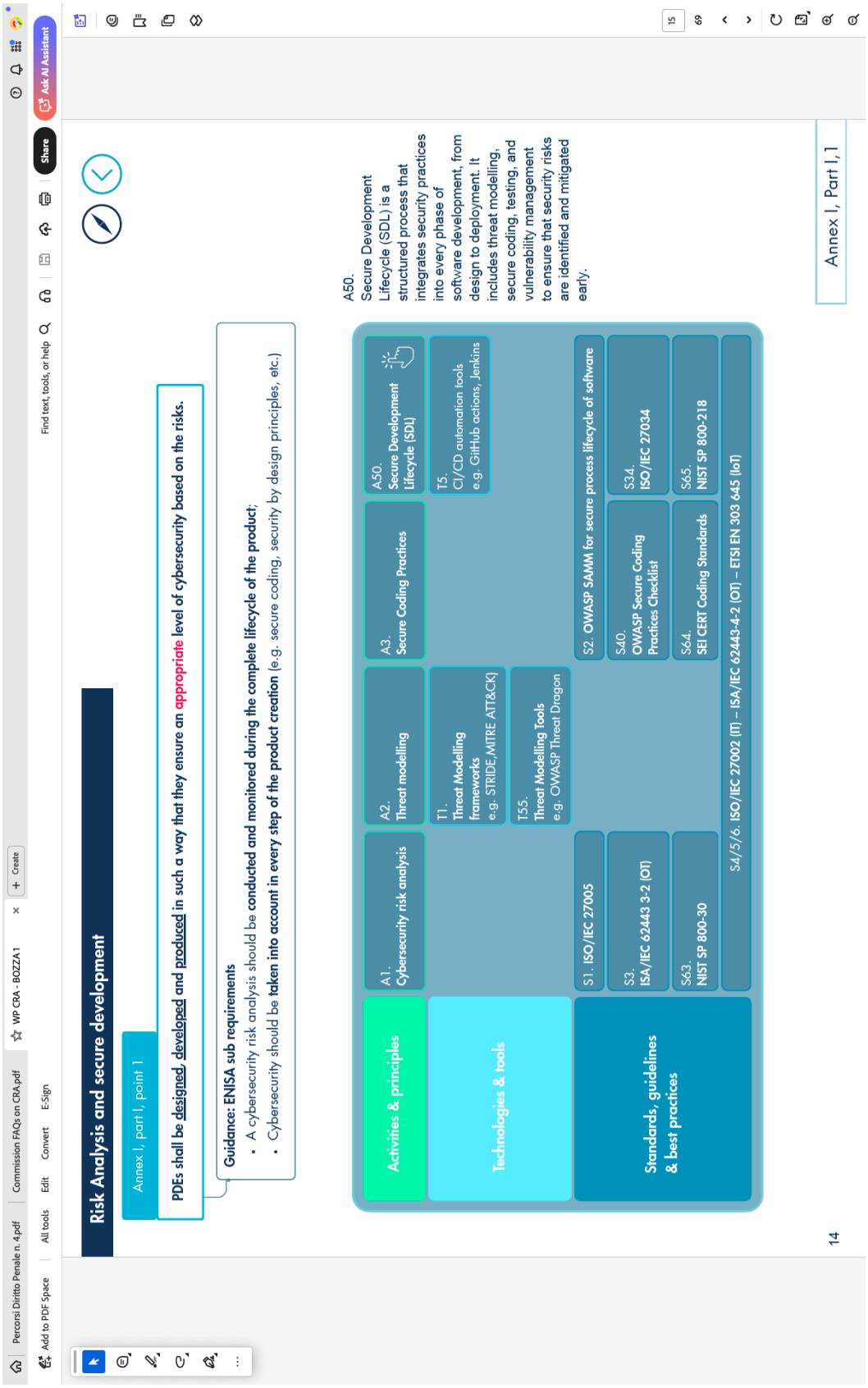

FIG. 5 — *Scheda sui requisiti essenziali ex Allegato I CRA*

practices, CIS benchmark), laddove ritenuti utili ai fini di una migliore comprensione dei requisiti del CRA. In particolare, sono stati analizzati nel dettaglio i requisiti (i.e., *Cybersecurity provisions*) proposti dalla versione 3.1.3 (la più recente a questa data) dell'ETSI EN 303 645, standard settoriale in materia di cybersicurezza per dispositivi IoT, e i requisiti (i.e., *Security practices*) definiti dalla versione 2 dell'OWASP SAMM, modello di maturità della sicurezza del software. Per ognuno dei requisiti definiti dagli standard citati, è stata identificata un'eventuale corrispondenza, forte o debole, con i requisiti del CRA, al fine di determinare standard specifici per vari settori (in questo caso rispettivamente IoT e sviluppo del software). Questo livello offre un fondamento normativo solido alle misure tecniche proposte, garantendo che siano in linea con gli standard internazionali più riconosciuti e fornisce al lettore un percorso di approfondimento autonomo, consentendogli di consultare le fonti ufficiali per estendere la propria conoscenza o per supportare futuri audit e processi di certificazione. La presenza di riferimenti incrociati, ad esempio tra *NIST SP 800-92* (per il log management) e *ISO/IEC 27002* (per i controlli di monitoraggio), permette inoltre di armonizzare il CRA con i framework esistenti, facilitando la convergenza tra compliance europea e standardizzazione globale.

2.3. Prototipazione

La rappresentazione grafica non ha seguito rigidamente l'ordine sistematico del regolamento, ma si è invece conformata a un criterio logico-procedurale di compliance, costruito attorno al ciclo di adempimento che l'operatore è tenuto a rispettare. Tale impostazione ha consentito di preservare la coerenza con la ratio e la struttura giuridica delle disposizioni, evitando al contempo una riproduzione meramente descrittiva del testo normativo[30]. Parallelamente, si è proceduto a un'ulteriore rifinitura dei testi, cioè un controllo terminologico e concettuale volto a garantire la fedeltà giuridica delle formulazioni, assicurando coerenza con la terminologia ufficiale del regolamento e con i principi generali del diritto dell'Unione europea in materia di armonizzazione tecnica e responsabilità degli operatori economici.

