

CERIDAP

RIVISTA INTERDISCIPLINARE SUL
DIRITTO DELLE
AMMINISTRAZIONI PUBBLICHE

Estratto

FASCICOLO
2 / 2026

APRILE - GIUGNO

Diritto delle tecnologie Quantum. Sfide regolatorie

Andrea Crismani

DOI: 10.13130/2723-9195/2026-2-41

Il saggio propone alcune riflessioni sul diritto delle tecnologie quantistiche, campo di studio entrato nell'agenda regolatoria europea nel 2025 con la proclamazione dell'Anno Internazionale ONU della Scienza e Tecnologia Quantistica e l'adozione, da parte della Commissione, della Quantum Europe Strategy. La tesi sostenuta è che la disciplina delle tecnologie quantistiche non richieda soltanto un nuovo atto legislativo, ma una ricostruzione multilivello del rapporto tra norme vigenti, standard tecnici e strumenti di industrial policy: il Quantum Act, annunciato per il 2026, dovrebbe funzionare non come codice settoriale autosufficiente, ma come norma di raccordo tra sicurezza, innovazione, certificazione e sovranità tecnologica. Il contributo distingue gli ambiti in cui la normativa esistente richiede adattamento interpretativo (GDPR, eIDAS 2, Reg. UE 2021/821, NIS2, Dir. UE 2024/2853) dagli ambiti ancora privi di sistemazione organica (certificazione integrata, coordinamento QKD/PQC, regime brevettuale dei protocolli quantistici), e li colloca nel più ampio quadro del diritto amministrativo dell'innovazione tecnologica.

Towards a law of quantum technologies: existing rules, regulatory gaps and prospects of the European Quantum Act

This essay offers a first systematic reconstruction of the law of quantum technologies, a field of scholarship that became firmly established on the European regulatory agenda in 2025 with the United Nations proclamation of the International Year of Quantum Science and Technology and the adoption, by the European Commission, of the Quantum Europe Strategy. The central thesis is that the regulation of quantum technologies requires not only a new European legislative act, but a multi-level reconstruction of the interplay between existing rules, technical standards and industrial policy instruments: the Quantum Act, announced for 2026, should function not as a self-contained sectoral code, but as a coordinating instrument between security, innovation, certification, and technological sovereignty. The

contribution distinguishes the areas in which existing rules require interpretative adaptation (GDPR, eIDAS 2, Reg. EU 2021/821, NIS2, Dir. EU 2024/2853) from those still lacking organic systematisation (integrated certification, QKD/PQC coordination, patent regime of quantum protocols), and locates them within the broader framework of the administrative law of technological innovation.

Sommario: 1. Premessa. L'emergere di un campo.- 2. Profilo metodologico. Le due dimensioni del diritto delle tecnologie quantistiche.- 3. Le tecnologie quantistiche come infrastrutture strategiche.- 3.1. La Quantum Europe Strategy.- 3.2. Il Quantum Act: industrial policy o product-safety?- 3.3. La cornice nazionale.- 4. Il diritto delle tecnologie quantistiche nel quadro del diritto dell'innovazione.- 4.1. L'innovazione come funzione amministrativa.- 4.2. Precauzione, innovazione e neutralità tecnologica.- 4.3. Golden Power e tecnologie critiche.- 4.4. La regulatory sandbox come modello applicabile.- 5. La normativa esistente da riconsiderare.- 5.1. Quanto del modello AI Act è trasferibile al quantum?- 5.2. Protezione dei dati personali: l'art. 32 GDPR e la riqualificazione dello "stato dell'arte".- 5.3. Identità digitale e prova documentale: eIDAS 2 e la firma qualificata.- 5.4. Controlli all'export e dual-use: il Regolamento (UE) 2021/821.- 5.5. Cybersicurezza delle infrastrutture critiche: NIS2 e PSNC.- 5.6. Responsabilità da prodotto: la Direttiva (UE) 2024/2853.- 6. Gli ambiti regolatori ancora privi di sistemazione organica.- 6.1. Verso un sistema integrato di certificazione delle tecnologie quantistiche.- 6.2. Il quadro giuridico della transizione quantum-safe: QKD e PQC.- 6.3. Il regime brevettuale dei "quantum-implemented inventions".- 7. Verso un Quantum Act europeo: una proposta di architettura.- 8. Conclusioni.

1. Premessa. L'emergere di un campo

Le riflessioni proposte in queste pagine hanno per oggetto i nodi giuridici che la diffusione delle tecnologie quantistiche pone all'ordinamento, in un momento di rapida evoluzione del quadro regolatorio europeo^[1]. L'Assemblea Generale delle Nazioni Unite ha proclamato il 2025 "International Year of Quantum Science and Technology", ricorrendo al centesimo anniversario della prima formulazione della teoria dei quanti^[2]. La ricorrenza non è meramente simbolica: nel medesimo

arco temporale la Commissione europea ha adottato, il 2 luglio 2025, una *Quantum Europe Strategy*^[3] e ha annunciato per il 2026 la presentazione di una proposta di *European Quantum Act*^[4]. Il 2025 non segna dunque la nascita di una riflessione giuridica sulle tecnologie quantistiche – contributi specialistici si sono susseguiti nei tempi^[5] – ma la sua stabilizzazione istituzionale: il passaggio dal dibattito accademico alla costruzione di un quadro regolatorio europeo dedicato. Si proverà a mostrare che la disciplina delle tecnologie quantistiche non richiede soltanto un nuovo atto legislativo europeo, ma una ricostruzione multilivello del rapporto tra norme vigenti, standard tecnici e strumenti di “*industrial policy*”. Il problema, in altre parole, non è stabilire se serva un diritto speciale del quantum, ma individuare quali parti dell’ordinamento vigente siano già idonee, quali richiedano adattamento interpretativo e quali invece impongano disciplina nuova. Il *Quantum Act*, in questa prospettiva, dovrebbe funzionare non come codice settoriale autosufficiente, ma come norma di raccordo tra sicurezza, innovazione, certificazione e sovranità tecnologica.

Ancora una precisazione preliminare. Nella dottrina straniera ha iniziato a circolare la formula “*quantum law*”, talvolta resa in italiano come “diritto quantistico”. L’espressione è suggestiva ma forse equivoca: in Italia il sintagma “quantistico” applicato al diritto evoca soprattutto la fortunata metafora epistemologica di Roberto Bin sulla teoria delle fonti, che utilizza la fisica quantistica come modello interpretativo dell’indeterminazione giuridica^[6]. È un uso del tutto diverso da quello qui in esame, che riguarda la disciplina giuridica positiva delle tecnologie basate sulla meccanica quantistica. Per evitare equivoci, e in attesa di un’eventuale stabilizzazione terminologica, in questo saggio si utilizzerà preferibilmente l’espressione “*diritto delle tecnologie quantistiche*”.

2. Profilo metodologico. Le due dimensioni del diritto delle tecnologie quantistiche

La ricostruzione che segue distingue due dimensioni che il diritto delle tecnologie quantistiche è chiamato a coprire, e che fungono da chiave di lettura dell’intero saggio.

La prima dimensione è quella della normativa esistente da riconsiderare. Sono norme già in vigore che continueranno ad applicarsi alle tecnologie quantistiche,

ma il cui significato e la cui applicazione concreta sono destinati a mutare per effetto del nuovo paradigma tecnologico. Sono norme nate per disciplinare l'informatica classica, la crittografia asimmetrica tradizionale, le infrastrutture deterministiche, e che ora si trovano a regolare fenomeni dotati di proprietà strutturalmente diverse: la natura probabilistica del calcolo quantistico, la vulnerabilità delle cifrature classiche all'algoritmo di Shor, la non-clonabilità degli stati quantistici, la possibilità di canali fisicamente sicuri per la distribuzione di chiavi. In questa dimensione il giurista è chiamato a un'opera di reinterpretazione e adattamento, talora di vera e propria riqualificazione concettuale.

La seconda dimensione è quella degli ambiti regolatori ancora privi di sistemazione organica. Non si tratta, a rigore, di norme inesistenti: esistono già standard tecnici di rilievo (ETSI GS QKD 016, ISO/IEC 23837, ISO/IEC 4879:2024, *infra*), comitati di standardizzazione attivi (CEN/CLC JTC 22, ISO/IEC JTC 3, *infra*) e prassi brevettuale consolidata in ambiti contigui. Mancherebbe però un quadro integrato, cogente e specificamente coordinato, che il *Quantum Act* in formazione e gli strumenti tecnico-normativi di standardizzazione sono chiamati a costruire. Vi rientrano il sistema di certificazione delle tecnologie quantistiche, il coordinamento giuridico tra “*Quantum Key Distribution*” (QKD) e “*Post-Quantum Cryptography*” (PQC) il regime brevettuale specifico dei “*quantum-implemented inventions*”.

Le due dimensioni non sono nettamente separate: l'adattamento della normativa esistente può richiedere modifiche legislative espresse, mentre la costruzione di nuovi quadri regolatori si appoggia inevitabilmente sui principi già consolidati. Tuttavia, la distinzione è utile: aiuta a non confondere ciò che il diritto può già fare attraverso l'interpretazione con ciò che richiede un intervento del legislatore.

3. Le tecnologie quantistiche come infrastrutture strategiche

Una questione teorica preliminare attraversa l'intera materia: quando una tecnologia emergente diventa “*infrastruttura strategica*” per il diritto pubblico? La risposta, nel diritto dell'Unione è oggi affidata a tre indici convergenti: l'inclusione nella Raccomandazione (UE) 2023/2113 della Commissione sui settori tecnologici critici per la sicurezza economica dell'Unione; la qualificazione

politica nei documenti programmatici della Commissione (in particolare la “*Competitiveness Compass*” e le strategie di settore); l’inclusione nei perimetri applicativi degli strumenti di protezione degli asset strategici (Reg. UE 2019/452 sul *foreign investment screening*; Reg. UE 2021/821 sul *dual-use*) e nei regimi nazionali di poteri speciali (in Italia, il d.l. n. 21/2012).

3.1. La Quantum Europe Strategy

La Comunicazione COM(2025) 363 final, recante “*Quantum Europe Strategy: Quantum Europe in a Changing World*”, costituisce il documento di indirizzo politico che ha aperto la fase attuale^[7]. Essa muove dalla constatazione che, nonostante l’eccellenza della ricerca europea, l’Unione sconta una difficoltà strutturale nel tradurre il proprio vantaggio scientifico in capacità industriale e quote di mercato, anche a causa della frammentazione delle strategie nazionali degli Stati membri. La Strategia individua cinque aree di azione interconnesse – ricerca e innovazione; infrastrutture quantistiche; rafforzamento dell’ecosistema; tecnologie quantistiche per lo spazio e “*dual-use*” (sicurezza e difesa); competenze – con l’obiettivo dichiarato di trasformare l’Unione in “*quantum industrial powerhouse*” entro il 2030^[8].

Due passaggi della Comunicazione hanno particolare rilievo per il giurista. Anzitutto la Strategia inserisce le tecnologie quantistiche tra i “*key tech sectors that will matter in tomorrow’s economy*” nel quadro della *Competitiveness Compass*^[9]. In secondo luogo, la Strategia precisa che, ai propri fini, “*dual-use potential*” denota la capacità delle tecnologie quantistiche di servire sia fini civili sia fini di sicurezza/difesa, ed è impiegato in un senso più ampio e prospettico rispetto al termine giuridico “*dual-use items*” di cui al Regolamento (UE) 2021/821^[10]. Si tratta di un’autoqualificazione politica che eccede la portata definitoria del regolamento europeo sul controllo all’export, e che orienta l’intera architettura strategica verso il paradigma dell’autonomia strategica aperta e della resilienza infrastrutturale dell’Unione.

