

Facial Recognition Through the Lens of National Legislations - Greece*

Konstantinos Kouroupis

(Associate Professor, Department of Law, Frederick University, Cyprus)

ABSTRACT This article explores the deployment and regulation of facial recognition technology (FRT) in Greece, with comparative references to Cyprus. It outlines the practical use of FRT in public security, law enforcement, and private institutions, highlighting controversial projects such as iBorderCtrl and enforcement actions like the Clearview AI fine. Despite the lack of a comprehensive national framework, the legal basis for FRT relies primarily on GDPR, Law 4624/2019, and Presidential Decree 75/2020. The study critically examines Greece's shortcomings in transparency, accountability, and data protection, emphasizing the urgent need for alignment with the EU's forthcoming Artificial Intelligence Act. The analysis demonstrates how the absence of clear legal safeguards raises concerns over fundamental rights, privacy, and democratic oversight.

KEYWORDS: Facial Recognition Technology - GDPR - Predictive Policing - Data Protection - Artificial Intelligence Act - Surveillance Law

TABLE OF CONTENTS: 1. Introduction. – 2.1. SECTION I. Deployments. – 2.2. SECTION II. Rule of Law. – 2.3. SECTION III. Perspectives for the Implementation of the AI Act. – 3. CYPRUS.

1. Introduction

Greece, a member of the European Union since 1981, operates under a civil law system significantly shaped by its constitutional traditions and European Union legislation. The Constitution of Greece, adopted in 1975 and subsequently amended, establishes the foundational legal framework for governance, human rights protection, and the rule of law. Key legal institutions include the Council of State, the Court of Cassation, and an independent judiciary, all of which play a crucial role in interpreting legislation, including matters involving privacy and surveillance.

The first section of this report presents an overview of the deployment of facial recognition technology in Greece, particularly within law enforcement, public surveillance, and border control contexts. Notable cases include the EU-funded “iBorderCtrl” project, which utilized facial and emotion recognition for pre-screening travelers at border checkpoints, and the acquisition of real-time FRT-enabled body-worn cameras by the Hellenic Police. These systems are intended to support predictive policing efforts and enhance crime prevention but have faced intense scrutiny from civil society and data protection authorities.

Another significant instance involved the Greek Data Protection Authority's (HDP) fine of

€20 million fine against Clearview AI, marking one of the strictest enforcements of the General Data Protection Regulation (GDPR) within the country. Similarly, the use of biometric access control systems at private institutions, such as the Vouliagmeni Nautical Club, was penalized due to the absence of lawful processing grounds and a failure to conduct a data protection impact assessment.

The second section examines the legal framework governing the use of FRT in Greece. While there is no dedicated national law specifically regulating facial recognition technology, several legislative instruments apply indirectly. These include the GDPR, national data protection Law 4624/2019, and Presidential Decree 75/2020, which governs the use of surveillance systems in public spaces by law enforcement authorities. The decree imposes conditions of necessity, proportionality, and judicial oversight for camera deployments but remains ambiguous about the use of AI-enhanced tools such as facial recognition. Several NGOs, including Homo Digitalis, have filed petitions to the HDPA accusing the Hellenic Police of breaching transparency obligations and operational safeguards under this decree.

The third and final section explores the anticipated impact of the EU's forthcoming Artificial Intelligence Act on facial recognition technology in Greece. While the country has taken steps toward formulating a national AI strategy - evidenced by the 2024 policy document “A Blueprint for Greece's AI

* Article submitted to double-blind peer review.

Transformation” - no comprehensive legal framework currently exists to regulate real-time facial recognition technologies. The strategy recognizes the potential of AI for public security applications but emphasizes that any deployment must adhere to fundamental rights and democratic values.

As the European Union moves toward a harmonized regulatory framework through the AI Act, Greece will be required to reassess and potentially revise its domestic policies and enforcement practices to ensure alignment with new EU standards, particularly those governing high-risk AI systems such as biometric surveillance. The implementation of the AI Act will be crucial in determining the scope and limits of FRT use in Greece, providing clearer legal safeguards and operational standards to protect individual rights.

Through this structured analysis, the report aims to provide a comprehensive overview of facial recognition technology's role in Greece while addressing the legal and ethical challenges posed by its deployment in both public and private sectors.

Cyprus, an EU member state since 2004, maintains a legal system rooted in common law traditions with increasing harmonization toward European Union standards. The Constitution of the Republic of Cyprus, adopted in 1960, serves as the supreme law, enshrining fundamental human rights and outlining the country's institutional architecture. The Cypriot legal framework includes an independent judiciary and strong protections for individual liberties, including the right to privacy and data protection.

The first section explores actual and proposed use cases of facial recognition technology in Cyprus. Although FRT has not been officially implemented by Cypriot law enforcement for general public surveillance, it is already in use in select areas. At Larnaca and Pafos airports, “BorderXpress” e-gates use FRT to verify travelers' identities by matching facial features to biometric passports. This system is operated jointly by Hermes Airports, the Cyprus Police, and the Ministry of Transport.

In addition, the Republic of Cyprus has announced plans to deploy advanced FRT at sports stadiums to curb violent incidents and identify troublemakers. This new system is capable of recognizing up to 80 facial features and aims to facilitate real-time identification

of individuals, even when partially obscured. Though not yet fully operational, the system is expected to be active by the end of the year and will be integrated with an upgraded fan card registry.

