

Degree programme	Type	Course
Prevention and Integral Safety and Security	OP	4

Contact lecturer

Name : Xavier Dorado Ferrer

Email : xavier.dorado@uab.cat

Prerequisites

This subject does not have any previous requirements, although it is advisable to have passed the following subjects:

-Safety Technology.

- Data Protection and Information Security.

Group languages

You can consult this information at the [end](#) of the document.

Objectives

The subject Security and Technology, within the framework of the public security coordinator mention, addresses the different issues that affect security processes in relation to new technologies.

Specifically, two cases closely related to artificial intelligence, big data and remote control devices will be studied:

A) Biometrics for public and private security purposes.

B) The use of drones for investigative purposes within the framework of public police and judicial powers.

More specifically, the impact of these technologies on the sophistication of security processes will be analyzed, taking into account the legal framework of automated decisions and their impact on fundamental rights, equality and the principle of transparency.

Learning outcomes

1. Coordinate the resources of the three main subsystems of the prevention and integral security sector: people, technology and infrastructures.
2. Use the capacity for analysis and synthesis to solve problems.
3. Respond to problems applying knowledge to practice.
4. Work in institutional and interprofessional networks.
5. Students must have and understand knowledge of an area of study built on the basis of general secondary education, and while it relies on some advanced textbooks it also includes some aspects coming from the forefront of its field of study.
6. Students must be capable of applying their knowledge to their work or vocation in a professional way and they should have building arguments and problem resolution skills within their area of study.
7. Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.

8. Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.
9. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
10. Propose new methods or well-founded alternative solutions.
11. Critically analyse the principles, values and procedures that govern professional practice.
12. Propose projects and actions that incorporate the gender perspective.
13. Propose viable projects and actions that promote social, economic and environmental benefits.
14. Draw up management proposals for prevention and security in an organisation.
15. Analyse the preventative interventions in matters of security, environment, quality and social corporate responsibility and identify the inherent risk factors.
16. Work and learn autonomously.
17. Know how to communicate and transmit ideas and result efficiently in a professional and non-expert environment, both orally and in writing.
18. Make efficient use of ITC in the communication and transmission of results.
19. Analyse the situation and identify the points that are best.

Contents

Technology applied to security and new risk scenarios

- 1.1. Technological transformation of public and private security systems.
- 1.2. Digitalisation of prevention, surveillance, identification, investigation and emergency management processes.
- 1.3. Artificial intelligence, big data, sensors, advanced video surveillance and automated systems applied to security.
- 1.4. Operational opportunities and new legal, ethical and organisational risks arising from the use of emerging technologies.
- 1.5. Impact of technology on fundamental rights, privacy, equality, non-discrimination and professional responsibility.

Biometric identification systems in public and private security

- 2.1. Concept of biometric identification, biometric authentication, biometric data, biometric sample and biometric template.
- 2.2. Basic functioning of biometric systems: capture, extraction of patterns, comparison, verification and identification.
- 2.3. Applications of biometrics in private and public security: access control, video surveillance, investigation, identification of persons and protection of facilities.
- 2.4. Reliability of biometric systems: false positives, false negatives, accuracy in real-world environments and algorithmic bias.
- 2.5. Legal framework for biometrics: GDPR, special categories of data, proportionality, data minimisation, transparency and processing of data relating to criminal convictions and offences. Analysis of biometrics within the framework of the European Artificial Intelligence Regulation, with particular attention to remote biometric identification, prohibited or high-risk AI systems, human oversight, data quality, traceability and safeguards against automated decision-making.

Drones and unmanned aircraft systems applied to security, prevention and emergencies

3.1. Concept, evolution and typology of drones or UAS: recreational, commercial, governmental and public service uses.

3.2. Professional applications of drones in security: surveillance, perimeter control, infrastructure inspection, traffic monitoring, support for major events and protection of critical infrastructure.

3.3. Use of drones in emergencies and civil protection: forest fires, floods, natural disasters, search and rescue, damage assessment and operational coordination.

3.4. European regulatory framework on drones: Delegated Regulation (EU) 2019/945, Implementing Regulation (EU) 2019/947, open, specific and certified categories, and standard scenarios.

3.5. Technical and administrative requirements: CE marking, classes C0 to C6, direct remote identification, geolocation, operator registration, pilot training, insurance and maintenance.

Operational planning, risk assessment, privacy and practical cases

4.1. Planning of technological operations in security: definition of the mission, purpose, operational environment, technology used and foreseeable risks.

4.2. Coordination of drone operations in Spain: AESA, ENAIRE, ENAIRE Drones, PLANEA, controlled airspace, NOTAM, aerodromes and flight plan.