3.2. Il Quantum Act: industrial policy o product-safety?

La Strategia annuncia che la Commissione presenterà nel corso del corrente anno una proposta di *Quantum Act*, destinata a istituire una “*Quantum Europe*

Research and Innovation Initiative” e a fungere da veicolo legislativo della Strategia stessa^[11]. Il Programma di lavoro della Commissione per il 2026 ne colloca la presentazione nel secondo trimestre del 2026 e ne individua la base giuridica indicativa negli articoli 173, 180 e 184 TFUE. Il 29 ottobre 2025 la Commissione ha aperto una “*Call for Evidence per l’impact assessment*” individuando tre criticità strutturali a cui l’Atto dovrebbe rispondere: frammentazione degli sforzi di ricerca tra Stati membri, insufficiente capacità industriale e vulnerabilità delle catene di approvvigionamento^[12].

Conviene tenere distinti due profili che la dottrina tende a sovrapporre. Quanto alla politica legislativa generale, le anticipazioni provenienti dal *Quantum Act* lasciano intendere che non assumerà l’impostazione “*product-safety oriented*” tipica dell’*AI Act*, ma si modellerà piuttosto sull’esperienza del *Chips Act*, privilegiando un approccio di “*industrial policy*” attuato attraverso uno schema di “*Joint Undertaking*”^[13]. Quanto agli strumenti tecnico-regolatori, invece, è ragionevole attendersi che l’Atto mutui dall’*AI Act* il modello standardizzazione/presunzione di conformità/sandbox: il “*New Legislative Framework*” europeo offre il “telaio” tecnico-giuridico più consolidato per disciplinare tecnologie emergenti senza ricorrere a regolazione di tipo prescrittivo. La tensione apparente tra i due modelli si risolve dunque su due piani diversi: macroscelta di policy industriale alla *Chips Act*, microarchitettura tecnico-regolatoria alla *AI Act*.

Nella dottrina questa impostazione ibrida è stata oggetto di una proposta organica articolata su un “*two-pillar framework*” che combina una regolazione di tipo “*New Legislative Framework*” (NLF) con una “*industrial and security policy*” sul modello del *Chips Act*, calibrata attraverso un “*risk-based tiering*” dei requisiti e l’impiego di “*regulatory sandboxes*” a presidio contro l’ipernormazione^[14]. La premessa metodologica si basa sull’assunto che la disciplina delle tecnologie quantistiche dovrebbe essere *sui generis*, in quanto i fenomeni quantistici fondamentali – sovrapposizione, “*entanglement*”, “*tunneling*” – sfidano le assunzioni classiche di certezza fattuale, causalità e località su cui si fondano i paradigmi giuridici esistenti^[15]. In senso parzialmente diverso la posizione che ha posto l’accento sulle lezioni critiche da trarre dall’esperienza dell’*AI Act*, in particolare sui rischi di sovraregolazione e sulla difficoltà di costruire una *governance* veramente adattiva^[16].

3.3. La cornice nazionale

Nel diritto nazionale, le tecnologie quantistiche rientrano già in alcune cornici giuridiche di rango primario. La disciplina dei poteri speciali del Governo a tutela degli assetti strategici, di cui al d.l. n. 21/2012 (c.d. Golden Power), si applica alle tecnologie critiche emergenti, categoria nella quale rientrano espressamente le tecnologie quantistiche secondo la Raccomandazione (UE) 2023/2113 della Commissione del 3 ottobre 2023 (C(2023) 6689 final)^[17]. Ciò comporta che operazioni di acquisizione di partecipazioni in società italiane attive nel settore quantistico da parte di soggetti extra-UE possano essere soggette agli obblighi di notifica e ai poteri di veto e prescrizione del Governo. Inoltre, talune categorie di prodotti, software, componenti e know-how quantistici possono rientrare, a seconda delle caratteristiche tecniche e della destinazione, nelle voci dell'Allegato I del Regolamento (UE) 2021/821, con il conseguente assoggettamento al regime autorizzatorio del “*dual-use*”. Infine, le reti quantistiche operative entreranno, al crescere del livello di maturità tecnologica, nel perimetro della direttiva NIS2 (Direttiva (UE) 2022/2555 del 14 dicembre 2022, recepita con d.lgs. n. 138/2024 del 4 settembre 2024) e, per i nodi qualificati come servizi essenziali, in quello del Perimetro di Sicurezza Nazionale Cibernetica (d.l. n. 105/2019, conv. nella l. n. 133/2019). A monte di queste cornici settoriali si colloca, sul piano del disegno di *policy* nazionale, la “*Strategia italiana per le tecnologie quantistiche*”^[18] che codifica una visione interministeriale italiana del settore e fornisce la base programmatica di raccordo con il futuro *Quantum Act* europeo^[19].

4. Il diritto delle tecnologie quantistiche nel quadro del diritto dell'innovazione

Collocare la riflessione sulle tecnologie quantistiche all'interno della più ampia disciplina del “*diritto amministrativo dell'innovazione tecnologica*”, oggetto di una sistemazione organica recentemente proposta da Antonio Bartolini^[20], consente di evitare l'isolamento metodologico e di mutuare strumenti concettuali già consolidati: l'innovazione come funzione amministrativa, i quattro modelli regolatori dell'innovazione, il bilanciamento tra principio di precauzione e principio di innovazione, la centralità della prudenza amministrativa (v. *infra*), il

rapporto tra Golden Power e tecnologie critiche.

4.1. L'innovazione come funzione amministrativa

Bartolini riconduce l'innovazione tecnologica a una vera e propria “*funzione amministrativa*”, apprezzabile sia in senso verticale (l'innovazione è interesse pubblico settoriale attribuito a specifici poteri amministrativi, anche attraverso la previsione – con un andamento carsico nei diversi governi – di un Ministro ad hoc) sia in senso orizzontale (l'innovazione è funzione implicita perseguibile da qualsiasi amministrazione attraverso strumenti come gli appalti precommerciali, i partenariati per l'innovazione, gli accordi per l'innovazione). Su questa base, le tecnologie quantistiche si collocano coerentemente come oggetto di una funzione di promozione e governo dell'innovazione che chiama in causa, nel caso italiano, AgID, ACN, INFN, il Ministero delle Imprese e del Made in Italy, il Ministero dell'Università e della Ricerca, nel quadro delle politiche europee di Horizon Europe e del programma EuroQCI. Le forme attuative – dagli appalti pre-commerciali alle convenzioni di trasferimento tecnologico per gli “*spin-off*” universitari operanti nel settore – trovano già nel diritto vigente strumenti di disciplina, anche se la loro applicazione specifica al quantum è ancora da costruire^[21].

Egli individua inoltre quattro modelli regolatori dell'innovazione: la regolamentazione per principi, la regolazione per esperimenti (“*regulatory sandbox*”), la regolazione condizionale e la regolazione etica^[22].

È un'articolazione che si applica con coerenza al diritto delle tecnologie quantistiche: la *Quantum Europe Strategy* si muove prevalentemente nella prima dimensione (principi, indirizzi, obiettivi); il *Quantum Act* in formazione si orienta verso uno strumento di *industrial policy* a base sperimentale, vicino al modello sandbox; la disciplina dei controlli all'export e del *Golden Power* costituisce un esempio paradigmatico di regolazione condizionale; le iniziative ELSI sulle tecnologie quantistiche sviluppano profili di regolazione etica.

4.2. Precauzione, innovazione e neutralità tecnologica

Per il diritto delle tecnologie quantistiche assume rilievo il principio di precauzione, nelle due accezioni – debole e forte – distinte dalla dottrina

amministrativistica^[23]. Le tecnologie quantistiche – in ambito di sicurezza informatica, sanità, finanza – sollevano il dilemma in forma peculiare: l'avvento del “*cryptographically relevant quantum computer*” comporta rischi non ancora attualizzati ma scientificamente fondati (l'algoritmo di Shor è dimostrato dal 1994), il che chiama in causa proprio quel calcolo del rischio che la dottrina del principio di precauzione ha elaborato a partire dal caso Sandoz.

Acquista poi rilievo l'emersione del “*principio di innovazione*”, ricostruibile in via interpretativa come corollario del principio di risultato di cui all'art. 1 del Nuovo Codice dei contratti pubblici (d.lgs. n. 36/2023), anche alla luce delle disposizioni di favore disseminate nel Codice (in particolare il partenariato per l'innovazione e i criteri premiali per le offerte a contenuto innovativo)^[24]. È un principio in via di consolidamento, che opera oggi come criterio di “*better regulation*” più che come principio generale, ma destinato ad assumere rilievo crescente nei settori – come il quantistico – in cui l'innovazione è interesse pubblico esplicito. La sua applicazione concreta al settore quantistico potrebbe per esempio orientare la formulazione di clausole di *favor* verso soluzioni a base quantistica negli appalti pubblici di servizi crittografici e di cybersicurezza.

Resta da considerare il principio di neutralità tecnologica, che nel campo delle tecnologie quantistiche assume connotati particolarmente delicati. Il principio – operante a livello settoriale nel diritto delle telecomunicazioni e nel diritto digitale dell'Unione – impone al regolatore di astenersi dall'individuare ex ante una soluzione tecnica vincolante. Le tecnologie quantistiche pongono però una tensione paradigmatica: la transizione “*quantum-safe*” richiede di scegliere tra QKD (basata sulla fisica) e PQC (basata sulla matematica), o di prevederne la combinazione. Un'imposizione normativa generalizzata di una sola delle due soluzioni potrebbe porsi in tensione con il principio di neutralità tecnologica, salvo che sia giustificata da esigenze prevalenti di sicurezza, interoperabilità o proporzionalità; un'astensione totale rischia però di produrre frammentazione applicativa e incertezza giuridica. È uno dei nodi che il *Quantum Act* dovrà sciogliere, presumibilmente attraverso un'architettura modulare costruita attorno a requisiti di sicurezza equivalente, che lasci agli operatori la scelta tecnica entro standard armonizzati di garanzia.

4.3. Golden Power e tecnologie critiche

Il riferimento normativo decisivo per il rapporto tra Golden Power e tecnologie quantistiche è l'art. 4, paragrafo 1, lettera b), del Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione, e che individua tra le tecnologie critiche, espressamente, anche la “*tecnologia quantistica*”^[25]. È la prima previsione di diritto positivo europeo che cristallizza la qualificazione delle tecnologie quantistiche come categoria autonoma di interesse strategico. Per il diritto delle tecnologie quantistiche questa qualificazione comporta conseguenze concrete su tre piani: le operazioni di acquisizione di partecipazioni in società italiane attive nel settore quantistico da parte di soggetti extra-UE possono essere soggette agli obblighi di notifica preventiva e ai poteri di veto e prescrizione del Governo; gli accordi di *joint venture*, di *licensing* e di trasferimento tecnologico verso soggetti stranieri rientrano nel perimetro applicativo dell'istituto; la stessa partecipazione di investitori esteri a programmi di ricerca strategici può attivare il meccanismo dei poteri speciali.

4.4. La regulatory sandbox come modello applicabile

Tra gli strumenti regolatori indicati per le tecnologie quantistiche figura la *regulatory sandbox*, che la dottrina ha analizzato con riferimento al «*diritto a innovare*» introdotto dall'art. 36 del d.l. n. 76/2020 e al sandbox dell'art. 57 dell'*AI Act* (Reg. UE 2024/1689)^[26]. È un modello particolarmente adatto al settore quantistico per due ragioni: il livello di maturità tecnologica (TRL) è variabile e in rapida evoluzione, sicché regole rigide rischiano di essere obsolete prima della loro entrata in vigore; la natura sperimentale dei protocolli quantistici richiede un'interlocuzione continua tra regolatore e regolato. L'introduzione di sandbox quantistiche dedicate, sul modello già operativo dell'*AI Act*, è una delle ipotesi più ragionevoli che il *Quantum Act* potrebbe accogliere.

