laws

MDPI

Article

Reconciling Remote Sensing Technologies with Personal Data and Privacy Protection in the European Union: Recent Developments in Greek Legislation and Application Perspectives in Environmental Law

Maria Maniadaki [1,*], Athanasios Papathanasopoulos [1], Lilian Mitrou [2] and Efpraxia-Aithra Maria [1]

[1] School of Environmental Engineering, Technical University of Crete, 73100 Chania, Greece; apapathanasopoul@isc.tuc.gr (A.P.); emaria@isc.tuc.gr (E.-A.M.)
[2] Department of Information and Communication Systems Engineering, University of the Aegean-Greece, 81100 Mitilini, Greece; L.Mitrou@aegean.gr
* Correspondence: mmaniadaki@isc.tuc.gr

Abstract: Using remote sensing technologies to ensure environmental protection responds to the need of protection of a right and a public good and interest. However, the increasing introduction of these technologies has raised new challenges, such as their interference with the rights of privacy and personal data, which are also protected fundamental rights. In this paper the importance of remote sensing technologies as tools for environmental monitoring and environmental law enforcement is analyzed, while legal issues regarding privacy and data protection from their use for environmental purposes are presented. Existing legislation for reconciling emerging conflicts is also examined and major European Court of Human Rights (ECtHR) and Court of Justice of the European Union (CJEU) case law on the issue is approached. Finally, recent developments in Greek legislation and their application perspectives in environmental law are presented as a timely "case study".

Keywords: Remote Sensing; personal data; privacy; drones; UAV; satellites; environmental monitoring; environmental law

Citation: Maniadaki, Maria, Athanasios Papathanasopoulos, Lilian Mitrou, and Efpraxia-Aithra Maria. 2021. Reconciling Remote Sensing Technologies with Personal Data and Privacy Protection in the European Union: Recent Developments in Greek Legislation and Application Perspectives in Environmental Law. *Laws* 10: 33. https://doi.org/10.3390/laws10020033

Received: 7 March 2021
Accepted: 7 May 2021
Published: 11 May 2021

1. Introduction

The development of remote sensing technologies, has led to numerous applications in several sectors. Remote sensing "provides tools for gathering data and solving real world problems[1]". Especially in the field of environmental monitoring, the development of remote sensing technologies has been proven more than crucial, as it enables the collection of a wealth of data for Earth's current and future state, affecting directly the decision making process as well as the environmental law enforcement sector (Mertikas et al. 2021). However, the transformation of collected data into useful information in the scope of environmental law, raises new challenges, such as their interference with the rights of privacy and personal data (Coffer 2020; Santos and Rapp 2019; Finn and Wright 2016; Sandbrook 2015; Doldirina 2014; Purdy 2011). Although it has become common knowledge that environmental problems have a global impact, calling thus for global action, nations still have their own role in legislation and regulation. In this sense, embracing new technologies such as remote sensing technologies in the case of Greece responds not only to Article 37 of EU Charter of Fundamental Rights[2] but also to the need of protection of a—in Greece constitutionally anchored—right and a public good and interest for environmental protection (Article 24 of the Greek Constitution). At the same time, key questions arise: is

[1] Available online: http://gsp.humboldt.edu/OLM/Courses/GSP_216_Online/lesson8-2/future.html (accessed on 5 April 2021).
[2] Article 37 of EU Charter of Fundamental Rights: "A high level of environmental protection and the improvement of the quality of the environment must be integrated into the policies of the Union and ensured in accordance with the principle of sustainable development".

the protection of privacy and personal data a normative restriction thereof and vice versa? How could a fair and balanced reconciliation of all rights be achieved? Does the law provide the instruments for striking this balance? What is the role of the existing ECtHR and CJEU case law for such an interpretation? Further, what is more: does national legislation play a role for a successful regulation? The paper is structured in four parts, as follows: in the first part, the importance of remote sensing technologies as tools for environmental monitoring and environmental law enforcement is analyzed. In the second part, legal issues regarding privacy and data protection from the use of remote sensing technologies for environmental purposes are presented. In the third part, existing legislation for reconciling emerging conflicts from the application of remote sensing technologies between the right for a high level of environmental protection and the rights for privacy and personal data protection is examined. In addition, major ECtHR and CJEU case law on the issue is approached focusing on the application of the principle of proportionality. In the fourth part, recent developments in Greek legislation and their application perspectives in environmental law are presented as a timely "case study". Greece, one of the oldest members of EU, with 80% of its surface belonging to mountainous areas and with thousands of islands, faces difficulties in the collection of data for its territory. As a result, the use of remote sensing technologies in Greece seems inevitable and therefore this country may become an excellent example for studying emerging challenges from the application of remote sensing technologies in the environmental sector.