Furthermore, during the period 2021–2022, the Cyprus Police's Photographic and Graphic Laboratory acquired a facial recognition platform known as “ISIS Faces Fire,” as part of the EU-funded TELEFI project (Towards the European Level Exchange of Facial Images). While initially positioned as a tool for cross-border criminal investigations, this development indicates that Cyprus is quietly building the technical capacity to apply FRT beyond airport or stadium use.

The second section evaluates the current legal framework regulating facial recognition in Cyprus. Unlike many EU countries, Cyprus lacks a dedicated law or policy governing the use of facial recognition technology. While the Data Protection Law (Law 125(I)/2018) transposes the GDPR into national law and provides a general basis for processing biometric data, there is no explicit legal provision defining the permissible scope, storage duration, or safeguards for FRT deployment. According to available information from the TELEFI project, current Cypriot law permits storing facial images only of convicted persons. The inclusion of suspects in such databases would require future legislative amendments.

The absence of legal clarity raises serious concerns regarding transparency, oversight, and the proportionality of biometric surveillance. Although discussions have taken place within academic and civil society settings - including forums organized by the Cyprus National Bioethics Committee - no public consultations or institutional AI strategies have been formally adopted.

The third section addresses the implications of the forthcoming EU Artificial Intelligence Act on the use of FRT in Cyprus. As a high-risk category under the proposed regulation, real-time biometric identification systems will face strict requirements relating to transparency, necessity, proportionality, and fundamental rights impact assessments. Given that Cyprus currently lacks an overarching AI governance framework, the enforcement of the AI Act is expected to play a critical role in shaping future policy and regulatory measures in the country.

The eventual adoption and enforcement of

the AI Act will require Cyprus to establish clear and binding legal provisions for the use of facial recognition technologies - particularly those deployed by public authorities or for security purposes. This will also entail stronger oversight mechanisms, greater accountability for data controllers, and harmonization with EU standards on fundamental rights protections.

Through this structured analysis, the report provides a comprehensive overview of the current state and future trajectory of facial recognition technology in Cyprus, highlighting the urgent need for legal and institutional development in light of the emerging European AI regulatory landscape.

2.1. SECTION I. Deployments

Facial recognition technology (FRT) has increasingly been deployed in Greece despite the absence of a comprehensive EU legal framework prior to the adoption of the AI Act. Applications range from EU-funded initiatives like the *iBorderCtrl* project to law enforcement uses such as predictive policing and body-worn surveillance cameras. Private entities have also implemented FRT, prompting legal scrutiny from the Hellenic Data Protection Authority (HDPA), which has issued significant fines, including a €20 million penalty against Clearview AI for GDPR violations.

These developments have sparked public debate and concern over privacy, transparency, and potential rights violations. Nevertheless, Greek authorities continue to expand FRT use, with plans to install 1,000 biometric surveillance cameras in Athens and facial recognition systems across regional airports. As the EU moves toward stricter AI regulation, Greece's experience highlights the urgent need for clearer legal safeguards to ensure the technology is deployed in alignment with fundamental rights and democratic principles.

Even though there was no solid legal framework in European Union for the lawful use of facial recognition, before the adoption of the AI Act, there may be found several cases in which such methods have been put in place either by private or public entities in EU member states. According to a relative study conducted by the press media "Euractiv" in 2021, eleven EU member states already use

biometric identification tools.¹ In fact, law enforcement authorities in those 11 EU member states participating in the aforementioned study employ that technology in their criminal investigation but only for "post-identification", meaning that the material is examined after an incident, rather than in real time. However, this distinction has no relation to the impact of these technologies on fundamental rights.² According to the non-profit organization "Carnegie Endowment for International Peace", in a recent report published on 2019, AI surveillance technology knows a great expansion, accelerating at an incredible fast rate and surpassing experts' anticipations. At the time of the research, at least seventy-five out of 176 countries globally were actively using AI technologies for surveillance purposes. Facial recognition systems are deployed in sixty-four countries.³

Following this practice, Greece has deployed several systems. Special emphasis shall be given on a technology called "iBorderCtrl" which was implemented in the framework of a EU funded project started on 1 September 2016 and ended on 31 August 2019. It focused on land border crossing points: roads, walkways, and train stations. The main objective of iBorderCtrl was to enhance security and trust in border control checks and prevent illegal immigration. The project was executed in three countries: Greece, Hungary and Latvia and was operated through the following methodology: at first

¹ L. Bertuzzi, *Facial recognition technologies already used in 11 EU countries and counting, report says*, in *Euractiv*, 16 June 2021, available at: www.euractiv.com/section/tech/news/facial-recognition-technologies-already-used-in-11-eu-countries-and-counting-report-says.

² According to euractiv, at the time of the research, biometric identification technology is used by the police authorities in Austria, Finland, France, Germany, Latvia, Lithuania, Slovenia, the Netherlands, Hungary and Greece, while Cyprus, Croatia, the Czech Republic, Estonia, Romania, Portugal, Spain and Sweden are expected to follow and adopt such tools. See the entire post by L. Bertuzzi, *Facial recognition technologies already used in 11 EU countries and counting, report says*, in *Euractiv*, 26 October 2021, available at: www.euractiv.com/section/data-protection/news/facial-recognition-technologies-already-used-in-11-eu-countries-and-counting-report-says, last retrieved 9 December 2024.