Resta però un tratto peculiare del quantum rispetto ad altre tecnologie emergenti, che la cornice generale del diritto dell'innovazione non coglie appieno. Le tecnologie quantistiche non incidono soltanto su singole applicazioni amministrative o industriali, ma sulle condizioni infrastrutturali di affidabilità

dell'intero ecosistema digitale: la regolazione non riguarda solo l'uso di tecnologie nuove, ma la sostituzione progressiva delle basi crittografiche su cui si fonda la fiducia dell'ordinamento giuridico digitale. Donde l'esigenza di un approccio che, accanto agli strumenti tradizionali della regolazione dell'innovazione, sappia accompagnare una vera e propria “*transizione infrastrutturale*” – paragonabile, per portata sistemica, a quella della transizione ecologica.

Soccorre qui la lettura in chiave funzionale che la dottrina italiana ed europea ha sviluppato, secondo cui digitalizzazione e tecnologie emergenti vanno apprezzate nel loro carattere strumentale rispetto al “*diritto a una buona amministrazione*” di cui all'art. 41 della Carta dei diritti fondamentali dell'Unione europea^[27]. Il punto vale a fortiori per le tecnologie quantistiche: la transizione “*quantum-safe*” non è fine a sé stessa, ma trova ragione e misura nella capacità di preservare – e, dove possibile, accrescere – le garanzie procedurali, di affidabilità e di trasparenza che il diritto a una buona amministrazione esige.

5. La normativa esistente da riconsiderare

5.1. Quanto del modello AI Act è trasferibile al quantum?

La domanda preliminare alla disamina delle singole discipline riguarda il rapporto tra il diritto delle tecnologie quantistiche e quello dell'intelligenza artificiale, oggi compiutamente regolato dall'*AI Act* (Reg. UE 2024/1689). L'*AI Act* offre alcuni schemi tecnico-regolatori – il sistema di classificazione del rischio, la presunzione di conformità basata su standard armonizzati, l'architettura sandbox, gli obblighi di trasparenza algoritmica – che possono fungere da modello anche per il diritto delle tecnologie quantistiche.

La trasferibilità di tali schemi al settore quantistico va però valutata con cautela. Vi è anzitutto una differenza quanto alla natura del rischio. Per l'IA il rischio attiene principalmente ai diritti fondamentali (discriminazione algoritmica, opacità decisionale, “*chilling effects*”); per il “*quantum*” il rischio attiene piuttosto alla sicurezza dei sistemi (vulnerabilità crittografica, compromissione di infrastrutture critiche, “*harvest now*”, “*decrypt later*”). Diversa la natura del rischio, diverso il modello di regolazione. Vi è poi una differenza nel livello di maturità tecnologica: L'*AI Act* regola tecnologie ormai diffuse e

commercializzate; il *Quantum Act* dovrà invece accompagnare un processo di sviluppo ancora in larga parte sperimentale, in cui rigidità regolatorie premature potrebbero soffocare l'innovazione. E vi è infine una divergenza nel rapporto con la sovranità tecnologica: Per l'AI il problema regolatorio principale è il bilanciamento tra innovazione e tutela dei diritti; per il quantum, dove l'Unione sconta un ritardo industriale rispetto a Stati Uniti e Cina, il problema principale è la costruzione di una capacità produttiva autonoma. Donde la più marcata vocazione di *industrial policy* del *Quantum Act* rispetto al modello *product-safety* dell'*AI Act*.

Posta questa premessa, e mantenuti i necessari distinguo, alcuni strumenti dell'*AI Act* – in particolare la presunzione di conformità basata su standard armonizzati e l'architettura sandbox – restano i candidati naturali per la disciplina delle tecnologie quantistiche, come si vedrà nei paragrafi che seguono.

5.2. Protezione dei dati personali: l'art. 32 GDPR e la riqualificazione dello “stato dell'arte”

L'art. 32 del Regolamento (UE) 2016/679 (GDPR) impone al titolare e al responsabile del trattamento di adottare «*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*», tenendo conto, tra l'altro, dello «*stato dell'arte*». La norma è strutturalmente aperta: il suo contenuto concreto dipende dall'evoluzione tecnologica.

L'avvento del calcolo quantistico modifica i parametri di applicazione di questa clausola generale. La prospettiva più seria di compromissione della sicurezza dei dati è rappresentata dall'attacco noto come “*harvest now*”, “*decrypt later*”: un soggetto malintenzionato raccoglie oggi i dati cifrati con algoritmi a chiave pubblica (in particolare RSA ed ECC), li conserva, e li decifra in un momento futuro quando i computer quantistici raggiungeranno la scala necessaria a eseguire l'algoritmo di Shor^[28]. Per i dati a lunga conservazione – sanitari, finanziari, biometrici, dati relativi a posizioni giuridiche soggettive durature – la cifratura odierna potrebbe risultare progressivamente inadeguata.

Sul versante della Post-Quantum Cryptography (PQC) gli standard tecnici di riferimento sono essenzialmente statunitensi: il National Institute of Standards and Technology (NIST) ha pubblicato nell'agosto 2024 i primi tre standard post-

quantum (FIPS 203, 204 e 205), Successivamente, nel marzo 2025, il NIST ha selezionato un ulteriore algoritmo, HQC, destinato a rafforzare la diversificazione delle soluzioni crittografiche, ma la relativa standardizzazione non risulta ancora conclusa. L'Unione europea pare non disporre allo stato di standard equivalenti; la "*Quantum Europe Strategy*" ne prevede uno, attraverso una "*Quantum Standards Roadmap*", per il 2026. Sul versante della "*Quantum Key Distribution*" (QKD) esiste invece un "*Protection Profile*" europeo (ETSI GS QKD 016) certificabile secondo lo schema "*Common Criteria*" del Cybersecurity Act^[29].

In termini ricostruttivi, è ragionevole sostenere che per i trattamenti aventi ad oggetto dati ad alta sensibilità e lunga durata di rilevanza l'art. 32 GDPR possa già fondare un obbligo almeno "*procedurale*" di valutazione della "*quantum-readiness*", anche se non ancora un obbligo generalizzato di migrazione immediata verso soluzioni "*quantum-safe*". La diligenza tecnica richiesta dal regolamento, letta congiuntamente al principio di *accountability* (art. 5, par. 2 GDPR), impone di valutare prospetticamente i rischi e di pianificare misure adeguate anche con riferimento a minacce non ancora attualizzate ma scientificamente fondate. La portata concreta dell'obbligo va però modulata in funzione di più variabili: natura dei dati, durata di rilevanza, settore del titolare, proporzionalità delle misure, disponibilità di soluzioni tecniche mature, costi di transizione. Una pronuncia di soft law del Comitato europeo per la protezione dei dati – oggi assente – sarebbe auspicabile per definire i criteri applicativi.

5.3. Identità digitale e prova documentale: eIDAS 2 e la firma qualificata

Il Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024, che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (eIDAS 2) conferma e potenzia la disciplina della firma elettronica qualificata, alla quale è riconosciuto effetto equivalente alla firma autografa ex art. 25. Il valore probatorio della firma qualificata si fonda su algoritmi crittografici asimmetrici (RSA, ECDSA, EdDSA) la cui sicurezza dipende dall'intrattabilità computazionale, per i computer classici, dei problemi di fattorizzazione e di

logaritmo discreto.

L'algoritmo di Shor risolverebbe entrambi i problemi in tempo polinomiale su un computer quantistico di scala sufficiente^[30]. Quando ciò avverrà – l'orizzonte stimato dalla letteratura specialistica si colloca tra dieci e venti anni – l'affidabilità crittografica delle firme qualificate apposte con algoritmi tradizionali potrebbe risultare compromessa.

Le conseguenze giuridiche sono notevoli. La presunzione legale di autenticità ex art. 25 eIDAS, oggi pacificamente applicabile, si troverà esposta a contestazione strutturale: l'avvento del "*cryptographically relevant quantum computer*" renderà in linea teorica possibile produrre firme apparentemente valide senza il consenso del titolare. Il valore probatorio del documento informatico sottoscritto con firma qualificata, di cui all'art. 20 del Codice dell'amministrazione digitale (d.lgs. n. 82/2005), risulterà esposto a fragilità retroattive per i documenti firmati ante-PQC. L'intero impianto dell'archiviazione a norma – disciplinata dal d.P.C.M. del 3 dicembre 2013 e dalle Linee Guida AgID – dovrà ripensare le proprie garanzie di integrità nel lungo periodo.

Le soluzioni si muovono su tre direttrici. La prima è la transizione progressiva ad algoritmi PQC standardizzati, da iniziarsi senza attendere l'avvento del computer quantistico criptanaliticamente rilevante. La seconda è l'introduzione di meccanismi di "*long-term archival*" che prevedano la ri-firma periodica dei documenti con algoritmi aggiornati, sul modello degli *archival timestamping* già previsti dallo standard ETSI EN 319 122^[31]. La terza, più ambiziosa, è l'utilizzo della QKD per la generazione e la distribuzione delle chiavi alla base della firma qualificata, lungo canali fisicamente sicuri. Spetterà alla Commissione, attraverso gli atti di esecuzione previsti dal regolamento, e all'ENISA, nella sua funzione di supporto tecnico, definire un quadro applicativo coordinato.

5.4. Controlli all'export e dual-use: il Regolamento (UE) 2021/821

Il Regolamento (UE) 2021/821 del 20 maggio 2021 istituisce il regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso. Le tecnologie quantistiche possono rientrare, a seconda delle caratteristiche tecniche e della

destinazione, in più voci dell'Allegato I, che ricomprende computer quantistici, algoritmi quantistici, sorgenti e detector di fotoni singoli, moduli di QKD, memorie quantistiche, sistemi di “*entanglement distribution*” e relativi software. Non tutte le tecnologie quantistiche sono però automaticamente beni “*dual-use*” controllati: una valutazione caso per caso, alla luce delle voci dell'Allegato I e delle clausole catch-all dell'art. 4, resta necessaria.

Due profili meritano attenzione dal punto di vista della ricerca scientifica universitaria. Primo: il regime delle “*deemed exports*”. La nozione di esportazione non si limita al trasferimento fisico di beni attraverso le frontiere. L'art. 2, n. 2, lett. b), del Regolamento qualifica come esportazione anche la «*trasmissione di software o tecnologia tramite mezzi elettronici*» verso una destinazione al di fuori del territorio doganale dell'Unione, mentre l'art. 8 disciplina i controlli sull'assistenza tecnica anche all'interno dell'Unione. La prassi applicativa statunitense – sotto la formula “*deemed export*” – estende il concetto al trasferimento di tecnologia controllata a soggetti extra-UE anche all'interno del territorio nazionale. In ambito UE, l'applicazione di tale concetto richiede maggiore cautela e va modulata sulla concreta formulazione del Regolamento, che non riproduce in modo identico l'architettura statunitense; resta tuttavia ragionevole ritenere che il ricercatore non-UE che accede al laboratorio dove si trova un'apparecchiatura quantistica controllata, oppure che riceve via email il codice sorgente di un protocollo quantistico, possa configurare un trasferimento soggetto ad autorizzazione.

Secondo: il confine con la “*basic scientific research exemption*” e con la “*information in the public domain*”. L'Allegato I del Regolamento esclude dai controlli la ricerca scientifica fondamentale, definita come l'attività sperimentale o teorica intrapresa principalmente per acquisire nuove conoscenze sui fenomeni fondamentali, non finalizzata in modo specifico a un obiettivo o uno scopo pratico; l'esenzione si estende anche alle conoscenze rese accessibili senza restrizioni. Nel settore quantistico l'identificazione del confine è particolarmente delicata: la pubblicazione su rivista “*peer-reviewed*” è generalmente sufficiente a far ricadere il contenuto nel pubblico dominio, ma la pre-pubblicazione, la condivisione su *preprint server*, la trasmissione di dataset associati restano ambiti grigi. Il bilanciamento con la libertà di ricerca scientifica garantita dall'art. 33 della Costituzione italiana e dall'art. 13 della Carta dei diritti fondamentali

dell'Unione europea è demandato in concreto alla prassi delle autorità competenti.