Così, riprendendo l'esempio dell'articolo 13 del regolamento, il prototipo della Guida ha tradotto graficamente il lavoro concettuale della precedente fase di mappatura. Come mostrato dalla Figura 6, la tavola racchiude al suo interno gli elementi ritenuti utili a orientare l'utente rispetto al frammento di regolamento oggetto di analisi. In alto a sinistra, la barra blu indica il *topic* specifico dell'articolo trattato, mentre nella parte inferiore destra lo stesso articolo è evidenziato per facilitarne il riconoscimento immediato. In alto a destra si trovano invece due strumenti di navigazione interattiva: l'icona color petrolio, che consente di tornare rapidamente all'ultima pagina visualizzata, agevolando la consultazione di sezioni correlate senza perdere la pagina di partenza; e l'icona blu, che permette di ritornare alla *dashboard* iniziale, una mappa dei contenuti del Regolamento, dalla quale è possibile accedere direttamente alle categorie, articoli o allegati di interesse. La parte centrale della tavola, che ne costituisce il fulcro visivo, è dedicata alla rappresentazione dell'articolo o di più articoli tra loro concettualmente connessi, riportati sempre sul margine sinistro. Questi sono affiancati, al centro, dai *box* contenenti il testo normativo, corredato da elementi grafici che ne facilitano la lettura lineare e la comprensione concettuale. All'occorrenza, sono state inserite anche icone segnaletiche che fungono da punti di attenzione, per evidenziare passaggi chiave contenuti nel testo normativo o peculiari procedure e adempimenti. I rinvii presenti nelle disposizioni analizzate all'Allegato I del regolamento, contenente i requisiti essenziali, sono rappresentati graficamente sotto forma di *box* che, se "cliccato", conduce all'apposita sezione nella Guida sui requisiti essenziali. L'uso dei colori, poi, è stato calibrato in modo pienamente funzionale alla comprensione cognitiva e intuitiva del contenuto: si è scelto, pertanto, di impiegare tinte distinte e non gradienti di una medesima palette, così da evidenziare visivamente le differenze concettuali e funzionali tra gli elementi rappresentati. Ad esempio, operando in questo senso, sono stati scelti tre colori nettamente differenti (rosso, verde, petrolio) per chiarire in quale delle tre fasi identificate sopra il singolo obbligo analizzato si trova. Con la stessa logica sono stati applicati i grassetti e gli evidenziatori cromatici per mettere in rilievo termini e