³ See the whole report of the Carnegie Endowment for International Peace S. Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, available at: <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en>, last retrieved 9 December 2024.

stage, before arrival at the border, travellers were informed on their rights and travel procedures. At the second stage taking place at the actual border, individuals were asked questions about their countries of origin and circumstances of departure. The answers were then evaluated by an AI-based lie-detecting system on the basis of several criteria, such as the frequency of eye blinking, the sound voice, a possible trembling and other biometric criteria. At the end of the process, travellers were classified in two categories: those who have been flagged as low risk during the pre-screening stage and would go through a short re-evaluation of their information for entry and those belonged in higher-risk level who would undergo a more detailed check.⁴

However, the implementation of the above technology was severely criticized not only from individuals and private entities but also from institutional bodies and human rights' protection organizations. Psychologists strongly contested the credibility of an AI-based lie-detecting system claiming that emotional or facial expressions may not lead to safe conclusions about an individual's personality.⁵ In addition, according to the well-known association of civil and human rights named "European Digital Rights" (EDRi) such pilot projects may seriously harm privacy and fundamental rights, since there are posed crucial questions regarding potential discriminatory applications of facial or emotional recognition technologies and the lawfulness of an automated individual decision-making, including profiling, according to the relative article 22 of the General Data Protection Regulation.⁶

⁴ See a detailed presentation of the project in the official report of the European Union, "iBorderCtrl Project," available at: <https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders>, published 24 October 2018, last retrieved 9 December 2024; see also iBorderCtrl official site, available at: www.iborderctrl.eu/iborderctrl-project-the-quest-of-expediting-border-crossing-processes.html, last retrieved 9 December 2024.

⁵ L.F. Barrett *et al.*, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, in *Psychological Science in the Public Interest*, 17 July 2019, <https://doi.org/10.1177/1529100619832930>, last retrieved 9 December 2024.

⁶ See a relative commentary of the "iBorderCtrl" by EDRi, *Immigration, iris-scanning and iBorderCTRL*, 26 February 2020, available at: <https://edri.org/our-work/immigration-iris-scanning-and-iborderctrl>, last retrieved 9 December 2024.

Moreover, the European Data Protection Supervisor, in his Opinion n.44/2023 desired to draw attention to the use of AI systems encompassing facial recognition tools due to their impact on human rights. On the occasion of the application of the iBorderCtrl the European Data Protection Supervisor underlined that "these AI systems should be properly regulated, including via express prohibition, in case of unacceptable risks, already at the design and development stages".⁷

The second case identified concerned Clearvi AI. Undoubtedly, special emphasis should be given on the imposition of fine on Clearview AI, Inc by the Hellenic Data Protection Authority. In fact, on 13 July 2022, following a complaint filed by Homo Digitalis in May 2021, the Hellenic Data Protection Authority (HDPA) issued Decision 35/2022 imposing a fine of 20 million euros on Clearview AI for its intrusive practices. This is the highest GDPR fine, ever imposed by the Hellenic DPA. By the same Decision, the DPA prohibits that company from collecting and processing the personal data of data subjects located in Greece using facial recognition methods and requires it to delete immediately any data it has already collected. It should also be noted that earlier on the same year, the Italian Data Protection Authority had decided to fine the company €20 million, while the UK's equivalent authority had decided to fine it £7.5 million.

In particular, the Hellenic Authority found that in this case the company, which markets facial recognition services, violated the principles of lawfulness and transparency (art. 5 paragraphs 1(a), 6, 9 GDPR) and its obligations under Articles 12, 14, 15 and 27 of the GDPR, imposing a fine of twenty million euros (20 000 000). In addition, the Authority issued a compliance order to the same company so that the latter satisfies the complainant's request for access to personal data, while imposing on the same company a prohibition on the collection and processing of personal data of subjects located in the Greek territory, using methods included in the facial recognition service. Finally, with this Decision, the Authority sent Clearview AI Inc.

⁷ See European Data Protection Supervisor, Opinion 44/2023 on the Proposal for Artificial Intelligence Act, published 23 October 2023, available at: www.edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinio_n_en.pdf, last retrieved 9 December 2024.

an order to delete the personal data of those subjects located in Greece, which the defendant collects and processes using those methods.⁸

Recently, especially during the period after the pandemic due to Covid19,⁹ facial recognition technology has been widely used by the police authorities in the context of the so called “predictive policing”.¹⁰ The

mentioned method is thoroughly applied in order to extract automated conclusions in real-time about the future likelihood of a crime being committed, based on body posture, movements, facial micro-expressions, and even the tone or pitch of a person's voice, depending on the intended purpose of the analysis, e.g., in relation to the probabilities of an individual committing a crime while standing outside a bank.¹¹

In that context, the Hellenic Police purchased body-worn cameras which aim to identify in real time criminal acts. Therefore, based upon the Greek Presidential Decree 75/2020,¹² there have been issued many announcements from the Hellenic Police Authorities for the use of such systems during operational planning.¹³ In an annual report of the Hellenic Data Protection Authority on 2020 it is explicitly mentioned the following:¹⁴

“The Authority became aware, both from media coverage and the official website of the Hellenic Police, that on 6/12/2020, as part of the Attica General Police Directorate operational planning, a portable surveillance system was installed and operated in areas of the Athens city centre following a decision made by the Hellenic Police Headquarters, in accordance with the provisions of presidential decree 75/2020. The Authority contacted ex officio the Ministry of Citizen Protection/Hellenic Police Headquarters on issues related to compliance with the current

⁸ Hellenic Data Protection Authority, Decision 35/2022, available at: www.dpa.gr/sites/default/files/2022-08/35_2022%20anonym_EN_FINAL.pdf, last retrieved 9 December 2024; A. Broumas and P. Charalampakis, *Greek DPA imposes 20M euro fine on Clearview AI for unlawful processing of personal data*, in *International Association of Privacy Professionals*, 20 October 2022, available at: <https://iapp.org/news/a/greek-dpa-imposes-20m-euro-fine-on-clearview-ai-for-unlawful-processing-of-personal-data>, last retrieved 9 December 2024; European Data Protection Board, *Hellenic DPA fines Clearview AI 20 million euros*, 20 July 2022, available at: www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en, last retrieved 9 December 2024.

