Scheda di Programma

Per l'attivazione nell'ambito del Corso di Dottorato di ricerca in Scienze delle Pubbliche Amministrazioni del seguente Programma di ricerca, a valere sulle risorse di cui al DM n. 351/2022, relativamente alla seguente Misura:

☐ **M4C1- Inv. 3.4** "*Didattica e competenze universitarie avanzate*" → **Dottorati dedicati alle transizioni digitali e ambientali.**

☒ **M4C1- Inv. 4.1** *"Estensione del numero di dottorati di ricerca e dottorati innovativi per la pubblica amministrazione e il patrimonio culturale".* In particolare:

☒ **Dottorati PNRR**

☐ **Dottorati per la Pubblica Amministrazione**
(selezionare l'area/le aree CUN di riferimento del programma tra quelle di seguito indicate)

- ☐ Area 09 – Ingegneria industriale e dell'informazione
- ☐ Area 11 – Scienze storiche, filosofiche, pedagogiche e psicologiche
- ☐ Area 12 – Scienze giuridiche
- ☐ Area 13 – Scienze economiche e statistiche
- ☐ Area 14 – Scienze politiche e sociali

☐ **Dottorati per il patrimonio culturale**
(selezionare l'area/le aree disciplinare/i e la tematica del programma tra quelle di seguito indicate)

- ☐ Area 01 – Scienze matematiche e informatiche **Tematica** – Informatica, patrimonio e beni culturali
- ☐ Area 02 – Scienze Fisiche **Tematica** – Fisica applicata al patrimonio culturale e ai beni culturali
- ☐ Area 03 – Scienze chimiche **Tematica** – Chimica, ambiente, patrimonio e beni culturali
- ☐ Area 04 Scienze della Terra **Tematica** – Georisorse minerarie per l'ambiente, il patrimonio e i beni culturali
- ☐ Area 05 Scienze Biologiche **Tematica** - Ecologia, patrimonio e beni culturali
- ☐ Area 08 – Ingegneria civile e Architettura **Tematiche** 1) Architettura, ambiente antropizzato, patrimonio e beni culturali 2) Architettura e paesaggio 3) storia dell'architettura; 4) Restauro; 5) Pianificazione e progettazione dell'ambiente antropizzato; 6) Design e progettazione tecnologica dell'architettura
- ☐ Area 10 Scienze dell'antichità, filologico-letterarie e storico -artistiche **Tematiche** 1) Archeologia; 2) Storia dell'arte; 3) Media, patrimonio e beni culturali
- ☐ Area 11 – Scienze storiche, filosofiche, pedagogiche, psicologiche **Tematiche** 1) Biblioteconoma; 2) Archivistica; 3) Storia del patrimonio e dei beni culturali 4) Paleografia; 5) Estetica; 6) Didattica dell'arte; 7) pedagogia dell'Arte
- ☐ Area 12 - Scienze giuridiche **Tematica** Diritto del patrimonio culturale
- ☐ Area 13 - Scienze Economiche e statistiche **Tematiche** 1) Economia della cultura e dell'arte 2) Economia e gestione delle imprese artistiche e culturali; 3) Statistica e Data Analytics per i beni culturali
- ☐ Area 14 Scienze Politiche e sociali **Tematiche** 1) Sociologia dei beni culturali 2) sociologia dell'ambiente e del territorio

- **Titolo del Programma di ricerca**: La sicurezza pubblica nazionale e comunitaria: i temi della cybersicurezza come declinati nel *next generation Ue e nel Pnrr*.

- **Title of the Research Programme**: National and EU public security: cybersecurity issues as declined in the next generation EU and in the PNRR.

- **Descrizione** (MAX 5000 CARATTERI SPAZI ESCLUSI)**:**

All’inizio del XXI secolo, il tema della sicurezza e dell'ordine pubblico conosce una particolare rilevanza in forza della emersione di tre fenomeni concomitanti: la messa in discussione dell’effettività dei diritti sociali a causa delle crisi economiche; l’emersione di conflitti politico-religiosi radicali; l’invasività delle nuove tecnologie nella sfera privata degli individui.

Nell’odierno «Stato di prevenzione» il rischio si atteggia a ordinaria condizione dell’esperienza sociale e fondamento delle discipline legislative che determinano un nuovo equilibrio tra libertà e sicurezza. L’aspirazione alla massima sicurezza correlata alla prevenzione pregiudica la certezza del diritto e pone un problema per i sistemi politici democratici. Nella società del rischio, con la crescita dei pericoli si devono affrontare sfide completamente nuove per la democrazia. La società del rischio ha insita una tendenza ad un «legittimo» totalitarismo di difesa dai pericoli, che partendo dal diritto di evitare il peggio conduce, com’è fin troppo noto, al «peggio ancora».