4.3. EASA and NO-EASA operations: police, customs, search and rescue, firefighting, border control, coastal surveillance and traffic monitoring activities.

4.4. Risk assessment and mitigation: operational concept, safety study, strategic, tactical and technical measures, people on the ground, manned aviation, critical infrastructure and urban environments.

4.5. Practical cases on the implementation of biometric systems, facial recognition, building inspection with drones, operations near airports, search and rescue, emergencies and analysis of the applicable legal safeguards.

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Individual study	86	3.44	
Continuous evaluation exercise I and II	20	0.8	
Evaluation	4	0.16	
Lectures	40	1.6	

Lengua de docencia: Español.

Llengua de docència: Espanyol.

Teaching language: Spanish.

Taking into account that the aim of achieving the learning objectives described in this Guide, we will develop a methodology that combines the individual study from the Manual, and the readings that will be presented in each topic, in addition of some documentaries.

Annotation: within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Assessment

Continuous assessment activities

Title	Weight	Hours	ECTS	Learning outcomes
Examination	30%	0	0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Continuous evaluation exercise 1 (Individual Work)	35%	0	0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Continuous evaluation test 2 (team Work)	35%	0	0	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

CONTINUOUS ASSESSMENT

There will be two individual PECs corresponding to the two topics studied in the course: biometric identification technology and drones.

Each PEC has a weight of 35% of the final grade of the course. The remaining 30% corresponds to the theoretical exam (open questions, case studies or multiple choice).

The exam averages with the continuous evaluation regardless of the grade obtained.

The total weighted average must be 5 points or higher in order to pass.

In order to be eligible for an honors degree it will be necessary to have obtained nine points or more in each of the tests (PECs and exam).

NOT EVALUABLE

A student who does not submit any of the PACS and who does not sit for the exam will have a final grade of "not evaluable".

SINGLE EVALUATION

Students who opt for the single evaluation will take a final synthesis test of all the content of the course (30%) and will hand in a document containing the solutions to the two PECs of the course (35% each).

The date for this test and the delivery of the work of the subject will be the same scheduled in the timetable for the last continuous evaluation exam.

The same recovery system will be applied as for the continuous evaluation.

EVALUATION OF THE STUDENTS IN SECOND OR MORE SUMMONS

Students who repeat the course will have to take the scheduled tests and exams and hand in the course work on the dates indicated in the Moodle classroom.

SECOND CHANCE EXAMINATION

The student who does not pass the course, who does not reach 5 (total) out of 10, according to the criteria established in the two previous sections may take a final exam provided that the student has been evaluated in a set of activities, the weight of which is equivalent to a minimum of two thirds of the total grade of the course. If the student has not been evaluated of these two thirds because he/she has not taken the tests, he/she will obtain a grade of Not Presented, without the possibility of taking the final exam.

In this exam the whole of the contents of the subject that have not been passed in the continuous evaluation will be re-evaluated.

In the case of passing the final exam, the course will be approved with a maximum of 5, regardless of the grade obtained in the exam.

CHANGE OF DATE OF A TEST OR EXAMINATION

Students who need to change an evaluation date must submit the request by filling out the document that can be found in the EPSI Tutoring Moodle space.

Once the document has been filled in, it must be sent to the professor of the subject and to the coordination of the Degree.

REVIEW

At the time of each evaluation activity, the faculty will inform the students of the grade review mechanisms.

For single evaluation students, the review process will be the same.

USE OF AI

In this course, the use of Artificial Intelligence (AI) technologies is permitted as an integral part of the work, provided that the final result reflects a significant contribution by the student in terms of analysis and personal reflection. Students must clearly identify which parts have been generated using this technology, specify the tools used, and include a critical reflection on how these have influenced the process and the final result of the activity. Failure to disclose the use of AI will be considered academic dishonesty and may result in a lower grade for the activity or more severe penalties in serious cases.

OTHER CONSIDERATIONS

Without prejudice to other disciplinary measures deemed appropriate, and in accordance with current academic regulations, "in the event that the student performs any irregularity that may lead to a significant variation in the grade of an act of evaluation, this act of evaluation will be graded with a 0, regardless of the disciplinary process that may be instigated. in the event that several irregularities occur in the acts of evaluation of the same subject, the final grade of this subject will be 0".

If there are unforeseen circumstances that prevent the normal development of the course, the teacher may modify both the methodology and the evaluation of the course.

Bibliography

Agencia Española de Protección de Datos. (2019). *Drones y protección de datos*. Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*. Agencia Española de Protección de Datos.

Agencia Estatal de Seguridad Aérea. (2024). *Actividades No EASA: Principales novedades introducidas por el Real Decreto 517/2024*. Ministerio de Transportes y Movilidad Sostenible.