5.5. Cybersicurezza delle infrastrutture critiche: NIS2 e PSNC

La direttiva NIS2 (Direttiva (UE) 2022/2555), recepita in Italia con d.lgs. n. 138/2024, ha esteso il perimetro applicativo della disciplina della sicurezza delle reti e dei sistemi informativi articolando i soggetti nelle categorie di «*essenziali*» e «*importanti*». Le reti quantistiche operative – al raggiungimento del “*technology readiness level 7-9*” e della loro integrazione in infrastrutture come EuroQCI – ricadranno verosimilmente nella categoria delle infrastrutture digitali. Parallelamente, l'inclusione di nodi di rete quantistica nel Perimetro di Sicurezza Nazionale Cibernetica (d.l. n. 105/2019 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (e di disciplina dei poteri speciali nei settori di rilevanza strategica) è prevedibile per le funzioni essenziali dello Stato e per i servizi essenziali, con l'attivazione del relativo regime di golden power cibernetico, di notifica degli affidamenti di forniture ICT e di valutazioni del CVCN.

Le categorie e gli obblighi di NIS2 sono però stati elaborati con riferimento a infrastrutture classiche e non considerano la specificità degli incidenti quantistici: la perdita di coerenza degli stati, gli attacchi “*side-channel*” sulle memorie atomiche o sui detector di fotoni singoli, le vulnerabilità delle interfacce ottiche, la “*photon-number splitting attack*”, gli attacchi “*Trojan-horse*” sui sistemi QKD. La “*supply-chain security*” delle componenti quantistiche è un ambito nuovo, in cui mancano standard consolidati e in cui la dipendenza tecnologica dell'Unione da fornitori esterni è accentuata. Il *Quantum Act* sarà chiamato a coordinarsi con NIS2 attraverso meccanismi di specificazione tecnica, plausibilmente attivati tramite atti di esecuzione della Commissione e linee guida ENISA.

5.6. Responsabilità da prodotto: la Direttiva (UE) 2024/2853

La Direttiva (UE) 2024/2853 del 23 ottobre 2024, che sostituisce la Direttiva

85/374/CEE in materia di responsabilità per danno da prodotti difettosi, ha incluso espressamente il software nella nozione di prodotto (art. 4, n. 1), così attraendo nel proprio ambito anche i sistemi di intelligenza artificiale, e ha introdotto presunzioni di difetto e di nesso causale a favore del danneggiato quando la complessità tecnica o scientifica del caso renda eccessivamente difficile la prova (art. 10, par. 4). È forse il terreno su cui la specificità delle tecnologie quantistiche emerge in forma più acuta^[32].

La natura intrinsecamente probabilistica del calcolo quantistico – l’output corretto si ottiene con una probabilità statistica e non con certezza deterministica – rende difficile l’applicazione del concetto tradizionale di “difetto”, che presuppone uno scarto rispetto a un risultato atteso univocamente determinato.

I protocolli di “*quantum error correction*”, i meccanismi di “*entanglement distribution*” e i sistemi QKD operano per natura con tassi di errore non nulli: lo stesso teorema di soglia, o “*threshold theorem*”, che fonda la correzione di errore quantistica afferma che un calcolo arbitrariamente lungo è possibile soltanto se la probabilità di errore per operazione resta sotto una certa soglia, non se essa è zero. La qualificazione di un risultato come “difettoso” richiede dunque di stabilire la soglia oltre la quale lo scarto dalla performance attesa diventa giuridicamente rilevante.

Una seconda specificità attiene al “*no-cloning theorem*”: lo stato quantistico non può essere copiato senza essere distrutto. Ne deriva l’impossibilità di replicare ex post le condizioni del danno per accertarne le cause, con effetti significativi sull’onere della prova e sul regime delle presunzioni introdotto dalla Direttiva 2024/2853. Una terza specificità attiene alla nozione di “*aggiornamento*” del prodotto: nei sistemi quantistici, la calibrazione è continua e influisce direttamente sulle prestazioni, sicché la distinzione tra «*difetto originario*» e «*difetto sopravvenuto*» è strutturalmente sfumata. Una quarta specificità attiene alla ripartizione del rischio nella filiera: l’architettura di una rete quantistica vede tipicamente concorrere produttori di hardware (sorgenti, detector, memorie), sviluppatori di software e di protocolli, integratori di sistema, operatori della rete, utilizzatori finali. L’individuazione del soggetto responsabile per un danno derivante da una distribuzione di chiave fallita o da una correzione di errore non riuscita richiede un’articolazione fine che il diritto vigente – pensato per prodotti monolitici e deterministici – non offre.

Le linee di soluzione si muovono lungo tre direttrici. La prima è la costruzione di standard tecnici di sicurezza minima che fungano da soglia di accettabilità del rischio probabilistico, in modo da rendere applicabile il concetto di difetto come scarto dallo standard piuttosto che come errore in senso assoluto. La seconda è l'introduzione di obblighi di documentazione tecnica rafforzati (*"logging"* continuo, certificazione delle calibrazioni) che consentano di ricostruire ex post l'operatività del sistema anche in presenza del *"no-cloning"*. La terza è l'eventuale previsione di meccanismi di *"risk pooling"* o di assicurazione obbligatoria per i danni di sistema, sul modello di quanto avvenuto in altri settori ad alta complessità tecnologica. La direttiva del 2024 lascia agli Stati membri ampi margini di adattamento, ma una riflessione dottrinale italiana sul punto non sembra ancora consolidata.

Una precisazione è utile per non generare aspettative incongruenti rispetto all'orientamento di *industrial policy* del futuro *Quantum Act*. La centralità dei profili di responsabilità non implica necessariamente l'introduzione di un regime speciale all'interno del *Quantum Act* stesso: suggerisce piuttosto la previsione di standard tecnici e obblighi documentali destinati a incidere indirettamente sull'applicazione della Direttiva 2024/2853, attraverso il meccanismo della presunzione di conformità. Il regime di responsabilità da prodotto resta cioè disciplina autonoma; il *Quantum Act* ne può facilitare l'applicazione tecnica, senza pretendere di riscriverla.

6. Gli ambiti regolatori ancora privi di sistemazione organica

6.1. Verso un sistema integrato di certificazione delle tecnologie quantistiche

Il modello di riferimento, anche se non esclusivo, è quello costruito per l'intelligenza artificiale. Esso combina un atto legislativo che fissa obblighi differenziati in base al livello di rischio (*AI Act*) con una presunzione di conformità per i sistemi che rispettino gli standard armonizzati sviluppati dal CEN/CENELEC JTC 21, oltre allo standard di sistema di gestione ISO/IEC 42001:2023 dedicato alla materia.

Per le tecnologie quantistiche un sistema analogo è oggi solo frammentariamente abbozzato. A livello internazionale, ISO e IEC hanno costituito un Joint Technical Committee 3 dedicato alle “*Quantum Technologies*”, che ha avviato i propri lavori nella primavera 2024; ISO/IEC JTC 1/SC 27 ha sviluppato lo standard ISO/IEC 23837 sui requisiti di sicurezza e i metodi di valutazione per i prodotti di “*Quantum Key Distribution*”; è stato inoltre pubblicato ISO/IEC 4879:2024 sul vocabolario del “*quantum computing*”.

A livello europeo, il CEN/CENELEC ha istituito il Joint Technical Committee 22 sulle “*Quantum Technologies*”, articolato in quattro working group, il cui primo deliverable – il Technical Report CEN/CLC/TR 18202:2025 “*Layer model of Quantum Computing*” – è stato pubblicato il 3 settembre 2025^[33]. A livello settoriale, ETSI ha sviluppato attraverso il proprio ISG-QKD, attivo dal 2008, la “*Group Specification*” ETSI GS QKD 016, primo “*Protection Profile*” al mondo per la valutazione di sicurezza dei moduli QKD secondo lo schema Common Criteria (ISO/IEC 15408)^[34].

Manca, tuttavia, un quadro integrato. Manca soprattutto il rinvio normativo cogente, ovvero il meccanismo per cui un atto legislativo dell’Unione attribuisce agli standard tecnici la funzione di presunzione di conformità rispetto a obblighi giuridici. La proposta della dottrina individua proprio nello “*standards-first approach*” l’elemento qualificante del *Quantum Act*^[35]. Un sistema di certificazione coerente potrebbe articolarsi su livelli distinti: una certificazione di prodotto, per i singoli moduli hardware, già parzialmente coperta dal Protection Profile ETSI GS QKD 016 / “*Common Criteria*”; una certificazione di processo, per i protocolli generativi, gli schemi di “*error correction*” e i meccanismi di “*entanglement distribution*”, oggi sostanzialmente scoperta; una certificazione di sistema di gestione, sul modello della ISO/IEC 42001, per le organizzazioni che operano reti quantistiche integrate.

6.2. Il quadro giuridico della transizione quantum-safe: QKD e PQC

La transizione verso un ecosistema “*quantum-safe*” procede su due binari paralleli, talora presentati come alternativi ma più correttamente da intendersi come complementari. Il primo binario è quello della Quantum Key Distribution

(QKD): la sicurezza della distribuzione della chiave non poggia sulla difficoltà computazionale di un problema matematico, ma sulle proprietà fondamentali della meccanica quantistica (in particolare sul teorema di “*no-cloning*” e sull’inevitabile perturbazione dello stato quantistico causata dalla misurazione).

Ne deriva la possibilità, in linea di principio, di canali “*information-theoretically secure*”. Il secondo binario è quello della Post-Quantum Cryptography (PQC): algoritmi crittografici a chiave pubblica costruiti su problemi matematici per i quali non si conoscono algoritmi quantistici di risoluzione efficienti. Gli standard NIST FIPS 203-205 del 2024 costituiscono il riferimento internazionale.

Una precisazione è qui necessaria. La QKD offre garanzie “*teoriche*” di sicurezza fondate sulla fisica, ma le implementazioni concrete restano esposte a vulnerabilità hardware, “*side-channel*” e supply-chain (“*photon-number splitting*”, attacchi sui detector, attacchi “*Trojan-horse*”). La sicurezza “*information-theoretic*” del protocollo non si traduce automaticamente in sicurezza operativa del sistema: è la differenza tra modello matematico e prodotto industriale. Questo profilo, oltre a giustificare l’esistenza di standard di certificazione come ETSI GS QKD 016, mostra perché la transizione “*quantum-safe*” non possa essere monistica.

Le due tecnologie operano a livelli diversi. La PQC è un sostituto diretto degli attuali algoritmi a chiave pubblica e può essere implementata via software su infrastrutture esistenti; la QKD richiede infrastrutture fisiche dedicate (fibre ottiche, satelliti) ma offre garanzie di natura fisica.

La comunità scientifica e regolatoria si sta orientando verso un approccio combinato: PQC come misura di base universale, QKD come livello aggiuntivo per contesti ad alta criticità. Sul piano giuridico, mancano oggi norme che disciplinino esplicitamente la coesistenza, la complementarità o l’eventuale cumulo delle due tecnologie ai fini della conformità agli obblighi di sicurezza.