30. Koulu–Pohle 2024, p. 5.

locuzioni giuridicamente rilevanti, garantendo una lettura stratificata che agevola sia la consultazione esperta sia quella operativa.

La Figura 7 illustra come l'approccio metodologico adottato sia stato concretamente operazionalizzato nella Guida. Essa rappresenta un chiaro esempio del fatto che il lavoro di "ricomposizione" normativa non ha seguito una mera progressione numerica e sequenziale degli articoli o dei paragrafi, ma ha invece privilegiato una logica di flusso ragionato, capace di valorizzare la connessione funzionale tra gli obblighi previsti (vedi sezione 2.2). Come si evince dalla Figura, infatti, i paragrafi riportati non seguono l'ordine originario dell'articolo, ma vengono collocati in base alla fase (progettazione e sviluppo, immissione sul mercato, e mantenimento) in cui i relativi obblighi devono essere adempiuti. Tale rappresentazione, frutto di una lettura sistematica del testo giuridico e di una precisa disposizione cromatica e spaziale degli elementi, consente di visualizzare le relazioni logiche e temporali tra gli adempimenti, evidenziando al contempo le interdipendenze e i rimandi interni al Regolamento. In questo modo, la Guida consente di passare da una struttura normativa rigidamente testuale a una struttura cognitiva e processuale, che rispecchia la concreta sequenza di azioni e verifiche che i fabbricanti sono chiamati a svolgere.

Una critica che può essere mossa alla Guida, come ad altri progetti di legal design, è che una comunicazione grafica-visuale di contenuti giuridici potrebbe comportare il rischio significativo di non cogliere tutte le sfumature del discorso normativo[31]. Ciò, in particolare, per due ragioni. Da un lato, l'uso di tecniche di plain language[32] (volte a semplificare il linguaggio e a ridurre la densità sintattica) e, dall'altro, l'impiego di elementi grafici (come schemi, infografiche, icone o mappe concettuali) introducono un doppio livello di sforzo cognitivo per l'utente finale. Prima di poter accedere al contenuto, infatti, l'utente deve comprendere la logica strutturale e visiva dello schema, cioè il nuovo "modo di leggere" che esso impone, e solo successivamente può concentrarsi sul testo che vi è inserito. In questo processo, il rischio concreto è che alcune sfumature normative come rimandi, condizioni o relazioni tra disposizioni, non vengano pienamente colte: la mente, impegnata a decifrare la forma grafica, può distogliere attenzione dal contenuto giuridico, con la conseguenza di attenuarne o distorcerne il significato. Paradossalmente, quindi, un testo normativo privo di elementi grafici, e dunque più vicino a ciò che l'utente è storicamente abituato a leggere, ma rifinito attraverso sole tecniche di plain language, può costituire un intervento di legal design persino più efficace rispetto all'adozione estesa di componenti visuali.