A livello legislativo, gli artt. 6 e 7 della legge 3 agosto 2007, n. 124 sul segreto di Stato hanno ricondotto la sicurezza nazionale alla «*difesa dell’indipendenza, dell’integrità e della sicurezza della Repubblica*» oppure alla «*sicurezza interna della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica*». In questa prospettiva, si può ritenere che la sicurezza nazionale vada intesa come interesse che prefigura sia azioni all’estero in settori prevalentemente non militari, cioè in ambito politico, diplomatico, economico e finanziario (ad es. sicurezza dei rifornimenti energetici, protezione dei connazionali residenti all’estero, commercio con l’estero di materiale strategico, trasferimenti tecnologici ed aiuti economici ai paesi in via di sviluppo), sia misure preventive e repressive di quelle situazioni interne al territorio nazionale, le quali, anche con le armi, mettano in concreto e grave pericolo il funzionamento o la stessa sopravvivenza degli organi costituzionali e delle altre istituzioni della Repubblica.

Quanto sopra investe un tema complesso e di particolare attualità, proiettandosi a pieno titolo sui temi della cyber sicurezza, che costituisce la più recente ed assai ambiziosa politica inserita nell'ambito del PNRR.

La prima proposta d’azione del Governo per la protezione tecnologica è la c.d. "Cloud First per la PA" (ovvero: Reti ultraveloci; 5G; Sviluppo di un Cloud nazionale; Interoperabilità delle banche dati; Tecnologie satellitari ed economia spaziale). La tecnologia cloud è utilizzata soprattutto in chiave difensiva e di protezione dei dati sensibili e delle infrastrutture critiche della pubblica amministrazione.

La seconda proposta d’azione del Governo sulla cyber-security concerne la sovranità tecnologica nazionale, nell'ambito della quale vi è l'intento di istituire (in sinergia tra *Ministero della Difesa*, *Pubblica Amministrazione*, *Intelligence* e *Presidenza del Consiglio*) l’*Agenzia Nazionale per la Cybersecurity*. La direzione è, dunque, quella di dar luogo ad una sovranità tecnologica nazionale, allo sviluppo di strategie difensive, nonchè alla condivisione di *know how* e *best practices*. Attraverso l’*Agenzia nazionale per la Cybersecurity* l'obiettivo è affrontare le nuove ed attuali sfide nazionali e internazionali, distinguendo concettualmente tra *cyber resilience*, *cyber intelligence*, *cyber defence* e *cyber investigation*. Il percorso per giungere a siffatto obiettivo comprende la relazione tra intelligenza artificiale e intelligenza umana e tra settore pubblico e privato.

La terza proposta d’azione del Governo per la sicurezza informatica in Italia è quella della partnership con le aziende (pubblico-privato). Il Polo strategico nazionale (Psn) è una infrastruttura che deve ospitare “in cloud” i dati strategici della *Pubblica Amministrazione*.

La quarta proposta d’azione del Governo per la cyber-security in Italia concerne la collaborazione tra Stati europei, attraverso la revisione della direttiva NIS, la creazione di un’unità congiunta per il cyberspazio per rafforzare la cooperazione tra le istituzioni, gli organismi e le agenzie dell’Ue, l'adozione di norme orizzontali per migliorare la cybersecurity dei prodotti connessi presenti sul mercato interno, l'istituzione del Centro europeo di competenza per la cybersicurezza e la rete dei centri nazionali di coordinamento, l'istituzione del Fondo europeo per la difesa. L'Ue e la Nato permarranno nell'attuale collaborazione nella cyberdefence tramite il Team CERT-UE (EU’s Computer Emergency Response Team) e la *Computer Incident Response Capability* della NATO.

L'idea è quella di raggiungere una sovranità cibernetica europea, funzionale alla difesa ed alla prevenzione dagli attacchi cyber, sempre più pericolosi per le nostre infrastrutture e per la sicurezza nazionale.

At the beginning of the twenty-first century, the theme of security and public order knows a particular relevance because of the emergence of three concomitant phenomena: the questioning of the effectiveness of social rights due to economic crises; the emergence of radical political-religious conflicts; the invasiveness of new technologies in the private sphere of individuals.