L’art. 32 GDPR, l’art. 21 della Direttiva NIS2, le norme del Cybersecurity Act (Reg. UE 2019/881), le norme prudenziali del Digital Operational Resilience Act (Reg. UE 2022/2554, DORA) per il settore finanziario: tutti rinviando genericamente allo «*stato dell’arte*» o a «*misure adeguate al rischio*», senza definire un quadro coordinato. Un primo tassello di coordinamento è stato posto dalla Raccomandazione (UE) 2024/1101 della Commissione, dell’11 aprile 2024, sulla “*Coordinated Implementation Roadmap for the transition to Post-Quantum*

Cryptography”, cui ha fatto seguito il documento del NIS Cooperation Group del 23 giugno 2025 che ne articola le milestone (transizione iniziale per i casi a rischio elevato entro il 2030; transizione integrale entro il 2035)^[36]. Si tratta però di soft law: un quadro giuridicamente cogente e tecnicamente coordinato resta da costruire, ed è in questo spazio che il *Quantum Act* è chiamato a intervenire.

6.3. Il regime brevettuale dei “quantum-implemented inventions”

I protocolli quantistici si collocano in una zona di confine particolarmente delicata per il diritto brevettuale. L’art. 52, par. 2, della Convenzione sul Brevetto Europeo esclude dal novero delle invenzioni brevettabili, fra l’altro, le scoperte, le teorie scientifiche e i metodi matematici; l’art. 52, par. 3, precisa che tale esclusione opera «*solo se la domanda di brevetto europeo o il brevetto europeo concernono uno solo di questi elementi, considerato in quanto tale*». La giurisprudenza dell’EPO ha sviluppato, con riferimento ai “*computer-implemented inventions*”, una distinzione tra il metodo matematico in sé (non brevettabile) e l’applicazione tecnica del metodo che produca un effetto tecnico ulteriore (brevettabile)^[37]. Per le “*quantum-implemented inventions*” non sembra ancora consolidata una prassi specifica. Tre questioni restano aperte: l’individuazione dell’effetto tecnico ulteriore; il requisito di “*enablement*” per protocolli ancora a basso TRL; il rischio di “*anticommons*”.

Il regime brevettuale dei protocolli quantistici si lega direttamente al tema della sovranità tecnologica europea e dell’*industrial policy* del *Quantum Act*. La frammentazione brevettuale, dominata oggi da soggetti statunitensi e cinesi, rischia di tradursi in un ostacolo strutturale all’autonomia tecnologica europea. Su questo terreno parte della dottrina propone modelli alternativi di gestione della proprietà intellettuale: “*patent pools, cross-licensing agreements*”, iniziative “*open-source*” coordinate, “*defensive publications*”^[38]. Sul versante dei finanziamenti pubblici, Horizon Europe impone già una “*exploitation obligation*” che bilancia la titolarità della ricerca con l’accesso ai risultati. Il *Quantum Act* potrebbe valorizzare ulteriormente strumenti specifici di gestione dell’IP per le tecnologie strategiche, sul modello delle “*standard essential patents*” nel settore delle telecomunicazioni, in modo da prevenire la formazione di

posizioni dominanti incompatibili con gli obiettivi di autonomia industriale e di capacità produttiva europea.

7. Verso un Quantum Act europeo: una proposta di architettura

L'annunciato *Quantum Act* troverà la propria cornice nella “*Quantum Europe Strategy*” della Commissione europea (COM(2025) 363 final del 2 luglio 2025), che si articola lungo cinque assi: ricerca e innovazione, infrastrutture quantistiche, rafforzamento dell'ecosistema industriale, tecnologie spaziali e “*dual-use*”, competenze e talenti. La Strategia individua nel *Quantum Act* il veicolo legislativo destinato a istituire formalmente la “*Quantum Europe Research and Innovation Initiative*” e a fornire la base giuridica del coordinamento dei programmi europei e nazionali. La presente sezione prova ad articolare, sulla base delle tensioni regolatorie analizzate nei paragrafi precedenti, una proposta di architettura interna del futuro *Quantum Act*, senza pretesa di formularne una bozza normativa^[39].

Una prima esigenza riguarda la definizione del campo di applicazione e l'enunciazione dei principi. Il *Quantum Act* dovrebbe anzitutto delimitare la nozione di tecnologie quantistiche rilevanti – coprendo, secondo l'articolazione ormai consolidata, “*computing*”, comunicazione, “*sensing e networking*” – e codificare i principi generali che ne guidano la regolazione: sovranità tecnologica, neutralità tecnologica fra QKD e PQC, principio di innovazione, principio di precauzione modulato sul rischio, principio di proporzionalità regolatoria. L'esplicitazione di tali principi assolverebbe a una funzione che, nel diritto amministrativo dell'innovazione tecnologica, è ormai riconosciuta come decisiva: indirizzare l'interprete in un settore in cui la tecnologia evolve più rapidamente della norma^[40].

Una seconda dimensione concerne l'iniziativa europea di ricerca e industria. La “*Quantum Europe Strategy*” adottata dalla Commissione europea (COM(2025) 363 final) – che individua nel preannunciato *Quantum Act* il proprio veicolo legislativo – ha previsto l'istituzione della “*Quantum Europe Research and Innovation Initiative*” attraverso lo stesso atto, presumibilmente nelle forme dell'impresa comune (“*Joint Undertaking*”, JO^[41]) sul modello già sperimentato

per EuroHPC JU (*“The European High Performance Computing Joint Undertaking”*), di cui la stessa Strategia prevede una modifica del regolamento istitutivo per estenderne il mandato al coordinamento di tutte le attività europee di ricerca e innovazione quantistica. Il coordinamento dovrebbe estendersi alle altre iniziative europee a vocazione quantistica –EuroQCI (*“Quantum communication infrastructure”*), EuroHPC nella sua dimensione quantistica, IRIS² per la connettività satellitare, *Chips Act* per la componentistica – e includere strumenti di sostegno alla *supply chain* e ai produttori europei, in coerenza con l’obiettivo di sovranità tecnologica espresso nella Strategia^[42].

Strettamente connesso è il tema della standardizzazione e della certificazione. La Strategia rinvia a una *“Quantum Standards Roadmap”* prevista per il 2026, e prefigura l’attivazione formale del comitato tecnico congiunto CEN/CENELEC JTC 22, in parallelo a quanto già avvenuto per JTC 21 in materia di intelligenza artificiale^[43]. Il *Quantum Act* potrebbe in questo quadro introdurre una presunzione di conformità ancorata a standard armonizzati costruiti attorno alla nozione di *“sicurezza equivalente”* – e non, dunque, alla scelta di una tecnologia unica, in coerenza con il principio di neutralità tecnologica. La certificazione, peraltro, dovrebbe articolarsi su tre livelli – prodotto, processo, sistema di gestione – e raccordarsi con il Cybersecurity Act (Regolamento (UE) 2019/881) e con gli schemi ENISA, evitando la sovrapposizione di regimi paralleli^[44].

La sicurezza è il versante che esige maggiore attenzione. Il Gruppo NIS Cooperation ha indicato la fine del 2026 quale orizzonte per l’avvio della transizione *“quantum-safe”* nelle infrastrutture critiche, con completamento previsto per il 2030. Il *Quantum Act* è la sede naturale per definire il quadro giuridico della coesistenza fra PQC e QKD, anziché lasciarne il governo alla sola pratica regolatoria settoriale. Qui possono trovare spazio obblighi di *“quantum-readiness assessment”* per i titolari di dati ad alta sensibilità e lunga durata di rilevanza, meccanismi di transizione graduale e disposizioni in materia di *“long-term archival”*.

Il raccordo con NIS2 (Direttiva (UE) 2022/2555 sulla sicurezza delle reti e dei sistemi informativi), DORA (Regolamento (UE) 2022/2554 sulla resilienza operativa digitale del settore finanziario), eIDAS 2 (Regolamento (UE) 2024/1183 sull’identità digitale europea) e GDPR (Regolamento (UE) 2016/679 sulla protezione dei dati personali) sarebbe in tal caso non meramente esortativo,

ma articolato in obblighi tecnici e documentali tracciabili^[45].

Sul terreno della regolazione sperimentale, l'alto tasso di incertezza tecnologica del settore rende particolarmente promettente l'estensione del modello dei sandbox già operativo nell'art. 57 dell'*AI Act*. Sandbox quantistiche nazionali consentirebbero lo sviluppo, l'addestramento, la sperimentazione e la validazione di protocolli innovativi sotto la supervisione delle autorità competenti, in un quadro temporalmente delimitato attraverso *sunset clauses* e meccanismi di valutazione periodica. È una soluzione che la Strategia europea non esclude espressamente, ma che il *Quantum Act* è chiamato a tradurre in disciplina effettiva, evitando la frammentazione applicativa tra Stati membri^[46].

Un'ultima esigenza riguarda la governance e il coordinamento. La Strategia ha già delineato un assetto di governance a due livelli^[47]: un "*high-level advisory board*" di esperti scientifici e tecnologici e un quadro strutturato di cooperazione con gli Stati membri. Il *Quantum Act* potrebbe consolidare tale assetto attraverso l'istituzione di un organismo di coordinamento europeo – qualificabile, ad esempio, come "*European Quantum Board*" – articolato su rappresentanze nazionali e contributi scientifici. Il coordinamento dovrebbe estendersi ai regimi di "*foreign investment screening*" (Reg. UE 2019/452), al regime "*dual-use*" (Reg. UE 2021/821) e al Golden Power nazionale, oltre che ai profili ELSI e di responsabilità. In prospettiva, non è precluso un raccordo con iniziative di governance internazionale, fino all'ipotesi, prospettata da parte della dottrina, di una "*International Quantum Agency*" sul modello dell'IAEA^[48].

L'architettura così abbozzata non pretende di sostituire le discipline settoriali esistenti, ma di organizzarne il raccordo. Il valore aggiunto del *Quantum Act* non consisterebbe nella produzione di un nuovo micro-codice del quantum, bensì nella costruzione di una infrastruttura comune tra sicurezza, standardizzazione e innovazione industriale.

8. Conclusioni

Le riflessioni che precedono consentono di formulare quattro proposizioni conclusive, disposte su piani analitici distinti ma reciprocamente integrati: il piano metodologico-ricostruttivo, quello della tecnica legislativa europea, quello dei rapporti tra livelli ordinamentali, quello dei rapporti tra diritto (pubblico) e

innovazione tecnologica.

Il diritto delle tecnologie quantistiche, in primo luogo, non si configura come campo originario, ma come effetto adattivo di una pluralità di discipline preesistenti messe in tensione dalla natura strutturalmente diversa dei fenomeni quantistici. Lo “stato dell’arte” dell’art. 32 GDPR – clausola aperta calibrata sulla crittografia classica – diventa parametro tecnico per la “*quantum-readiness*”; la presunzione di autenticità di cui all’art. 25 eIDAS 2 entra in tensione con la vulnerabilità delle firme asimmetriche all’algoritmo di Shor; la nozione di «difetto» della Direttiva 2024/2853 si confronta con la natura strutturalmente probabilistica del calcolo quantistico e con il “*no-cloning theorem*”; il concetto di “incidente significativo” della NIS2 deve integrare le specificità degli attacchi “*side-channel*” sui sistemi QKD; la qualificazione brevettuale ex art. 52 CBE è sfidata dalla logica delle “*quantum-implemented inventions*”. La funzione primaria del giurista, di fronte a questo quadro, non è invocare un diritto speciale “*ex novo*”, ma identificare i punti di rottura interpretativa delle discipline vigenti e proporre soluzioni adattive coerenti con il principio di proporzionalità regolatoria.