Nel nostro lavoro, tuttavia, abbiamo scelto un approccio di equilibrio. Da un lato, l'intervento sul testo normativo è stato mirato: abbiamo operato soltanto nei passaggi che presentavano maggiore complessità sintattica (ad esempio, per la lunghezza dei periodi, l'uso di termini densi o di numerosi rimandi interni) evitando di sostituire integralmente il testo con una versione in *plain language*. Gran parte delle disposizioni è rimasta invariata, ove ritenuta già chiara e coerente con la terminologia e la logica del regolamento. Dall'altro lato, l'integrazione di schemi e altri elementi grafici è stata sempre accompagnata da una legenda esplicativa iniziale, volta a orientare l'utente nella lettura del modello visuale. Tale indicazione specifica come interpretare i diversi elementi grafici e logici, ricorrendo a strumenti di chiarezza percettiva (come grassetti, frecce, colori ben differenziati) per distinguere concetti, categorie e condizioni. Dunque, l'intento è stato quello di ridurre il carico cognitivo legato all'introduzione di una struttura visiva inedita, preservando al contempo la fedeltà giuridica, la precisione terminologica e una maggiore navigabilità dell'informazione normativa.

Inoltre, grazie alla fase di ricerca preliminare e, in particolare, ai risultati emersi dalla survey condotta sui destinatari del regolamento, è stato possibile mappare il percorso logico-pratico che gli utenti seguono per comprendere il nuovo testo normativo. Non sorprende che il regolamento rappresenti il primo punto di riferimento cui essi si rivolgono, al fine di acquisire un quadro istituzionale e completo del precetto normativo. Solo in un secondo momento gli utenti tendono a effettuare ricerche mirate presso fonti ed enti autorevoli, per ottenere chiarimenti operativi e guide interpretative che agevolino la corretta applicazione della normativa. In questo