In today's "state of prevention" risk poses as an ordinary condition of social experience and the foundation of the legislative disciplines that determine a new balance between freedom and security. The aspiration to maximum security related to prevention undermines legal certainty and poses a problem for democratic political systems. In the risk society, with the growth of dangers, completely new challenges to democracy must be faced. The risk society has inherent a tendency towards a "legitimate" totalitarianism of defense against dangers, which starting from the right to avoid the worst leads, as is all too well known, to the "worst still". At the legislative level, Articles 6 and 7 of Law No 124 of 3 August 2007 on State Secrecy have brought national security back to the 'defence of the independence, integrity and security of the Republic' or to the 'internal security of the Republic and the democratic institutions laid down by the Constitution as its foundation from any threat, from any subversive activity and from any form of criminal or terrorist aggression'. In this perspective, it can be considered that national security should be understood as an interest that prefigures both actions abroad in mainly non-military sectors, that is, in the political, diplomatic, economic and financial spheres (e.g. security of energy supplies, protection of compatriots residing abroad, foreign trade in strategic material, technological transfers and economic aid to developing countries). preventive and repressive measures of those situations within the national territory, which, even with weapons, put in concrete and serious danger the functioning or the very survival of the constitutional bodies and other institutions of the Republic.

The above involves a complex and particularly topical issue, projecting itself fully on the issues of cyber security, which is the most recent and very ambitious policy included in the PNRR.

The first proposal for action of the Government for technological protection is the so-called "Cloud First for the PA" (i.e.: Ultrafast networks; 5G; Development of a national Cloud; Interoperability of databases; Satellite technologies and space economy). Cloud technology is mainly used in terms of defense and protection of sensitive data and critical infrastructures of the public administration.

The second proposal for action of the Government on cyber-security concerns national technological sovereignty, within which there is the intent to establish (in synergy between the Ministry of Defense, Public Administration, Intelligence and the Presidency of the Council) the National Agency for Cybersecurity. The direction is, therefore, to give rise to a national technological sovereignty, to the development of defensive strategies, as well as to the sharing of know-how and best practices. Through the National Cybersecurity Agency, the goal is to address new and current national and international challenges, conceptually distinguishing between cyber resilience, cyber intelligence, cyber defence and cyber investigation. The path to achieving this goal includes the relationship between artificial intelligence and human intelligence and between the public and private sectors.

The third proposal for action of the Government for IT security in Italy is that of partnership with companies (public-private). The National Strategic Pole (PSN) is an infrastructure that must host "in the cloud" the strategic data of the Public Administration.

The fourth proposal for action of the Government for cyber-security in Italy concerns collaboration between European States, through the revision of the NIS Directive, the creation of a joint unit for cyberspace to strengthen cooperation between EU institutions, bodies and agencies, the adoption of horizontal rules to improve the cybersecurity of connected products on the internal market, the establishment of the European Cybersecurity Competence Centre and the Network of National Coordination Centres, the establishment of the European Defence Fund. The EU and NATO will remain in their current cyberdefence collaboration through the EU's Computer Emergency Response Team (CERT-EU) and NATO's Computer Incident Response Capability.

The idea is to achieve a European cyber sovereignty, functional to the defense and prevention of cyber attacks, increasingly dangerous for our infrastructures and for national security

✥ PERIODO IN IMPRESA – CENTRI DI RICERCA – P.A.:

Il Programma di ricerca sarà svolto in collaborazione con il seguente soggetto:

Ragione sociale: Studio legale "Mannuccia"
Sede legale: Via Camiciotti 8 - Messina
Rappresentante legale: Avv. Giovanni Mannuccia

L''ente sopra citato ospiterà il dottorando beneficiario della borsa finanziata sulle risorse del DM 351/2022 per n. 6 mesi nel corso del dottorato.

❖ **PERIODO ALL'ESTERO:**

Il Programma di ricerca prevede un periodo all'estero di n. 6 mesi presso la seguente istituzione:
UNIVERSETI SHKODRES LUIGJ GURAKUQI - SHKODER (Albania)

Si dichiara inoltre che il presente programma è conforme al principio "di non arrecare un danno significativo" (DHSH) ai sensi dell'art. 17 del regolamento (UE) 2020/852 in coerenza con gli orientamenti tecnici predisposti dalla Commissione Europea (Comunicazione della Commissione Europea 2021/C58/01) e garantisce il rispetto dei principi orizzontali del PNRR (contributo all'obiettivo climatico e digitale c.d. tagging, il principio della parità di genere e l'obbligo di protezione e valorizzazione dei giovani).