RESEARCH THEME

XXVII cycle – a.y. 2021/2022

Title of the doctoral research	Knitting Adversarial Patches through Machine Learning for Privacy and Ethics
Proponent professor	Giovanni Maria Conti
Abstract	The following PHD program regards the design, development and validation of models, methods, and tools aimed at dealing with one of these large-scale changes from the interdisciplinary perspective of Design (Textile and Knitwear) and of Computer Engineering (Machine Learning and Privacy), when they operate in a specific industrial sector such as that of knitwear, where advanced technological innovation coexists with traditional technologies and with the obsessive care for craftsmanship. The goal is to integrate knitwear skills with Machine Learning techniques to realize a set of tools for the production of antagonistic patches integrated into the texture, designed to be worn and to blend perfectly with the shape of the body. These clothes will be able to make customers aware of the importance of preserving their privacy and allow them to protect their identity in the presence of facial recognition cameras, also in the light of ethical aspects related to use of personal information. First of all, studying these techniques for textiles serves both to evade face recognition systems (adversarial attack) in order to protect one's privacy, and on the contrary to neutralize their evasion and therefore to develop more robust and safer biometric systems. Therefore, the research represents a cutting-edge issue. In both cases (adversarial attacks and defense) these researches use Machine Learning techniques, in the first case to select the most effective adversarial patterns and vice versa in the second case to make the systems resistant to adversarial attacks (including these patterns in the training). In addition to face recognition, the theme of adversarial attacks is also critical for other computer applications, such as self-driving vehicles and various systems based on computer vision. The challenge lies in the inclusion of adversarial patches into knitwear in an automatic and privacy-preserving way.
Keywords	Textile, Knitwear, Adversarial Patches, Computer vision, Artificial Intelligence, Facial Recognition Cameras, Privacy Awareness, Human Rights