31. Rossi–Palmirani 2020.

32. Ducato–Strowel 2021.

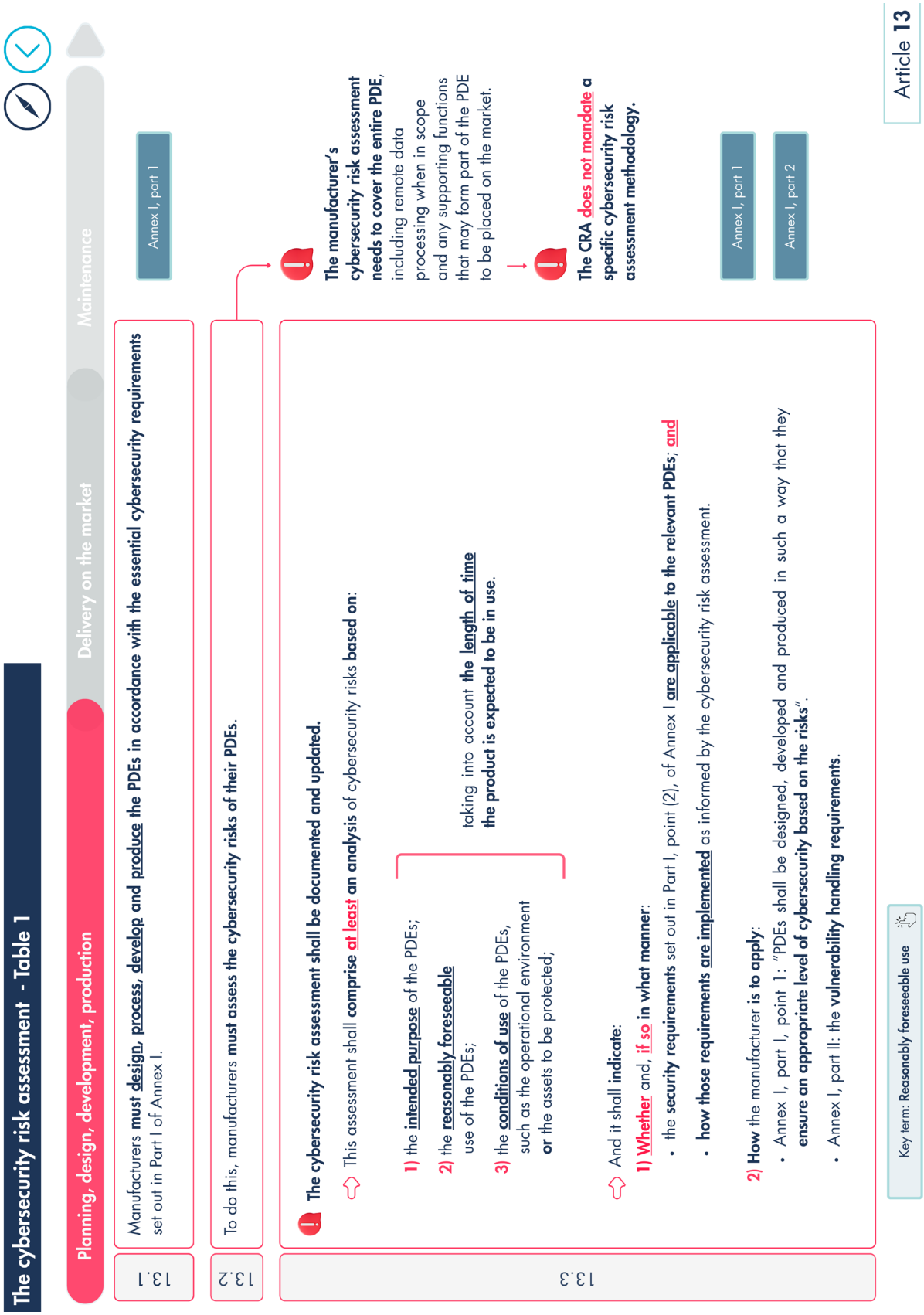

Fig. 6 — *Prima tavola articolo 13 CRA*

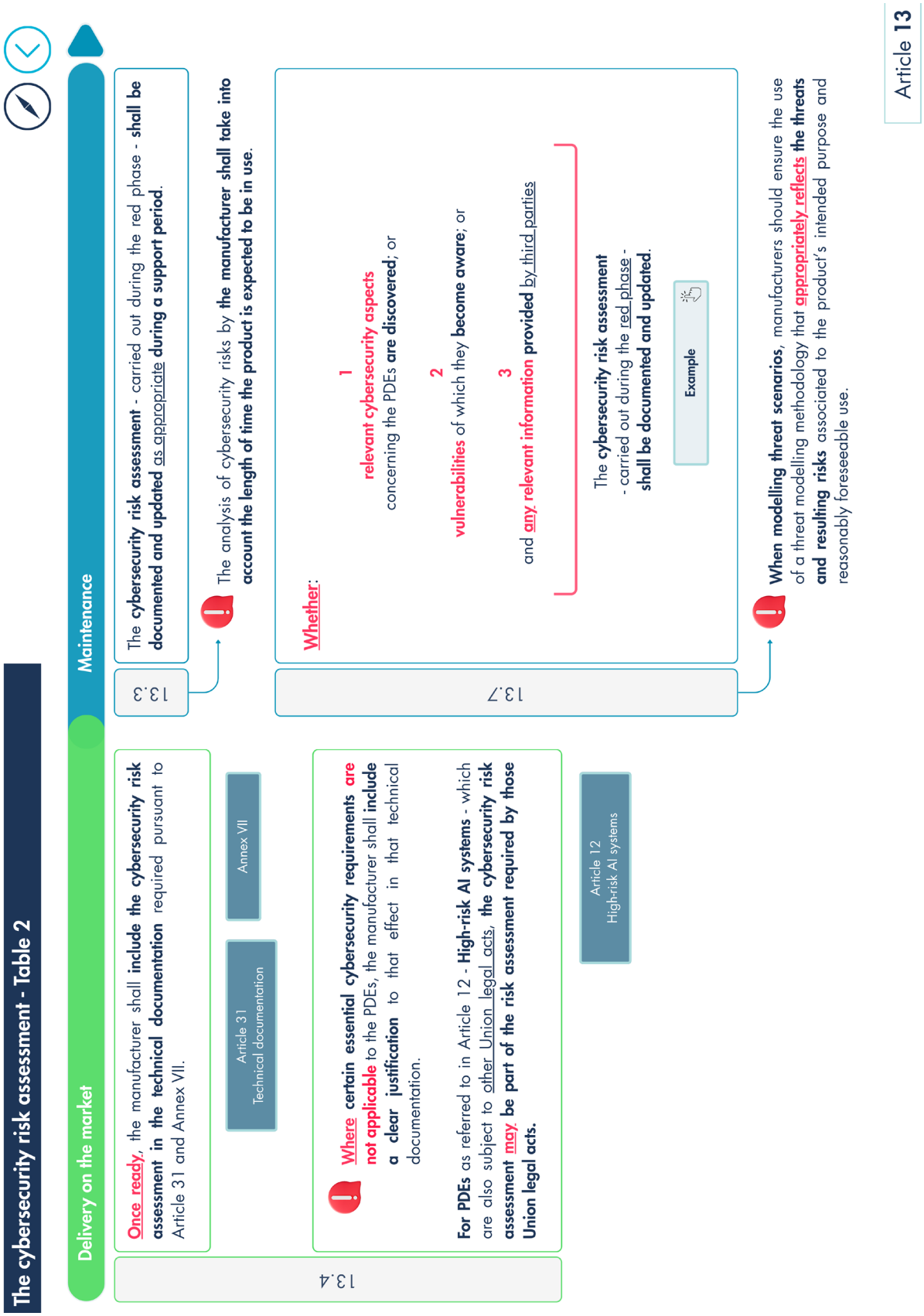

FIG. 7 — *Seconda tavola articolo 13 CRA*

senso, riteniamo che l'approccio da noi proposto non sia da intendersi in un'ottica di sostituzione del testo normativo, quanto di complementarietà[33]: gli elementi visuali della struttura compliance-friendly del regolamento, che evidenzia raccordi e sinergie tra disposizioni e meccanismi logicamente collegati (es., condizioni, criteri, ecc.), chiariscono e migliorano la fruibilità e navigazione dell'informazione contenuta nella norma[34].

2.4. User test

Questa fase ha previsto nuovamente il coinvolgimento dei soggetti che hanno partecipato alla survey nella prima fase, nonché di altri soggetti dalle diverse formazioni (es., consulenti tecnici; giuristi; informatici; responsabili aziendali), al fine di testare il prototipo, valutandone l'efficacia comunicativa e la fruibilità operativa. Questo passaggio di validazione empirica[35] basato sull'esperienza del settore privato è essenziale per evitare che la Guida diventi "solamente" un costrutto teorico privo di applicabilità pratica. I feedback raccolti, sia sul piano percettivo-visivo, sia concettuale-logico, hanno consentito di apportare le necessarie modifiche e ottimizzazioni in vista del rilascio definitivo della Guida.