Quanto alla tecnica legislativa europea, il *Quantum Act* non dovrebbe duplicare né l’*AI Act* né il *Chips Act*, ma combinarne i modelli secondo una geometria a piani sovrapposti, in parte già attivata dall’evoluzione legislativa: macroscelta di “*industrial policy*” mutuata dal *Chips Act*, microarchitettura tecnico-regolatoria mutuata dal sistema standardizzazione/presunzione di conformità/sandbox dell’*AI Act*. La dimensione di “*industrial policy*” è già in larga parte attivata attraverso il Regolamento (UE) 2026/150, che ha esteso il mandato dell’impresa comune EuroHPC alle tecnologie quantistiche istituendo un *Quantum Pillar*; il *Quantum Act*, atteso per il secondo trimestre del corrente anno secondo il Programma di lavoro della Commissione (basi giuridiche indicate negli artt. 173, 180 e 184 TFUE), è chiamato ad innestare su tale telaio industriale la dimensione tecnico-regolatoria del “*New Legislative Framework*”. La cifra distintiva dell’Atto sarà perciò non innovativa rispetto ai modelli regolatori europei consolidati, ma combinatoria: l’originalità giuridica risiederà nella selezione e nell’integrazione di strumenti già esistenti.

Il diritto delle tecnologie quantistiche, nei rapporti tra livelli ordinamentali, si articola fisiologicamente come ordinamento multilivello: il livello internazionale

(Risoluzione ONU 78/287 del 2024 e prospettiva di una “*International Quantum Agency*” sul modello IAEA prospettata in dottrina), il livello unionale (Quantum Europe Strategy, Reg. (UE) 2026/150 sull’estensione di EuroHPC, futuro *Quantum Act*, normativa settoriale di adattamento) e il livello nazionale (Strategia italiana per le tecnologie quantistiche approvata dal CITD il 10 luglio 2025; quadro PNRR di sostegno alla ricerca quantistica; regimi del Golden Power, NIS2 e Perimetro di Sicurezza Nazionale Cibernetica). Il rapporto tra i livelli non è meramente verticale: la pubblicazione anticipata della Strategia italiana – antecedente di pochi mesi al *Quantum Act* – mostra che il livello nazionale può fornire elementi di disegno regolatorio assorbibili dal livello unionale, in una circolarità che valorizza il principio di sussidiarietà. Per l’Italia, la sfida è far valere il modello di coordinamento interministeriale formalizzato dalla Strategia (MUR, MIMIT, Difesa, MAECI, ACN, Dipartimento per la Trasformazione Digitale) come architettura proponibile al livello europeo.

Nei rapporti fra diritto pubblico e innovazione, infine, la dottrina – segnatamente la sistemazione del diritto amministrativo dell’innovazione tecnologica proposta da Bartolini – offre al dibattito europeo un telaio concettuale particolarmente fertile: l’innovazione come funzione amministrativa (verticale e orizzontale), i quattro modelli regolatori (per principi, per esperimenti, condizionale, etica), il bilanciamento dinamico tra principio di precauzione e principio di innovazione, la neutralità tecnologica come limite alla discrezionalità regolatoria, il Golden Power come strumento di difesa degli asset strategici. Tali categorie consentono di leggere il *Quantum Act* non come fenomeno di rottura, ma come momento di consolidamento di un modello di governance amministrativa dell’innovazione il cui nucleo dottrinale è già disponibile nel diritto vigente. Il legislatore europeo dovrebbe muoversi non nella direzione di un’applicazione massimalista del principio di precauzione – che si tradurrebbe in iperregolazione – ma in quella della prudenza amministrativa nel senso proposto da Bartolini: una misura del decisore che calibri l’intervento sul concreto livello di maturità tecnologica e sul rischio sistemico effettivo^[49].

Le quattro proposizioni convergono verso una considerazione di taglio prospettico. La presentazione della proposta di *Quantum Act* aprirà una finestra di negoziazione interistituzionale in cui la dottrina europea – e specificamente quella italiana – è chiamata a fornire il proprio contributo, non come voce

reattiva ma come interlocutore strutturato.

Il compito della riflessione giuridica nei prossimi mesi è duplice: per un verso, presidiare il momento ricostruttivo, distinguendo ciò che il diritto vigente può già fare attraverso l'interpretazione adattiva da ciò che richiede un intervento del legislatore; per l'altro, presidiare il momento propositivo, indicando nella combinazione tra macroarchitettura *Chips Act* (*industrial policy*) e microarchitettura *AI Act* (NLF) la geometria istituzionale verso cui il *Quantum Act* è coerentemente orientato.

Pur condotto dalla prospettiva del diritto amministrativo, e dunque con i limiti propri di chi non appartiene alla comunità delle scienze fisiche e ingegneristiche da cui il lessico tecnico delle tecnologie quantistiche proviene, il presente lavoro intende offrire un contributo in questa direzione, nella convinzione che la qualità di una disciplina giuridica si misura non tanto dalla quantità di norme nuove che introduce, quanto dalla coerenza con cui sa coordinare le norme già esistenti attorno a un disegno regolatorio comune.

1. Il presente scritto rientra nelle attività del Progetto EQUIP-FVG, dedicato alla realizzazione di un'infrastruttura per la comunicazione sicura, con particolare riferimento al settore della logistica e all'impiego di tecnologie quantistiche.
2. United Nations General Assembly, *International Year of Quantum Science and Technology, 2025*, Resolution 78/287, 7 giugno 2024, UN Doc A/RES/78/287.
3. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Quantum Europe Strategy: Quantum Europe in a Changing World*, COM(2025) 363 final, Bruxelles, 2 luglio 2025 (CELEX 52025DC0363; in EUR-Lex, <http://data.europa.eu/eli/com/2025/363/oj>).
4. La proposta di *Quantum Act* è annunciata dalla Commissione al punto 3.1 della Comunicazione COM(2025) 363 final, con presentazione prevista per il corrente anno. Cfr. anche European Parliament, Legislative Train Schedule, *Quantum Europe Strategy*, in <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-eu-quantum-strategy>.
5. Tra i primi contributi v. S. Gulyamov, *Quantum Law: Navigating the Legal Challenges and Opportunities in the Age of Quantum Technologies*, in *Uzbek Journal of Law and Digital Policy*, vol. 1, 1, 2023; K. Balarabe, *Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap*, in *European Journal of Risk Regulation*, vol. 16, 2025, p. 794 ss., doi:10.1017/err.2025.8; M. Kop, *Towards a European Quantum Act: A Two-Pillar Framework for Regulation and Innovation*, in *Columbia Journal of European Law*, vol. 31, 1, 2025, in corso di pubblicazione (preprint su SSRN, abstract n. 5480630, e su arXiv:2509.14262); R.J. Neuwirth, *A Future European Union 'Quantum*

- Act? Critical Lessons from the Global AI Governance Debate*, in *Macau Journal of Global Legal Studies*, vol. 2, 2025. Per una ricognizione precedente sui profili IP v. M. Kop, M. Aboy, T. Minssen, *Intellectual Property in Quantum Computing and Market Power: A Theoretical Discussion and Empirical Analysis*, in *Journal of Intellectual Property Law & Practice*, vol. 17, 8, 2022, p. 613 ss.
6. R. Bin, *A discrezione del giudice. Ordine e disordine: una prospettiva «quantistica»*, FrancoAngeli, Milano, 2013; Id., *Ordine delle norme e disordine dei concetti (e viceversa). Per una teoria quantistica delle fonti del diritto*, paper disponibile sul sito dell'Autore. Si tratta di un uso epistemologico della metafora quantistica applicato alla teoria dell'interpretazione, distinto dall'oggetto del presente saggio.
 7. Commissione europea, COM(2025) 363 final, cit., qualificata come espressione ufficiale della posizione politica e dell'intento strategico della Commissione indirizzata alle altre istituzioni dell'Unione.
 8. COM(2025) 363 final, sezione 2. Le cinque aree sono: (1) Research and Innovation; (2) Quantum Infrastructures; (3) Strengthening the Quantum Ecosystem; (4) Space and Dual-Use Quantum Technologies (Security and Defence); (5) Quantum Skills.
 9. Cfr. Commissione europea, *A Competitiveness Compass for the EU*, COM(2025) 30 final, 29 gennaio 2025, che include il quantum tra i settori tecnologici chiave.
 10. COM(2025) 363 final, nota 3: «*For the purposes of this Strategy, dual-use potential denotes the capacity of quantum technologies to serve both civilian and security/defence ends. It is employed here in a broader, forward-looking sense than the legal term 'dual-use items' under Regulation (EU) 2021/821 on export controls*». Sui rapporti con la dottrina dell'autonomia strategica aperta v. Commissione europea, *Joint Communication on the European Economic Security Strategy*, JOIN(2023) 20 final.
 11. COM(2025) 363 final, sezione 3.1: «*In 2026, Propose the 'Quantum Act' establishing a Quantum Europe Research and Innovation Initiative*».
 12. Commissione europea, *Call for Evidence – Quantum Act*, lanciata il 29 ottobre 2025, scadenza prorogata al 15 dicembre 2025, pubblicata sull'Have Your Say Portal. I tre «structural problems» sono individuati nel documento di consultazione.
 13. Le anticipazioni di metodo provengono in particolare dall'intervento di Gustav Kalbe, Head of Unit Quantum Technologies della DG CNECT, alla conferenza del 1° ottobre 2025, riportate da Global Legal Insights, *Quantum Computing Laws and Regulations 2026 – European Union*. La proposta di emendamento al Regolamento EuroHPC per l'introduzione di un *Quantum Pillar* è stata presentata dalla Commissione il 15 luglio 2025 (COM(2025) 414 final) e definitivamente adottata dal Consiglio il 16 gennaio 2026 con il Regolamento (UE) 2026/150, pubblicato in GU L del 19 gennaio 2026 (ELI: <http://data.europa.eu/eli/reg/2026/150/oj>). Il regolamento — adottato sulla base degli artt. 187 e 188, primo comma, TFUE — modifica il Reg. (UE) 2021/1173 estendendo il mandato dell'impresa comune EuroHPC alle tecnologie quantistiche e alle *AI gigafactories*. Tra le novità rilevanti sul versante quantistico: introduzione (i) della definizione di «*centro nazionale di competenza per il settore quantistico*» quale soggetto

giuridico o consorzio che offre alle PMI e alle amministrazioni l'accesso a tecnologie, strumenti, applicazioni, servizi e infrastrutture quantistiche (art. 1, par. 1, n. 1, che inserisce un nuovo n. 19-bis nell'art. 2 del Reg. 2021/1173); (ii) estensione degli obiettivi dell'impresa comune al «*calcolo quantistico*» e al «*supercalcolo*» integrati, federati, sicuri e iperconnessi a livello unionale, con il dichiarato fine di sostenere la transizione delle tecnologie quantistiche «*dal laboratorio alla produzione*» e di garantire la leadership europea nel calcolo, nella comunicazione e nel rilevamento quantistici; (iii) previsione che gli Stati membri possano destinare quote dei propri programmi nazionali (FESR, FSE+, PNRR rinnovati ecc.) al cofinanziamento di infrastrutture quantistiche europee, secondo modalità di *co-procurement* coordinate dall'impresa comune. Il regolamento è entrato in vigore il 20 gennaio 2026 (giorno successivo alla pubblicazione in GU L).