Agencia Estatal de Seguridad Aérea. (s. f.). *Normativa de UAS/drones*. Ministerio de Transportes y Movilidad Sostenible.

Castellanos Ruiz, M. J. (2019). Régimen jurídico de los drones: El nuevo Reglamento (UE) 2018/1139. *Cuadernos de Derecho Transnacional*, 11(1), 171-234. <https://doi.org/10.20318/cdt.2019.4618>

Castellanos Ruiz, M. J. (2024). El impacto de la Ley de Inteligencia Artificial en la regulación europea sobre drones. *Cuadernos de Derecho Transnacional*, 16(2), 330-377. <https://doi.org/10.20318/cdt.2024.8915>

Comisión Europea. (2019). *Reglamento Delegado (UE) 2019/945 de la Comisión, de 12 de marzo de 2019, sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas*. Diario Oficial de la Unión Europea.

Comisión Europea. (2019). *Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, relativo a las normas y procedimientos aplicables a la utilización de aeronaves no tripuladas*. Diario Oficial de la Unión Europea.

Comisión Europea. (2024). *Reglamento Delegado (UE) 2024/1108 de la Comisión, de 13 de marzo de 2024, por el que se modifica el Reglamento (UE) n.º 748/2012 en lo que respecta a la aeronavegabilidad inicial de los sistemas de aeronaves no tripuladas sujetos a certificación y el Reglamento Delegado (UE) 2019/945 en lo que respecta a los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas*. Diario Oficial de la Unión Europea.

Comisión Europea. (2024). *Reglamento de Ejecución (UE) 2024/1110 de la Comisión, de 10 de abril de 2024, por el que se modifican el Reglamento (UE) n.º 748/2012 en lo que respecta a la aeronavegabilidad inicial de los sistemas de aeronaves no tripuladas sujetos a certificación y el Reglamento de Ejecución (UE) 2019/947 en lo que respecta a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas*. Diario Oficial de la Unión Europea.

Comité Europeo de Protección de Datos. (2023). *Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley (Versión 2.0)*. Comité Europeo de Protección de Datos.

Consejo de Europa. Comité Consultivo del Convenio 108. (2021). *Guidelines on facial recognition*. Council of Europe.

Cotino Hueso, L. (2023). Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos. En F. Balaguer Callejón & L. Cotino Hueso (Coords.), *Derecho público de la inteligencia artificial* (pp. 347-402). Fundación Manuel Giménez Abad.

España. Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. (2024). *Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas (UAS)*. Boletín Oficial del Estado.

European Union Agency for Fundamental Rights. (2019). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement*. Publications Office of the European Union.

European Union Aviation Safety Agency. (2024). *Easy Access Rules for Unmanned Aircraft Systems: Regulations (EU) 2019/947 and (EU) 2019/945*. European Union Aviation Safety Agency.

European Union Aviation Safety Agency. (2024). *Easy Access Rules for U-space: Regulation (EU) 2021/664*. European Union Aviation Safety Agency.

González Botija, F., & Zamora Santa Brígida, I. (2019). Drones y seguridad pública. *Cuadernos de Gobierno y Administración Pública*, 6(1), 57-70. <https://doi.org/10.5209/cgap.64618>

Izquierdo Carrasco, M. (2020). La utilización policial de los sistemas de reconocimiento facial automático. *IUS ET VERITAS*, 60, 86-103. <https://doi.org/10.18800/iusetveritas.202001.004>

Martínez Ramil, P. (2021). ¿Es el marco legal de derechos humanos de la UE capaz de hacer frente a la IA discriminatoria? *IDP. Revista de Internet, Derecho y Política*, 34, 1-14. <https://doi.org/10.7238/idp.v0i34.387481>

Ministerio de Transportes, Movilidad y Agenda Urbana. (2023). *Plan de Acción Nacional para el Despliegue del U-space 2022-2025* (versión 2.1). Gobierno de España.

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea.*

Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la Unión Europea.*

Pérez Esquivel, A. (2021). Desafíos de la videovigilancia automatizada. *Derecho y Ciencias Sociales*, 24, 100-122. <https://doi.org/10.24215/18522971e087>

Simón Castellano, P., & Dorado Ferrer, X. (2022). Límites y garantías constitucionales frente a la identificación biométrica. *IDP. Revista de Internet, Derecho y Política*, 35, 1-13. <https://doi.org/10.7238/idp.v0i35.392324>

Software

This subject will use the basic software of the Office 365 package

Course groups and languages

The information provided is provisional until November 30. After this date, you will be able to consult the language of each group through this [link](#). To access the information, you will need to enter the course CODE

Type of teaching	Group	Language	Semester	Shift
(TE) Theory	1	Spanish	second semester	afternoon