⁹ It should also be mentioned that during the Covid19 pandemic many local authorities purchased biometric facial recognition systems as well as temperature detection machines in order to prevent the expansion of the pandemic. All relative contracts are published on the official site Greek Ministry of Digital Governance, “Diavgeia,” available at: <https://diavgeia.gov.gr/search?query=q:%22CF%84%CE%B5%CF%81%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AC%20%CE%B2%CE%B9%CE%BF%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%AE%CF%82%20%CE%B1%CE%BD%CE%B1%CE%B3%CE%BD%CF%8E%CF%81%CE%B9%CF%83%CE%B7%CF%82%20%CF%80%CF%81%CE%BF%CF%83%CF%8E%CF%80%CE%BF%CF%85%20%CE%BA%CE%B1%CE%B9%20%CE%B1%CE%BD%CE%AF%CF%87%CE%BD%CE%B5%CF%85%CF%83%CE%B7%CF%82%20%CE%B8%CE%B5%CF%81%CE%BC%CE%BF%CE%BA%CF%81%CE%B1%CF%83%CE%AF%CE%B1%CF%82%22&page=0>, last accessed on 9 December 2024.

¹⁰ Predictive policing refers to the use of systems and software, particularly through algorithmic processing of personal data, which can reveal patterns of potential future criminal activity and victimization. It concerns situations where no crime has yet been committed; however, in the context of either prevention to deter it or proactive data collection that will facilitate future investigation, this type of policing is activated.

The methods are divided into four (4) main categories: a) Prediction of crimes or locations and times of criminal activity with increased likelihood of occurrence, b) Prediction of offenders or identification of individuals likely to commit crimes or reoffend based on their past, c) Prediction of characteristics or creation of profiles of offenders, and finally, d) Prediction of victims. See a detailed presentation of the predictive policing in S. Gless, *Predictive Policing – In Defense of ‘True Positives*, available at: <https://jstor.org/stable/j.ctvhrd092.14>; L. Kanellos, *Applications of Artificial Intelligence in Law and Judicial Practice* (in Greek), Athens, Nomiki Bibliothiki, 2021, 228. As far as the process of personal data taking place during the use of

such method see European Parliament, *Artificial Intelligence and Law Enforcement – Impact on Fundamental Rights*, Study requested by the LIBE Committee, July 2020, available at: [www.europarl.europa.eu/thinktank/en/document.html?reference=2020/2016\(INI\)](http://www.europarl.europa.eu/thinktank/en/document.html?reference=2020/2016(INI)).

¹¹ See an intense analysis regarding the lawfulness of surveillance systems in G.V. Tsolias, *The recognition and identification of individuals for the purposes of prosecuting crime in accordance with Presidential Decree 75/2020 and the proposed EU Regulation on Artificial Intelligence* (in Greek), in *Nova Criminalia*, vol. 14, 7-8.

¹² The Presidential Decree No. 75/2020 will be thoroughly analyzed in the section of the presentation of legal basis of face surveillance systems.

¹³ See a full list of announcements from the Hellenic Police regarding the use of portable surveillance system here: Hellenic Police, *Dash Cameras*, available at: www.astynomia.gr/s/dash+camera, last retrieved 9 December 2024.

¹⁴ See the full text of the report in Hellenic Data Protection Authority, *Summary Report 2020*, available at: www.dpa.gr/sites/default/files/2022-06/Summary%202020.pdf, last retrieved 9 December 2024.

legal framework.

In particular, the Authority requested information on whether a data protection impact assessment had been carried out in this specific case of a portable surveillance system and, if so, it requested that the DPIA be submitted. Furthermore, it also requested a copy of the decision made by the Hellenic Police Headquarters, and to receive more detailed information about how data subjects are informed, especially as far as their rights are concerned under the applicable provisions of Regulation (EU) 2016/679 and Law 4624/2019 (as specified further, in this case, in Article 10 of p.d. 75/2020). Finally, the Authority also requested information about the advisory role of the Hellenic Police Data Protection Officer. The Authority is pursuing the investigation of this case¹⁵.