14. M. Kop, *Towards a European Quantum Act*, cit.
15. Ivi, abstract: «*Such a framework must be sui generis, as foundational quantum mechanical phenomena – incl. superposition, entanglement, and tunneling – defy the intuitive classical assumptions of factual certainty, causality, and locality that underpin existing legal paradigms, demanding a bespoke regulatory architecture that contributes to the emerging lex specialis for quantum information technologies*».
16. R.J. Neuwirth, *A Future European Union 'Quantum Act'?*, cit. L'Autore sottolinea l'importanza di trasformare gli stati attuali di incertezza in possibilità attraverso l'evidenziazione delle lacune della *global AI governance*.
17. Raccomandazione (UE) 2023/2113 della Commissione del 3 ottobre 2023 sui settori tecnologici critici per la sicurezza economica dell'UE. Il documento individua quattro aree tecnologiche di priorità immediata: semiconduttori avanzati; intelligenza artificiale; tecnologie quantistiche; biotecnologie.
18. La Strategia italiana per le tecnologie quantistiche è stata approvata dal Comitato Interministeriale per la Transizione Digitale il 10 luglio 2025 e pubblicata nella versione definitiva il 5 settembre 2025.
19. È un documento redatto dal Gruppo di lavoro coordinato dal prof. Tommaso Calarco e composto da esperti scientifici e da rappresentanti del Ministero dell'Università e della Ricerca, del Ministero delle Imprese e del Made in Italy, del Ministero della Difesa, del Ministero degli Affari Esteri e della Cooperazione Internazionale, dell'Agenzia per la Cybersicurezza Nazionale e del Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri. La bozza è stata posta in consultazione pubblica il 26 febbraio 2025; il documento è stato approvato dal Comitato Interministeriale per la Transizione Digitale (CITD) il 10 luglio 2025 e pubblicato nella versione definitiva il 5 settembre 2025. Sul piano sostanziale, la Strategia si fonda su quattro assi prioritari: (i) sviluppo scientifico e industriale lungo i cinque pilastri delle TQ (calcolo, simulazione, comunicazione, sensoristica, scienza di base); (ii) costruzione di un ecosistema nazionale integrato (ricerca, trasferimento tecnologico, industria, formazione); (iii) internazionalizzazione e tutela delle tecnologie critiche, con esplicito raccordo con i programmi UE; (iv) governance e misurabilità. Sul piano finanziario, la Strategia rileva che

i finanziamenti pubblici MUR alle TQ nel quadriennio 2021-2024 ammontano a 228,9 milioni di euro (di cui l'86% di derivazione PNRR), e individua nella creazione di reti pubblico-privato, nei dottorati industriali e nel sostegno al *venture deep-tech* gli strumenti per contrastare il fenomeno del *companies flight*. Sul versante della standardizzazione, la Strategia richiama il ruolo del Focus Group on Quantum Technologies (FGTQ) dell'ITU-T – sostituito dal 2024 dal nuovo ISO/IEC JTC 3 – e dichiara l'intento di rappresentare il consenso europeo nei consessi internazionali. La Strategia rinvia infine, per i profili di governance, a futuri sviluppi normativi che dovranno raccordarsi con il quadro europeo del *Quantum Act* in formazione.

20. A. Bartolini, *Diritto amministrativo dell'innovazione tecnologica*, Giappichelli, Torino, 2025. Una anticipazione del Capitolo II è pubblicata in *Diritto amministrativo*, 3, 2025, con il titolo *Dilemmi amministrativi e innovazione tecnologica, ovvero la signoria della prudenza amministrativa*. Per una distinta ma complementare ricostruzione sistematica, con specifico riguardo al rapporto tra digitalizzazione, intelligenza artificiale e procedimento amministrativo, v. R. Cavallo Perin, D.-U. Galetta (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Giappichelli, Torino, 2020 (con II ed. accresciuta, 2024); D.-U. Galetta, J. Ziller, *EU Administrative Law*, Edward Elgar, Cheltenham, 2024.
21. La prospettiva di una voce dottrinale di stakeholder industriale è offerta da *European Quantum Industry Consortium* (QuIC), *Position Paper on the Quantum Europe Strategy*, 2025, che, articolato sulle cinque aree della Strategia e su un sesto capitolo dedicato a software e algoritmi quantistici, propone fra l'altro: una governance europea capace di interrompere iniziative non più allineate alla visione strategica; un esplicito coordinamento fra estensione del mandato EuroHPC, linee pilota e futuro *Quantum Act*; il rafforzamento della *supply chain* europea con strumenti dedicati di sostegno alle PMI. Sul piano dottrinale italiano, per il parallelismo con il diritto amministrativo dell'intelligenza artificiale, v. G. Marchianò, *Intelligenza artificiale: IA specifiche e l'amministrazione provvedimentale – IA generali e i servizi pubblici*, in *Federalismi.it*, n. 11/2021, p. 137 ss., che distingue tra «*IA specifiche*» (algoritmi deboli applicati all'amministrazione provvedimentale e ai servizi pubblici) e «*IA generali*» (algoritmi forti), distinzione la cui logica – calibrare il regime giuridico al grado di autonomia decisionale del sistema – è in parte trasferibile al regime dei dispositivi quantistici secondo il loro “*technology readiness level*” e alla loro funzione (sostitutiva, ausiliaria, sperimentale).
22. A. Bartolini, *Diritto amministrativo dell'innovazione tecnologica*, cit., Cap. II, § 2, che ripercorre la tassonomia di Th. Schrepel (*Law and technology realism*, in MIT Computational Law Report, 14 agosto 2020).
23. A. Bartolini, *Diritto amministrativo dell'innovazione tecnologica*, cit., Cap. II, § 5. Sull'accezione debole del principio v. F. De Leonardis, *Il principio di precauzione*, in M. Renna, F. Saitta (a cura di), *Studi sui principi del diritto amministrativo*, Giuffrè, Milano, 2012, p. 413 ss.
24. A. Bartolini, *Diritto amministrativo dell'innovazione tecnologica*, cit., Cap. II, § 6. Sulla

- «precauzione inversa» v. Cons. St., sez. III, 20 ottobre 2021, 7045 in materia di vaccini.
25. A. Bartolini, *Diritto amministrativo dell'innovazione tecnologica*, cit., Cap. III, § 9, che segnala come la disciplina sia «sempre più orientata a difendere le nuove tecnologie e i nuovi beni, indicati dalla normativa europea e nazionale come tecnologie critiche», con riferimento espresso al Regolamento (UE) 2019/452, art. 4, § 1, lett. b), che include tra di esse la tecnologia quantistica.
 26. A. Bartolini, *Diritto amministrativo dell'innovazione tecnologica*, cit., Cap. IV, Parte I, § 2. V. anche E. Cirone, *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative*, in *Riv. it. informatica e diritto*, 1, 2025, p. 257 ss.
 27. Per questa impostazione è d'obbligo rinviare alla riflessione sviluppata da D.-U. Galetta in più sedi: in particolare D.-U. Galetta, *Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE e tecnologie ICT)*, in R. Cavallo Perin, D.-U. Galetta (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Giappichelli, Torino, 2020, p. 85 ss.; Ead., *Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal PNRR e problemi ancora da affrontare*, in *Federalismi.it*, 7, 2022. Sulla nozione di IA come strumento dell'azione amministrativa e non come fine v. D.-U. Galetta, J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019; D.-U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Rivista italiana di diritto pubblico comunitario*, 6, 2020, p. 501 ss.; Ead., *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini?*, in *Cyberspazio e Diritto*, 2020. Per una sintesi di livello europeo v. D.-U. Galetta, J. Ziller, *EU Administrative Law*, Edward Elgar, Cheltenham, 2024.
 28. P.W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, in *SIAM Journal on Computing*, vol. 26, 5, 1997, p. 1484. Sul rilievo per la cybersicurezza v. D.J. Bernstein, T. Lange, *Post-Quantum Cryptography*, in *Nature*, vol. 549, 2017, p. 188 ss.
 29. Sul versante della Post-Quantum Cryptography (PQC), il National Institute of Standards and Technology statunitense ha finalizzato nell'agosto 2024 i primi tre standard post-quantum: FIPS 203 (ML-KEM, basato su CRYSTALS-Kyber), FIPS 204 (ML-DSA, basato su CRYSTALS-Dilithium) e FIPS 205 (SLH-DSA, basato su SPHINCS+). L'allineamento ISO/IEC è in corso. Sul versante della Quantum Key Distribution (QKD), è disponibile un Protection Profile certificabile secondo lo schema Common Criteria (ETSI GS QKD 016). Per orientare il lettore non specialista, conviene chiarire la portata dei riferimenti tecnici appena richiamati. Gli standard NIST rispondono alle due funzioni fondamentali della crittografia a chiave pubblica oggi esposte all'algoritmo di Shor: lo scambio sicuro delle chiavi e la firma digitale. FIPS 203 (denominato Module-Lattice-Based Key-Encapsulation Mechanism, in sigla ML-KEM) è un meccanismo di

incapsulazione delle chiavi che consente a due soggetti di stabilire una chiave segreta condivisa attraverso un canale non sicuro, in funzione sostitutiva di RSA o di Diffie-Hellman; FIPS 204 (Module-Lattice-Based Digital Signature Algorithm, ML-DSA) e FIPS 205 (Stateless Hash-Based Digital Signature Algorithm, SLH-DSA) sono schemi di firma digitale, destinati a rimpiazzare progressivamente RSA ed ECDSA. La sicurezza dei primi due (ML-KEM e ML-DSA) si fonda sulla presunta difficoltà computazionale di problemi su reticoli matematici – segnatamente il problema Module Learning With Errors – per i quali allo stato non sono noti algoritmi quantistici di risoluzione efficiente; quella del terzo (SLH-DSA) si fonda invece sulla sicurezza delle funzioni hash crittografiche, considerata più conservativa ma meno efficiente in termini di dimensione delle firme. Le denominazioni CRYSTALS-Kyber, CRYSTALS-Dilithium e SPHINCS+ corrispondono ai progetti originari di ricerca da cui gli standard NIST derivano per selezione e adattamento, all’esito di un processo competitivo di valutazione pubblica avviato nel 2016. Nel marzo 2025 il NIST ha inoltre selezionato HQC quale ulteriore algoritmo di Post-Quantum Cryptography, destinato ad assicurare una diversificazione del rischio crittografico rispetto agli schemi basati su reticoli matematici; tale selezione non coincide tuttavia con la pubblicazione di un nuovo standard FIPS definitivo.

30. P.W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, p. 124, in <https://ieeexplore.ieee.org/document/365700>.
31. Lo standard ETSI EN 319 122 definisce i requisiti per le firme elettroniche avanzate basate su CMS (CAeS - CMS Advanced Electronic Signatures), conformi al regolamento eIDAS per firme e sigilli digitali.
32. Si riporta il considerando n. 3: «*La direttiva 85/374/CEE ha rappresentato uno strumento efficace e importante, ma dovrebbe essere rivista alla luce degli sviluppi legati alle nuove tecnologie, compresa l'intelligenza artificiale (IA), ai nuovi modelli imprenditoriali dell'economia circolare e alle nuove catene di approvvigionamento globali, che sono fonte di incoerenze e di incertezza giuridica, specialmente in relazione al significato del termine "prodotto"*». L'esperienza maturata con l'applicazione di tale direttiva ha dimostrato inoltre che per il danneggiato è difficile ottenere il risarcimento del danno a causa sia delle limitazioni alla possibilità di presentare domande di risarcimento sia della difficoltà di raccogliere elementi di prova per dimostrare la responsabilità, soprattutto alla luce della crescente complessità tecnica e scientifica. Ciò riguarda anche le domande di risarcimento del danno in relazione alle nuove tecnologie. La revisione di tale direttiva promuoverebbe pertanto la diffusione e l'adozione di tali nuove tecnologie, compresa l'IA, riconoscendo nel contempo all'attore il medesimo livello di protezione indipendentemente dalla tecnologia interessata e a tutte le imprese maggiore certezza del diritto e condizioni di parità.
33. CEN-CENELEC, *Layer model of Quantum Computing*, CEN/CLC/TR 18202:2025, pubblicato il 3 settembre 2025 (annuncio CEN-CENELEC del 23 ottobre 2025). Si tratta del primo deliverable del JTC 22.