2.5. Miglioramento & Lancio

In questa fase finale sono state apportate le modifiche necessarie alla luce dei feedback emersi nella fase precedente. Inoltre, sono state completate le attività necessarie al rilascio della Guida e alla sua diffusione, incluse la predisposizione di un sito web con dominio Unibo[36] dedicato al progetto che accoglie la Guida e la documentazione pertinente. Ancorché non sia formalmente richiesto dalla governance del Partenariato Esteso SERICS[37] che i prodotti della ricerca condotta all'interno dei progetti afferenti al Partenariato siano pubblicati in open access, la Guida è stata rilasciata in modalità aperta, con licenza CC-BY-NC-SA[38], per due ordini di ragioni. In primo luogo, riteniamo giusto che il prodotto di una ricerca finanziata con fondi pubblici sia liberamente disponibile alla collettività, in linea con i principi che sorreggono il movimento del libero accesso alla conoscenza[39]. In secondo luogo, la scelta dell'open access garantisce la massima diffusione e accessibilità della ricerca, permettendo pertanto la possibilità di raggiungere il più alto numero di destinatari della Guida (in particolare, gli operatori economici, molti dei quali potrebbero essere PMI). Connesso a ciò, per garantire una maggior diffusione dello strumento, la Guida è stata inizialmente prodotta in lingua inglese; peraltro, i fondi che hanno permesso lo sviluppo della Guida derivano da risorse finanziate dal piano dell'Unione europea Next Generation EU. In una fase successiva del progetto, è prevista una traduzione in italiano della stessa per un maggior allineamento al mercato nazionale. Un altro passaggio successivo al rilascio della Guida è legato alla sua trasformazione da file PDF interattivo a web tool interattivo, al fine di permettere una navigazione tra i contenuti più immersiva e intuitiva.

3. Conclusioni

Nel contesto attuale di "ipertrofia normativa" nell'ambito digitale[40], o di "tsunami di legislazione digitale"[41], le imprese sono sempre più destinatarie di oneri normativi e regolamentari, i quali

33. Ducato–Strowel–Marique 2024.
34. Perondi 2024.
35. Lewrick–Link–Leifer 2018; Lewrick-Link-Leifer 2020.
36. https://site.unibo.it/cybersecurity-legal-lab.
37. Decreto Direttoriale MUR, n. 1556 dell'11 ottobre 2022, con risorse a valere sull'Avviso Decreto Direttoriale 15 marzo 2022 n. 341, in attuazione dell'Investimento 1.3, finanziato dall'Unione europea - NextGenerationEU - nell'ambito della Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" del Piano Nazionale di Ripresa e Resilienza.
38. Si veda nel sito di Creative Commons il codice legale della licenza Attribuzione – NonCommerciale - CondividiAlloStessoModo 4.0 Internazionale.
39. Caso 2022.
40. Papakonstantinou–De Hert 2024.
41. EDRi 2022.

risultano particolarmente costosi per le PMI[42]. I molteplici e diversi obblighi derivanti dalla regolamentazione del digitale di matrice eurounitaria (ma anche nazionale, in realtà) spesso risultano particolarmente complessi da tradurre in indicazioni operative per raggiungere il desiderato stato di conformità. Ciò è riconducibile non solo alla novità del perimetro normativo stesso, ma anche all'interazione tra l'elemento tecnico-giuridico e quello tecnico-informatico. Il regolamento europeo Cyber Resilience Act non è un'eccezione in tal senso. Anzi, ne costituisce forse la più chiara espressione.

La Guida al CRA qui presentata, con un'attenzione particolare soprattutto alla sua metodologia, alle varie fasi, cioè, che hanno costituito la sua ideazione e sviluppo, mira pertanto a risolvere le principali criticità interpretative dell'atto giuridico da parte degli operatori attraverso l'implementazione di principi e tecniche di legal design. Per quanto sia ancora prematura una valutazione in ordine all'impatto di tale strumento sul mercato, riteniamo che la diffusione e l'adozione di questa metodologia, e quindi per estensione di questi strumenti, possa rappresentare un elemento importante anche nell'ottica degli obiettivi di semplificazione della complessità (e quindi dei costi) della cd. "normativa digitale" dell'Ue, uno dei cardini politici del secondo mandato della presidente della Commissione europea Von der Leyen attraverso il cd. "pacchetto Omnibus"[43].