Finally, recently the Hellenic Data Protection Authority imposed an administrative fine of €56,000 on the Vouliagmeni Nautical Club for a series of violations of the GDPR due to the installation and operation of a biometric identification system using facial recognition technology for its members' access to its facilities. The Authority received an inquiry from a data subject (an accompanying member) regarding the lawfulness of the processing of their biometric data. According to the relevant message, the processing of biometric data was unconditionally required in order to access to the Nautical Club facilities, instead of the accompanying member card which was required at the past. The Authority found that the Group, as the data controller, processed personal biometric data in a controlled access system to its facilities, violating the principle of lawfulness (Article 5(1)(a) of the GDPR) and the obligation to conduct an impact assessment of the processing activities related to this system (Article 35 of the GDPR). It imposed a fine of €28,000 and €14,000 respectively, as well as the obligation to cease the processing of personal data through the system until an impact assessment is conducted and submitted to the Authority. The Authority also found that the Group violated Article 38(3) of the GDPR and imposed a fine of €14,000.¹⁵

¹⁵ Hellenic Data Protection Authority, *Self-Assessment and Submission of Complaints Regarding the Legality of*, available at: www.dpa.gr/el/enimerwtiko/prakseis/Arxis/aytepaggelti-exetasi-kai-ypoboli-kataggelion-gia

Despite its limited application, facial recognition technology has been tested both by public and private entities while it has been deployed at institutional level, as exposed in the case of the “iBorderCtrl”. In addition, in all cases either such methods have been severely criticized or banned by the Hellenic Data Protection Authority due to their harm to fundamental rights and freedoms.

However, a large public debate regarding the use of the aforementioned technology has already been launched and particularly documented by human rights' protection associations, such as the Non-Governmental Organization named “Homo Digitalis”, focused on the safeguard of digital rights.¹⁶ Therefore, the Greek Police is proceeding with the adoption of an advanced facial recognition system using biometric data. This system is expected to be connected to 1,000 new cameras that will be installed on central avenues in Athens and surrounding areas. These cameras will not only record speeding violations or whether vehicles enter bus lanes but will also be capable of detecting various very dangerous offenses.¹⁷

For example, they would detect whether the driver or other passengers are wearing seat belts, if the driver is speaking on the phone while driving, or if motorcyclists are wearing helmets. Those who violate the law will receive a ticket, which will be sent to their mobile phone via text message or through Viber.

This system will also assist in the broader surveillance of public spaces, as is the case in several European capitals, and will rely on the identification of individuals through biometric characteristics.

The Hellenic Police will enhance the camera software system with thousands of photographs of individuals wanted for criminal activities, incitement to incidents, or other offenses that threaten public safety, in order to facilitate easy identification.

-ti-nomimotita-tis (in Greek), last retrieved 9 December 2024.

¹⁶ Homo Digitalis, *Campaign to Cease Facial Recognition Technology*, available at: <https://homodigitalis.gr/en/?s=ban+facial+recognition>, last retrieved 9 December 2024.

¹⁷ See the whole provisioned project in the article written by C.P. Papadiochos and S. Papanioniou, *Smart road safety system across Attica, Kathimerini*, available at: www.ekathimerini.com/news/1249071/smart-road-safety-system-across-attica/, last retrieved 9 December 2024.

However, a critical point in the entire process mentioned above is obtaining approval from the Hellenic Data Protection Authority, as the use of such a powerful surveillance system raises serious concerns regarding the protection of citizens' privacy and personal data.¹⁸

Finally, plans for permanent deployments of facial recognition technology have been drafted to be established across all terminals in airports. In particular, air transport company Fraport AG which operates 14 regional airports in Greece, announced that facial recognition systems are ready to be installed across all terminals. Frankfurt airport has already installed them enabling travellers to pass through each stage of the airport journey - from check-in, through to security and boarding - by simply scanning their face.¹⁹

2.2. SECTION II. Rule of Law

In Greece the Presidential Decree 75/2020 constitutes the legal instrument regulating the use of surveillance systems in public spaces.²⁰ It has been published on 10 September 2020 and has been issued following the article 14 of Law 3917/2011. Adopting a broad concept of the term “surveillance systems” the P.D. 75/2020 applies in all surveillance systems installed in public spaces, to the extent that they process personal data.

The installation and operation of surveillance systems in public spaces is permitted only by state authorities (article 14 par. 2 Law 3917/2011). These public authorities can be in particular the Hellenic Police, the Fire Brigade and the Coast Guard – Hellenic Coast Guard (article 4 PD 75/2020). The operation of surveillance systems in

public spaces is permitted only for specific purposes mentioned in article 14 of Law 3917/2011 and article 3 of this Presidential Decree (national defense, public security - suppression of specific crimes mentioned in the Greek Penal Code, and traffic management). Principles of necessity and proportionality shall be respected any time of use of such methods.

The installation and operation of surveillance systems in public spaces is permitted only for: a) the prevention and suppression of specific criminal acts, such as violent crimes, drug trafficking, etc., b) traffic management, the regulation of vehicle traffic, as well as the prevention and management of road accidents (article 14 par. 1 Law 3917/2011 and article 3 PD 75/2020).

The installation and operation of surveillance systems in public spaces is permitted only to the extent necessary and when the above-mentioned objectives cannot be achieved as effectively by lesser means. Especially regarding the installation and operation of surveillance systems for the prevention or suppression of crimes, are sufficient indications are required that the specifically provided for offenses are committed or will be committed in the specific space (article 5 par. 1 PD 75/2020). Regarding portable surveillance systems, it is provided that their operation is permitted only in cases where there is an imminent serious risk that the specifically provided for offenses will be committed (article 5 par. 3 PD 75/2020).

Such sufficient evidence is justified by the factual circumstances such as, “*in particular, statistical or empirical data, studies, reports, testimonies and information on the frequency, type and specific characteristics of the crimes committed in a particular area and information on the possibility of spread or transfer of the criminal acts to another public space*”. In addition, following the same article in the second paragraph, surveillance is deemed necessary when a reasonable belief is established that there are serious public safety hazards in the specific area. Therefore, the surveillance cannot be extended in a wider area.