34. ETSI, *Quantum Key Distribution (QKD); Protection Profile (PP)*, ETSI GS QKD 016 (V1.1.1, aprile 2023; versione aggiornata V2.1.1, gennaio 2024). V. anche ETSI Press Release, *ETSI releases World First Protection Profile for Quantum Key Distribution*.
35. M. Kop, *Towards a European Quantum Act*, cit., sezione su *standards-first approach*. Per la composizione e gli obiettivi del WG 4 di CEN/CLC JTC 22 v. *Cybersecurity / network and information security (RP 2025)*, *Interoperable Europe Portal*: «CEN/CLC/JTC 22 WG4 is working on PQC, in particular on equitable analysis of and comparison between PQC and Quantum Cryptography (more specifically Quantum Key Distribution, QKD)».
36. Raccomandazione (UE) 2024/1101 della Commissione, dell'11 aprile 2024, su una *Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*, in GU L, 2024/1101, 12 aprile 2024 (ELI: <http://data.europa.eu/eli/reco/2024/1101/oj>). Il documento attuativo è NIS Cooperation Group, *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography – Part 1*, EU PQC Workstream, versione 1.1, 23 giugno 2025. Tra gli atti tecnici sopravvenuti v. anche NIST, *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (FIPS 203), *Module-Lattice-Based Digital Signature Standard* (FIPS 204), *Stateless Hash-Based Digital Signature Standard* (FIPS 205), agosto 2024; la selezione di HQC come quinto algoritmo PQC (marzo 2025); ETSI, *Quantum-Safe Hybrid Key Exchanges* (marzo 2025); ENISA, *Post-Quantum Cryptography – Integration study* (ed. aggiornata 2025).
37. EPO Boards of Appeal, decisione T 0641/00 *Two identities/COMVIK*, e successiva giurisprudenza consolidata sui *computer-implemented inventions*.
38. M. Kop, M. Aboy, T. Minssen, *Intellectual Property in Quantum Computing and Market Power*, cit. supra, nota 4.
39. Cfr. COM(2025) 363 final, cit., sezione 1, in cui la Commissione qualifica la Quantum Europe Strategy come «*evolving framework for Europe's quantum future*» e individua cinque assi interconnessi: (i) ricerca e innovazione; (ii) infrastrutture quantistiche; (iii) rafforzamento dell'ecosistema; (iv) tecnologie quantistiche per lo spazio e *dual-use* (sicurezza e difesa); (v) competenze. La medesima Comunicazione, alla sezione 3.1, individua nel *Quantum Act* il veicolo legislativo destinato a istituire la *Quantum Europe Research and Innovation Initiative*; al punto «*Smart implementation approach*» la Commissione precisa che la Strategia poggia su una «*tailored technology lifecycle implementation logic*», di cui la futura Iniziativa costituisce il nucleo operativo.
40. La Comunicazione COM(2025) 363 final, cit., riconduce ripetutamente l'azione strategica al binomio «*sovereign quantum ecosystem*» e «*scientific leadership*»: la sezione introduttiva qualifica la Strategia come strumento per «*turn Europe into a quantum powerhouse by fostering a resilient, sovereign quantum ecosystem*», mentre la sezione sulle infrastrutture insiste sulla «*strategic autonomy*» e sulla «*technological sovereignty*» come obiettivi di sistema. L'enunciazione di principi nel futuro *Quantum Act* troverebbe, in questa cornice, un fondamento ricavabile dalla stessa Strategia, oltre che dal quadro più ampio della *European Economic Security Strategy* (JOIN(2023) 20 final).
41. L'impresa comune costituisce uno degli strumenti di amministrazione indiretta

dell'Unione europea per l'esecuzione dei programmi di ricerca, sviluppo tecnologico e dimostrazione: la sua base nel diritto primario è l'art. 187 TFUE, ai sensi del quale «*per la realizzazione del programma quadro pluriennale, l'Unione può istituire imprese comuni o qualsiasi altra struttura necessaria all'efficace esecuzione dei programmi di ricerca, sviluppo tecnologico e dimostrazione dell'Unione*», mentre l'art. 188, primo comma, TFUE attribuisce al Consiglio, su proposta della Commissione e previa consultazione del Parlamento europeo e del Comitato economico e sociale, la competenza ad adottare le relative disposizioni attuative. Si tratta di una figura ibrida, costruita come partenariato istituzionalizzato a base composita, nella quale convergono – quali membri di un soggetto dotato di personalità giuridica autonoma – l'Unione (rappresentata dalla Commissione), gli Stati partecipanti e, di regola, soggetti privati riuniti in associazioni industriali rappresentative del settore. La governance tipica prevede un Governing Board a composizione pubblica per le decisioni strategiche, un Executive Director per la gestione operativa e organi consultivi a partecipazione mista per l'indirizzo scientifico e industriale. Sul piano finanziario l'impresa comune opera in regime di gestione indiretta ai sensi dell'art. 62, paragrafo 1, lett. c), del regolamento finanziario dell'Unione, con un bilancio alimentato da contributi della Commissione, contributi (anche in natura) degli Stati partecipanti e contributi dei membri privati; sul piano della responsabilità, è soggetta al controllo della Corte dei conti europea e al discharge annuale del Parlamento europeo, in un assetto di accountability che riproduce, mutatis mutandis, quello delle agenzie dell'Unione pur senza esserne formalmente assimilabile. L'EuroHPC Joint Undertaking, istituita nel 2018 dal regolamento (UE) 2018/1488 e rifondata dal regolamento (UE) 2021/1173 del Consiglio del 13 luglio 2021, è stata successivamente modificata dal regolamento (UE) 2024/1732 – che ha introdotto il pilastro delle *AI Factories* – e dal regolamento (UE) 2026/150 del Consiglio del 16 gennaio 2026, che vi ha aggiunto un autonomo pilastro dedicato alle tecnologie quantistiche e un pilastro dedicato alle *AI Gigafactories*. Sul piano amministrativo, lo strumento solleva profili che meritano attenzione: l'articolazione del rapporto con i programmi nazionali degli Stati partecipanti, di cui l'impresa comune diviene a un tempo destinataria di contributi e strumento di coordinamento; la convivenza, nei medesimi organi consultivi, di rappresentanti pubblici e privati portatori di interessi industriali, con le classiche questioni di prevenzione del conflitto di interessi e di trasparenza dei procedimenti decisionali; la sovrapposizione, sul piano funzionale, con le competenze tradizionalmente esercitate dalle amministrazioni nazionali della ricerca e dell'innovazione, in un equilibrio retto dal principio di sussidiarietà e dal correlato test di valore aggiunto unionale.

42. Cfr. COM(2025) 363 final, cit., sezione 3.1, ove la Commissione enuncia l'azione «In 2026, Propose the 'Quantum Act' establishing a Quantum Europe Research and Innovation Initiative» e precisa che l'Iniziativa «*will be implemented through an EU-level governance framework*». La medesima sezione prefigura, quale prima azione attuativa, la modifica del Regolamento (UE) 2021/1173 istitutivo dell'European High Performance Computing Joint Undertaking, al fine di includere un dedicato *Quantum Pillar* e di

coordinare le attività con Horizon Europe (Reg. UE 2021/695). La proposta di modifica è stata presentata dalla Commissione il 15 luglio 2025 quale prima azione attuativa della Strategia.

43. <https://jtc21.eu/>
44. Cfr. COM(2025) 363 final, cit., sezione 3.3 («*Strengthening the Quantum Ecosystem*»), che prefigura per il 2026 l'adozione di due *roadmaps* – la prima sull'industrializzazione dei *quantum chips*, la seconda sugli «*European quantum standards*» – e l'avvio di linee pilota in coerenza con il *Chips Act* (Reg. UE 2023/1781). L'impianto rinvia implicitamente al *New Legislative Framework*: l'ancoraggio della presunzione di conformità a standard armonizzati elaborati dai comitati tecnici europei (CEN/CLC JTC 22) costituisce, nell'esperienza dell'AI Act (Reg. UE 2024/1689) e del *Cybersecurity Act* (Reg. UE 2019/881), il principale strumento di adattabilità della disciplina alle evoluzioni tecnologiche.
45. Le milestone sono enunciate da NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, cit.: entro il 31 dicembre 2026, avvio delle strategie nazionali di transizione e degli inventari crittografici; entro il 31 dicembre 2030, completamento della migrazione PQC per i *high-risk use cases*; entro il 31 dicembre 2035, transizione completa per la generalità dei sistemi. La medesima Strategia (COM(2025) 363 final, cit., sezione 3.2) qualifica la transizione *quantum-safe* come una delle dimensioni costitutive delle infrastrutture quantistiche europee, prefigurandone il coordinamento con EuroQCI e con gli schemi ENISA.
46. La COM(2025) 363 final, cit., al paragrafo dedicato allo «*smart implementation approach*», descrive un modello «*tailored technology lifecycle implementation logic*» finalizzato ad accelerare il passaggio dalla ricerca al mercato; in quella sede la Commissione enuncia il ricorso a meccanismi di sostegno mirati (tra i quali le *quantum grand challenges*), che non escludono ma anzi presuppongono spazi normativi di sperimentazione assimilabili, sul piano regolatorio, alle *regulatory sandboxes* già delineate dall'art. 57 dell'AI Act. La trasposizione di tale modello al Quantum Act presupporrebbe, per garantire uniformità applicativa, una disciplina europea uniforme dei requisiti di accesso, vigilanza e *sunset*.
47. La COM(2025) 363 final, cit., sezione conclusiva, qualifica espressamente il proprio assetto di governance come «*two-level governance framework*»: un *high-level advisory board*, composto da scienziati ed esperti tecnologici europei, incaricato di una «*independent strategic guidance*» sull'attuazione della Strategia, e un «*structured cooperation framework*» con gli Stati membri, volto ad assicurare l'allineamento dei programmi nazionali con l'azione di livello unionale. La proposta di un *European Quantum Board* avanzata nel testo, oltre che il coordinamento con il regime di *foreign investment screening* (Reg. UE 2019/452) e con la cornice della European Economic Security Strategy (JOIN(2023) 20 final), si collocano in continuità con tale impostazione bipartita, di cui costituirebbero un'istituzionalizzazione più stabile.
48. In tal senso M. Kop, *Towards a European Quantum Act*, cit., § 7.3 e § 9, che propone una

- «International Quantum Agency (IQA)» sul modello dell'AIEA; in senso critico R.J. Neuwirth, *A Future European Union 'Quantum Act'?*, cit.
49. La nozione di prudenza amministrativa è categoria sistematicamente sviluppata da Bartolini (op. cit., pp. 45-47 e 93). L'A. la riconduce alla virtù cardinale classica della *phronesis* aristotelica e alla tradizione romana della *iuris prudentia*, da cui deriva il moderno canone della ragionevolezza nel diritto amministrativo: Zagrebelsky, citato da Bartolini, osserva infatti che «*“ragionevolezza” è una discutibile espressione per indicare ciò che classicamente si indicava come la “prudenza” nella trattazione del diritto*» (G. Zagrebelsky, *Il diritto mite*, Torino, 1992, p. 168). Nella sistemazione di Bartolini, la prudenza amministrativa è espressamente qualificata come «*virtù dinamica, capace di ponderare i rischi senza paralizzare le opportunità offerte dal progresso*», e quindi «*lungi dall'essere sinonimo di conservatorismo*» (op. cit., p. 93). Sul piano operativo, l'A. ne ricava un esito significativo: «*il criterio della prudenza applicato all'innovazione dovrebbe tradursi in quel principio di fiducia [...] che spinge a sostenere l'innovazione anziché a bloccarla*» (ibidem). La prudenza amministrativa, così intesa, non si oppone al principio di precauzione, ma alla sua applicazione massimalista: ne è anzi la versione ragionevole, capace di calibrare l'intervento sul concreto livello di maturità tecnologica e sul concreto rischio sistemico, evitando sia l'iperregolazione sia l'astensione totale. Per una ricostruzione filosofica del concetto cui Bartolini si richiama esplicitamente v. R. Bodei, *Prudenza*, in R. Bodei, G. Giorello, M. Marzano, S. Veca, *Le virtù cardinali*, Bari, 2018.