Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Computer Science for Societal Challenges and Innovation**
Tipologia di borsa	Ex DM 630/2024
Titolo del progetto	Tecnologie di Intelligenza Artificiale per lo Sviluppo di Software
Referente Scientifico	Alessandro Sperduti
Email Referente Scientifico	alessandro.sperduti@unipd.it
Descrizione del progetto	This Ph.D. research project aims to develop and explore the application of Artificial Intelligence (AI) in enhancing the capabilities of Digital Adoption Platforms (DAPs). The primary focus is on leveraging AI to improve the efficiency, effectiveness, and user experience of these platforms. By integrating advanced machine learning techniques, the research intends to optimize the performance of DAPs, making them more responsive and adaptive to user needs. Additionally, the study will delve into the realm of Human-Computer Interaction (HCI) within the DAP sector. It will analyze how users interact with these platforms and identify opportunities for AI to make these interactions more intuitive and seamless. The integration of AI and HCI aims to provide personalized user experiences that cater to individual preferences and behaviors.
Periodo da svolgere in impresa	6
Soggetto finanziatore o cofinanziatore	myMeta S.r.l

Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Computer Science for Societal Challenges and Innovation**
Tipologia di borsa	Ex DM 630/2024
Titolo del progetto	Metodi e Applicazioni dell'Apprendimento Automatico Continuo
Referente Scientifico	Alessandro Sperduti
Email Referente Scientifico	alessandro.sperduti@unipd.it
Descrizione del progetto	This Ph.D. research project aims to study novel methodologies and applications of continual learning for Deep Learning models. The main focus of the project will be on efficiency and effectiveness, with the aim of developing approaches that are sustainable from the point of view of required training data and compute, as well as applicable in all application domains where the environment is continuously changing and/or new functionalities should be gradually and autonomously acquired by the system implementing them. Examples of potential applications will be in the context of Smart Cities, Sustainable Agriculture, Smart Healthcare, and Human-Computer Interaction (HCI). Moreover, the developed methodologies should take into consideration all the dimensions of trustworthy AI, as described in the EU ethics guidelines, and in agreement with the human-centered AI approach outlined in the FBK 2024-2027 Strategic Plan (https://www.fbk.eu/wp-content/uploads/2024/04/PDM_ENG_web.pdf).
Periodo da svolgere in impresa	6
Soggetto finanziatore o cofinanziatore	Fondazione Bruno Kessler

Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Computer Science for Societal Challenges and Innovation**
Tipologia di borsa	Borsa da Finanziatori Esterni e da Dipartimenti
Titolo del progetto	Robust AI
Referente Scientifico	Mauro Conti
Email Referente Scientifico	mauro.conti@unipd.it
Descrizione del progetto	AI is being widely adopted in several areas, from healthcare to the automotive industry, and from agriculture to the industrial sector. Many of these applications are sensitive both in terms of safety and security. Therefore, it becomes of paramount importance to understand if and how attackers can exploit such systems and to design more robust ones. This project aims to focus on “adversarial machine learning,” both from the attacker’s point of view, to understand ways an adversary can abuse AI solutions to gain an advantage (with attacks such as model stealing, model poisoning, or membership inference), and from the defense’s point of view, to explore novel techniques to make AI solutions more robust against these attacks.
Periodo da svolgere in impresa	n.a.
Soggetto finanziatore o cofinanziatore	Fondazione Bruno Kessler - FBK

Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Computer Science for Societal Challenges and Innovation**
Tipologia di borsa	Borsa da Finanziatori Esterni e da Dipartimenti
Titolo del progetto	Intelligenza artificiale per le città intelligenti
Referente Scientifico	Alessandro Sperduti
Email Referente Scientifico	alessandro.sperduti@unipd.it
Descrizione del progetto	The research activity will involve one or more of the following topics: Use of generative AI in the context of citizen access to services; Analytics in the context of city mobility; Analytics in the environmental field; Analytics in the field of real estate.
Periodo da svolgere in impresa	n.a.
Soggetto finanziatore o cofinanziatore	Comune di Padova con il contributo del Centro Interdipartimentale di Ricerca "Human Inspired Technologies Research Center - HIT"

Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Computer Science for Societal Challenges and Innovation**
Tipologia di borsa	Borsa da Finanziatori Esterni e da Dipartimenti
Titolo del progetto	Verso una Intelligenza Artificiale Esplicabile e Sicura con Prevenzione dell'Utilizzo Improprio nei LLMs
Referente Scientifico	Roberto Confalonieri
Email Referente Scientifico	roberto.confalonieri@unipd.it
Descrizione del progetto	Verso una Intelligenza Artificiale esplicabile e sicura con prevenzione dell'utilizzo improprio nei LLMs Towards Secure Explainable AI and Misuse Prevention in LLMs Understanding machine learning models, also known as opaque or black-box models, is crucial to ensure the transparency of their decisions. Explicable AI (XAI) has emerged as a research field with practical and ethical benefits in various fields [1]. Despite the significant progress of XAI, significant challenges persist for its adoption and applicability in AI [2]. This project focuses on two main challenges. On the one hand, although XAI provides techniques to explain opaque models, their applicability is limited to classification and regression problems. Furthermore, generative AI, especially Large Language Models (LLMs), has revolutionised human-computer interaction by demonstrating how Deep Neural Networks (DNNs) can understand complex texts, but are opaque and prone to hallucination. Explaining how they generate content is essential to guarantee transparency and improve the training process. On the other hand, current XAI methods show vulnerabilities and security problems [2], with explanations that can be exploited for attacks such as model poisoning, membership attacks and model extraction. Generative models show vulnerabilities in the security of training data [3], leading to an increase in social engineering campaigns. LLMs require huge training sets and continuous updates with user feedback, including potentially sensitive data. Once in production, DNNs and LLMs can be tricked [4], forcing them to reveal sensitive information. This project proposes to examine new explainability approaches for generative AI, aiming to protect the data used in training and explaining opaque models, especially from a privacy perspective. It is proposed to study the application of data protection techniques such as differential privacy or multiparty computation, and to investigate mechanisms to detect and prevent attacks based on explanation and social engineering. Approaches such as output watermarking and detection of characteristic patterns in the outputs of LLMs will be explored to improve the security and transparency of such models. The proposal aims to advance the state of the art in the area of XAI, and protection of private data and protection against misuse of DNNs and LLMs. The results of the proposed research will contribute to increasing trust in AI applications, XAI, and protecting users from privacy violations and social engineering attacks. The objectives of the project are as follows: 1) To create new secure and privacy-preserving XAI methods for generative AI. 2) To detect privacy violations in sensitive data storage processes of DNNs and LLMs. 3) To detect of social engineering activities based on LLMs. 4) To develop an end-to-end methods for secure and privacy-preserving training, inference and explanation.

Periodo da svolgere in impresa	n.a.
Soggetto finanziatore o cofinanziatore	Agenzia per la Cybersicurezza Nazionale – ACN – CUP C96E24000010005

Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Computer Science for Societal Challenges and Innovation**
Tipologia di borsa	Borsa da Finanziatori Esterni e da Dipartimenti
Titolo del progetto	Profilazione e Gestione a Run-time degli Attacchi a Process-aware Information Systems
Referente Scientifico	Massimiliano De Leoni
Email Referente Scientifico	massimiliano.deleoni@unipd.it
Descrizione del progetto	The steps of automation and digitalization of our society have naturally unfolded through the deployment of on-line information systems and portals that provide support to citizens and enterprises with the participation and management of their organizational processes. It is clearly critical these systems and portals be secure and trustable: this project aims to ensure potential real-time attacks be detected and subsequently managed so as to mitigate their negative effect on systems and processes. The final deliverable is a prototype of a software module to connect to information systems, in order to identify, profile and mitigate the attacks. The project will start from the analysis of the activity logs carried out by users via information systems, so as to extract the patterns of the (il)legitimate users. In doing so, the methodology and algorithms will leverage on Process-Mining techniques, which, among different goals, focus on the analysis and monitoring of business processes.
Periodo da svolgere in impresa	n.a.
Soggetto finanziatore o cofinanziatore	Agenzia per la Cybersicurezza Nazionale – ACN – CUP C96E24000010005

Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Computer Science for Societal Challenges and Innovation**
Tipologia di borsa	Borsa da Finanziatori Esterni e da Dipartimenti
Titolo del progetto	Resilienza dei Sistemi Collaborativi di Guida Autonoma: Trusted Computing e Garanzie di Privacy
Referente Scientifico	Mauro Conti
Email Referente Scientifico	mauro.conti@unipd.it
Descrizione del progetto	Autonomous driving systems require a collaborative approach in which each vehicle receives data about the vision of a group of other nearby vehicles in order to make informed decisions. This opens the scenario to new threats to vehicle privacy, such as tracking, identification, and profiling of vehicles and their drivers. In this project, we want to redefine the concept of an autonomous and intelligent transport system to make it both resilient and privacy-preserving. In the first phase of the project we will define new online attacks against current cooperative autonomous driving systems. In the second phase, we will develop algorithms for resilience to both state-of-the-art attacks and those defined by us in the first phase. In the third step, we will assess the sensitivity of shared data and define new strategies for minimising the sharing of shared data that can at the same time ensure the fundamental security requirements.
Periodo da svolgere in impresa	n.a.
Soggetto finanziatore o cofinanziatore	Agenzia per la Cybersicurezza Nazionale – ACN – CUP C96E24000010005

Corso di Dottorato	**BRAIN, MIND AND COMPUTER SCIENCE**
Curriculum *(eventuale)*	**Neuroscience, Technology and Society**
Tipologia di borsa	Ex DM 630/2024
Titolo del progetto	Validazione di una nuova strumentazione bioimpedenziometrica per la valutazione della composizione corporea
Referente Scientifico	Antonio Paoli
Email Referente Scientifico	antonio.paoli@unipd.it
Descrizione del progetto	The project is aimed to validate a new device, developed by Technogym for body composition analysis. This innovative device will use bioimpedance technique to evaluate subjects' body composition in a standing position together with numerous other fitness outcomes. The project will validate the device with DXA (Dual energy Xray absorptiometry) in a general population of both sexes and different ages. Moreover, we will estimate water content and compare it with another bioimpedance device that uses a hand-to-foot technology. The expected results are the validation of this new instrument and the creation of an algorithm specifically studied for this new standing bioimpedance device. This new device will allow to determine health condition in the population (body composition will be integrated with other physical fitness and psychological tests) and, consequentially, to adopt and design healthier personalized lifestyle interventions.
Periodo da svolgere in impresa	6
Soggetto finanziatore o cofinanziatore	Technogym S.p.A.