In addition, the Presidential Decree regulates some specific circumstances concerning the operation of surveillance systems of public spaces, which are as follows:

¹⁸ *Ibid.*

¹⁹ See more details in the article written by L. Arena, *Frankfurt airport rolls out facial recognition across all terminals*, Business Travel News Europe, 27 October 2023, available at: www.businesstravelnewseurope.com/Air-Travel/Frankfurt-airport-rolls-out-facial-recognition-across-all-terminals, last retrieved 9 December 2024. In addition see GTP Editing Team, *Frankfurt Airport First in Europe to Offer Full-coverage Biometric Systems*, available at: <https://news.gtp.gr/2023/10/27/frankfurt-airport-first-in-europe-to-offer-full-coverage-biometric-systems/>, last retrieved 9 December 2024.

²⁰ See the full text of the Presidential Decree Greek Government, *Presidential Decree 75/2020*, available at: www.kodiko.gr/nomothesia/document/638933/p.d.-75-2020, last retrieved 9 December 2024.

The operation of portable surveillance systems is allowed only in cases where there is an immediate and serious risk of commission of the crimes referred to in article 3 of the Presidential Decree; Zoom functionality of surveillance systems is permitted only for the identification of crimes and under specific circumstances. The approval of the competent prosecutor is necessary for the legitimate operation of cameras with zoom functionality.

According to the article 6, on public gatherings, cameras may be used upon approval of the competent prosecutor and notification of the entity that organizes such gathering. Such operation is legitimate only when it keeps up with the specific purposes mentioned hereabove and under the condition that the cameras do not focus on people.

Furthermore, the Decree provides for a general prohibition of the processing of audio data in so far as it contains identifiable data. Exceptionally, audio data may be processed upon reasonable decision of the data controller for the sole purpose of identifying persons involved in criminal acts, the investigation of which is impossible or substantially difficult without the processing of audio data. Such decision explicitly mentions the specific circumstances that justify the collection of audio data and is submitted for approval before the competent prosecutor. At this stage, it is highlighted that the Hellenic Data Protection Authority has already mentioned in its Opinion 3/2020 on the use of CCTV and audio recording in public spaces the issues of compatibility that arise between this provision and the constitutional right of privacy of communication.

Regarding the retention period of data collected using surveillance systems, according to the provisions of Article 8, paragraph 2 of Presidential Decree 75/2020, the collection and retention of personal data (image or sound) of individuals entering the surveillance systems' field of capture is stipulated, with the data being retained in three (3) cases:

i) for fifteen (15) days and then automatically deleted unless they are suspected of committing the crimes specified in Article 3, paragraph a of the Presidential Decree,

ii) until the irrevocable acquittal or conviction of those who have been designated as suspects and subsequently charged for the

same crimes, and

iii) those who, while not falling into either of the previous two (2) categories, gather justified suspicions of future preparation or commission of the same crimes, based on the delimitation criteria provided in the same provision.

Citizens enjoy all the rights provided for by the General Data Protection Regulation, known as GDPR, and implementing Law 4624/2019 (article 10 paragraph 1 of the P.D. 75/2020), depending on which individual regulations are applicable. In any case, there is an obligation to inform the public that it is going to enter a space in the range of installed or portable surveillance systems, especially by conspicuously placed signs (article 10 paragraph 2 of the P.D. 75/2020).

Consequently, the Presidential Decree 75/2020 may regulate at a large scale the use of surveillance systems in public places but not those which encompass AI tools. Despite the absence of an explicit provision for the installation and operation of Artificial Intelligence systems, the wording of Article 2 of the Presidential Decree, referring to "additional equipment for the transmission, storage, and any further processing of image and sound", could be interpreted as including them.

Even though the Presidential Decree contains specific requirements for the legitimate deployment of portable surveillance camera, Greek police authorities are many times accused of breaching the legislation. As such, the Greek Non-Governmental Organization named "Homo Digitalis" in collaboration with the private entities Reporters United and the Press Project, addressed a petition before the President of the Hellenic Data Protection Authority (No. Prot. G/EIS/3129/12-05-2021), in which at least sixty-four (64) violations of the provisions of the legislation concerning the use of portable cameras in public places are complained of by the Hellenic Police (Hellenic Police). At the same time, the organizations are requesting that the Hellenic authority exercise its investigative, corrective and advisory powers on this important issue.

In particular, in accordance with the provisions of Article 12 paragraph 2 of the Decree 75/2020, the Hellenic Police, as the controller, must each time before the operation of a surveillance system in a public place, issue and notify the decision to operate

this system at least on its website, specifying obligatorily: a) the time of activation, b) the duration of its operation, c) the range of its operation, d) its specific characteristics, and e) the justification of the feasibility of its use.

However, the Hellenic Police has not complied with the obligation to publish on its website the decisions to operate the surveillance systems it uses in public places. On the contrary, in breach of its statutory obligations, the Hellenic Police Service has consistently confined itself to publishing a simple notice on its website, which indicates only the number of each operating decision, the duration of operation of the surveillance systems and their place of operation in a general and vague manner.²¹

At the same time, Amnesty International²² claimed that Greek authorities have seriously violated specific provisions of the Presidential Decree 75/2020 regarding the use of surveillance systems during the period of Covid19 pandemic. In particular, one of the crucial issues was the lawfulness of the 2021's National Plan on the management of assemblies (Guidelines) which enabled the use of body worn or hand-held cameras and drones for the effective management of demonstrations and other purposes. As analyzed above, the legal basis for the adoption of those Guidelines was the Presidential Decree 75/2020 which, according to Homo Digitalis, was adopted without any type of public consultation with civil society.