Riferimenti bibliografici

R. Caso (2022), *Open data, ricerca scientifica e privatizzazione della conoscenza*, in "Il Diritto dell'Informazione e dell'Informatica", 2022, n. 4-5

P. G. Chiara (2025), *Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?*, in "European Journal of Risk Regulation", vol. 16, 2025, n. 2

P.G. Chiara (2022), *Commission Delegated Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices*, in "European Data Protection Law Review", vol. 8, 2022, n. 1

Commissione europea (2025), *Omnibus package*, in "Simplifying the Single Market", single-market-economy.ec.europa.eu

Commissione europea (2022), *La guida blu all'attuazione della normativa UE sui prodotti 2022*, 2022/C 247/01

M. Draghi (2024), *The future of European competitiveness: a competitiveness strategy for Europe*, in commission.europa.eu, 2024

R. Ducato, A. Strowel (eds.) (2021), *Legal Design Perspectives. Theoretical and Practical Insights from the Field*, Ledizioni, 2021

R. Ducato, A. Strowel, E. Marique (eds.) (2024), *Design(s) for Law*, Ledizioni, 2024

EDRi (2022), *How it started, how it's going: Halfway through the current European Commission's legislative term*, in "edri.org", 2022

Garante per la Protezione dei Dati Personali (2025), *Rendere le informative privacy più chiare e rapidamente comprensibili – il Legal Design come approccio rivolto all'utente*, in "www.igsg.cnr.it", 2025

M. Hagan (2020), *Legal design as a thing: A theory of change and a set of methods to craft a human-centered legal system*, in "Design Issues", vol. 36, 2020, n. 3

42. Draghi 2024, p. 30 e 68-69.

43. Commissione europea 2025.

Joint Research Centre & ENISA (2024), *Cyber Resilience Act Requirements Standards Mapping*, Publications Office of the European Union, 2024

I. Kamara (2025), *Standardising personal data protection*, Oxford University Press, 2025

R. Koulu, J. Pohle (2024), *Legal Design Patterns: New Tools for Analysis and Translations Between Law and Technology*, in "Digital Society", vol. 3, 2024, n. 22

Legal Design Alliance (2018), *The Legal Design Manifesto v 1.0*, in "www.legaldesignalliance.org", 2018

M. Lewrick, P. Link, L. Leifer (2020), *The Design Thinking Toolbox. A Guide to Mastering the Most Popular and Valuable Innovation Methods*, Wiley, 2020

M. Lewrick, P. Link, L. Leifer (2018), *The Design Thinking Playbook. Mindful Digital Transformation of Teams, Products, Services, Businesses and Ecosystems*, Wiley, 2018

A. Mantelero, G. Vaciago, M.S. Esposito, N. Monte (2020), *The common EU approach to personal data and cybersecurity regulation*, in "International Journal of Law and Information Technology", vol. 28, 2020, n. 4

C.F. Mondschein (2016), *Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12 (1) and (7) GDPR*, in "European Data Protection Law Review", vol. 2, 2016, n. 4

V. Papakonstantinou, P. De Hert (2024), *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play*, Routledge, 2024

L. Perondi (2024), *La forma grafica del testo*, in B. Pasa, G. Sinni (a cura di), "Transparency by Design. Incontro interdisciplinare sul principio di trasparenza dei dati personali" (Venezia, 19 dicembre 2022), Bembo Officina Editoriale, 2024

A. Rossi, M. Palmirani (2020), *Can visual design provide legal transparency? The challenges for successful implementation of icons for data protection*, in "Design Issues", vol. 36, 2020, n. 3

A. Rossi, R. Ducato, H. Haapio, S. Passera (2019), *Legal Design Patterns: Towards A New Language for Legal Information Design*, in E. Schweighofer, F. Kummer, A. Saarenpää (eds.), "Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS 2019", Weblaw ed., 2019

A. Rossi, H. Haapio (2019), *Proactive Legal Design: Embedding Values in the Design of Legal Artefacts*, in E. Schweighofer, F. Kummer, A. Saarenpää (eds.) "Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS 2019", Weblaw ed., 2019

M. Rundle (2006), *International Personal Data Protection and Digital Identity Management Tools*, in "Berkman Center Research Publication" No. 2006–06, 2006

F. Teichmann, B.S. Sergi (2025), *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in "Computer Law & Security Review", vol. 59, 2025