In our case, the use of such methods could violate the fundamental right of freedom of assembly as this practice could be intimidating to peaceful protestors and, therefore, prevent them from exercising their right. Homo Digitalis's criticism of the Hellenic Police's practices concerning the use of facial recognition technologies is both timely and justified, particularly in light of the recurring and well-documented regulatory violations. Despite the clear procedural requirements set forth in Presidential Decree 75/2020 - such as the obligation to publish detailed operational decisions, conduct data protection impact

assessments, and obtain prosecutorial approval - the Hellenic Police have repeatedly bypassed or inadequately fulfilled these legal duties. The consistent failure to provide transparent justifications and specific operational details not only undermines legal accountability but also erodes public trust in law enforcement. Homo Digitalis, by bringing forward evidence of at least 64 violations and collaborating with investigative journalism networks, has highlighted the institutional opacity and systemic disregard for citizens' data protection and fundamental rights. Their actions serve as a crucial check against the normalization of opaque and potentially discriminatory surveillance practices. In a democratic society, the deployment of facial recognition systems - particularly in public spaces - demands the highest levels of transparency, legal oversight, and public consultation, all of which appear to have been significantly lacking. Thus, Homo Digitalis's advocacy not only defends constitutional and GDPR-based protections but also reinforces the broader democratic imperative of ensuring that high-risk technologies are deployed with due regard for legality, proportionality, and human dignity.

Amnesty International also claimed that there was lack of transparency as well as principles of necessity and proportionality since, according to the authors of the report, there were not any concrete indications that serious criminal offenses are actually taking place.²³

Despite the aforementioned allegations for infringement of the national regulatory framework, the competent authorities (neither the Hellenic Data Protection Authority nor the Hellenic Police) did not give any official stance.²⁴ In addition, contrary to what was expected, the petitions of the non-governmental organizations were not investigated. Indicatively, according to a press release published by Homo Digitalis, The Press Project and Reporters United, the cases for which accountability and transparency are requested from the Hellenic Police have

²¹ See more details regarding the petition of the non-governmental organization in Homo Digitalis, *Petition*, available at: <https://homodigitalis.gr/en/posts/10376/>, last retrieved 9 December 2024.

²² Amnesty International is an international non-governmental organization focused on human rights. See Amnesty International, *About Us*, available at: www.amnesty.org/en/about-us, last retrieved 9 December 2024.

²³ See the full report of Amnesty International, *Greece: Freedom of assembly at risk and unlawful use of force in the era of COVID-19*, 14 July 2021, available at: www.amnesty.org/en/documents/eur25/4399/2021/en, last retrieved 9 December 2024.

²⁴ This is not the case of the fine imposed on the Vouliagmeni Nautical Club nor on ClearViewAI by the Hellenic Data Protection Authority, as it has been widely exposed through the first section.

reached 64 in a period of seven months from 2020 to 2021. This number corresponds to the cases in which the Hellenic Police “informed” on the use of portable means of surveillance and audio and video recording, in its official website. Despite the concrete requirements declared by the Presidential Decree 75/2020 regarding the duties of the data controller (article 12 paragraph 2), the Hellenic Police issued formal announcements, which only mention the number of each operational decision, the duration of the surveillance systems' operation and the location of their operation in a general and vague manner. Thus, references to the operational range, justification as well as specific aspects of the surveillance procedure are absent, raising serious questions about whether the legislation is being adhered to. Thus, it is strongly claimed that the Hellenic Police has violated it at least 64 times.²⁵

2.3. SECTION III. Perspectives for the Implementation of the AI Act

At the time of the research, on November 25, 2024, the Prime Minister's High-Level Advisory Committee on Artificial Intelligence, in coordination with the Special Secretariat of Foresight, published a national policy proposal on how Greece could leverage artificial intelligence (AI) entitled “A Blueprint for Greece's AI transformation”.²⁶ The document aims to foster the development of Greece's economy and society while safeguarding against the risks posed by the unregulated use of AI. The study investigates the rapid advancements in AI and the unique opportunities they create to transform various aspects of human activity.

The AI national policy is focused on four key areas: a) innovation and entrepreneurship, b) education and research, c) regulatory frameworks and d) AI applications in Government.

²⁵ See more details on the issue in the article published by T. Kamilalis, *Drone and Hellenic Police: claims about the continuous infringement of legislation during the use of portable cameras* (in Greek), 14 May 2021, available at: <https://thepressproject.gr/ena-drone-pano-apo-tin-el-as-anafora-gia-systimatikes-paravaseis-sti-ch-risi-foriton-kameron/>, last retrieved 9 December 2024.

²⁶ See a detailed presentation of the Greek national AI policy proposal in *Greek National AI Policy Proposal*, available at: <https://legacy.dataguidance.com/news/greece-government-publishes-national-ai-policy-proposal>, last retrieved 9 December 2024.

Following this classification there is a provision for the use in real-time of surveillance cameras, sensors and social media in order to prevent criminal acts. Certainly, principles of law, necessity and proportionality as well as all constitutional guarantees should be respected. However, it seems that there are not any plans or projects at institutional level aiming to integrate facial recognition into public surveillance systems.

Finally, in the framework of drafting the national AI policy, it should also be highlighted the establishment of a High-Level Advisory Committee on Artificial Intelligence (AI)²⁷ under the Prime Minister, which is coordinated by the Special Secretariat of Foresight. The Committee will formulate policy recommendations and outline guidelines for the long-term planning of a national strategy for IT, focusing on crucial areas, such as those described above.

Concluding, Greece has actively deployed facial recognition technologies, particularly in law enforcement, often without full compliance with legal safeguards. Despite existing regulations, oversight has been weak and frequently criticized by civil society. While a national AI strategy has been proposed, it lacks concrete measures for FRT governance. The gap between policy and practice remains significant. As the EU AI Act approaches enforcement, Greece must urgently align its framework to protect fundamental rights.

3. CYPRUS

Contrary to the Greek reality, in Cyprus facial recognition surveillance systems have never been deployed, at least at an official level. In addition, at the time of the research, Cyprus has not yet published a concrete and complete AI policy, as other EU member states have done. Moreover, there is not – at the moment- a legal basis for a potential use of facial recognition technology.

However, a large social debate has been launched regarding the new challenges, opportunities and risks caused by the expansion of artificial intelligence while academic institutions, national independent

²⁷ See the official announcement of the establishment of the High Level Advisory Committee on AI in Greece in *High Level Advisory Committee on AI in Greece*, available at: <https://foresight.gov.gr/en/studies/A-Blueprint-for-Greece-s-AI-Transformation>, last retrieved 9 December 2024.

committees (such as the Cyprus National Bioethics Committee) and non-governmental organizations have organized special fora and conferences on the issue.²⁸

Notwithstanding the current standby status, we may make special remarks on the following issues:

At Larnaca and Pafos airports facial recognition technology is used through e-gates and border control. In particular, as it is explicitly declared,²⁹ Hermes Airports – the company which manages the Larnaca and Pafos airports- together with the Cyprus Police and the Ministry of Transport, Communications and Works, have introduced the operation of the “BorderXpress” interactive kiosks at Larnaca and Pafos airports.

Through this high-level technology, either on departure or arrival in Cyprus, passengers may be in the position to independently scan their identity card or passport as an intermediate step of the passport control procedure. When approaching an automatic gate and placing the open passport into the scanner, the gates use facial recognition technology to compare the face to the photograph recorded on the chip in passenger’s passport. A receipt will be issued which should be presented at a predefined check point. If the check is successful, the procedure of passport control has been implemented successfully. If not, passengers will need to go to a control gate operated by an Immigration Officer.

The Republic of Cyprus plans to deploy advanced facial recognition technology to help prevent disturbances at sports stadiums.³⁰

²⁸ Indicatively, The National Commission for Bioethics and Technoethics (NCBT) of Greece and the Cyprus National Bioethics Committee (CNBC) have decided to jointly issue an Opinion on the emerging and critical issue of “predictive analytics” in the field of Health. The Opinion is available in English National Commission for Bioethics and Technoethics (NCBT) and Cyprus National Bioethics Committee (CNBC), *Joint Opinion on Predictive Analytics in Health*, available at: https://bioethics.gr/api/files/download/2387/Joint%20Opinion_CNBC%20and%20NCBTG_Ethics%20of%20Predictive%20Analytics%20in%20Health_31%2010%202024.pdf?attachment=false, published 31 October 2024.

²⁹ See the official announcement by Hermes Airports, *E-Gates and Boarding Pass Readers*, available at: www.hermesairports.com/prepare-your-journey/flyout/e-gates-boarding-pass-readers, last retrieved 9 December 2024.

³⁰ See a relative press announcement entitled *Cyprus buys new facial recognition tech to curb stadium violence*, in *In-Cyprus*, 8 August 2024, available at:

The new software, which can identify individuals even when partially obscured, is expected to be operational by Christmas. According to Giorgos Karas, Chairman of the Stadium Licensing Authority, the system is capable of recognizing up to 80 facial features and matching them with a central database within minutes.

The goal of this technology is to facilitate quick arrests of troublemakers: it intends to enable police to apprehend individuals before they leave the stadium, as it can identify faces within three to five minutes. The new system will be integrated with an updated fan card system. Stadium security personnel will manage the software and coordinate with the police.

Even though facial recognition has never been deployed not implemented officially by Cyprus police authorities, the Photographic and Graphic Laboratory of Criminalistic Services responsible for the implementation of that technology has acquired a F.R (Facial Recognition) system (ISIS Faces Fire from Unidas). This project took place during 2021-2022.

That information is extracted throughout a project named “TELEFI” (Towards the European Level Exchange of Facial Images) which was funded by the European Union’s Internal Security Fund-Police and was implemented on 2021.

In its official report it is explicitly mentioned that, according to Cypriot legislation, only the database storage of facial images for convicted persons is permissible. In the future, when an amendment to the law has been adopted, the images of unconvicted suspects will also be stored.³¹

Therefore, it is concluded that facial recognition technology has been deployed, even in pilot form. However, serious concerns may be raised regarding the lawfulness of such method since there is not a clear legal provision on the period of storage of such data.

<https://in-cyprus.philenews.com/local/cyprus-buys-new-facial-recognition-tech-to-curb-stadium-violence>, last retrieved 9 December 2024.

³¹ See the full report of TELEFI project, *Summary Report*, available at: www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf, published January 2021.