2. Remote Sensing Technologies as Tools for Environmental Monitoring and Environmental Law Enforcement

2.1. Definitions-Brief Description of Current and Future Capacities

"Remote sensing may be broadly defined as the collection of information about an object without being in physical contact with the object. Aircraft and satellites are the common platforms from which remote sensing observations are made. The term remote sensing is restricted to methods that employ electromagnetic energy as the means of detecting and measuring target characteristics" (Sabins 1978). Remote sensing systems are based on signals and images acquired by sensors installed on artificial satellites or aircraft and are used for vast geographical phenomena (di Vimercati et al. 2013). The advancement of satellite technologies and unmanned aerial vehicles has been remarkable last decades. The technological development of satellite technologies on one hand has led to on-demand satellite constellations, which deliver high resolution data (0.75 m) with a daily revisit interval anywhere around the globe. In addition to the high resolution, they can acquire a sequence of images with a small time interval (video persistent mode) due to their unique rapid sensor depointing agility (Almar et al. 2019). Furthermore, as more countries gain their own Earth observation capability, commercialization is a common theme (Harris and Baumann 2021). On the other hand, unmanned aerial vehicles or "drones", although initially used almost exclusively for military applications, it is now to mention their rapid development for civil applications, and it has even been said that "we are entering the drone age" (Anderson 2012). The surveillance capabilities of drones are rapidly advancing and cheap storage is now available[3]. The capabilities of drones depend on what they are able to carry. Due to the growing commercialization of drones, commercial UAV manufacturers will increasingly improve their products following the needs of their clients. Additionally, a service sector will evolve to offer UAV services such as leased systems, on-demand flights, or consultation for choosing appropriate platforms or analyzing UAV-generated data (Watts et al. 2012).

To sum up, the future of remote sensing technologies can be described into three words: development, privatization, commercialization.

[3] Drones and Environmental Monitoring. 2017. Environmental Law Institute, Washington, DC, USA.

2.2. Applications of Remote Sensing Technologies in Environmental Monitoring and Environmental Law Enforcement

Remote sensing is used in numerous fields for environmental purposes. Remote sensing has provided the means for detecting and quantifying the rates of pollution, as well as for mapping and monitoring sources of pollution and the degree of remediation for their management. It has the means to respond and facilitate environmental management, and makes sound and evidence-based decisions in relation to Earth's resources at a global scale and across different continents, nations, and domains (Mertikas et al. 2021). Such a collection of environmental monitoring data through remote sensing technologies is undoubtedly essential for the effective decision making of environmental authorities.

Simultaneously, the most important applications of remote sensing technologies in environmental law enforcement consist of their use from public authorities for their work (duty) known as "environmental compliance assurance". Environmental compliance assurance describes all the ways in which public authorities promote, monitor and enforce compliance with environmental law. Through the Copernicus program and the relevant EU action plan, the EU Commission promotes the use of satellite images and other geospatial data resources to detect illegal disposal of waste, illegal land use and other breaches[4]. Earth observation technology may also contribute to implementing and ensuring compliance with multilateral environmental agreements (Kuriyama 2005) and they have been actually used to monitor the implementation of environmental agreements such as the World Heritage Convention, the Convention of Biological Diversity, the Ramsar Convention, the UN Convention to Combat Desertification, and the UN Framework Convention on Climate Change. In some countries, such as the Netherlands, earth observation technology is also used in the preparation of 'environmental impact reports' to obtain permits for new water projects, in order to verify their compliance with the legal framework[5]. Another significant application of remote sensing technologies in environmental law enforcement refers to collecting reliable information that can provide solid evidence to combat environmental crime (Patias et al. 2020). However, remote sensing technologies as means of proof are subject to certain limitations and are therefore preferably used as complementary means of proof. In particular, data collected by remote sensing technologies are of digital nature which means that they are subject to alterations and thus need to be verified[6]. In addition, strict control of the whole process of data collection and interpretation is essential, from the moment the data is obtained, in order to avoid wrong evidence (Laituri 2018).

3. Privacy and Data Protection: Legal Issues from the Use of Remote Sensing Technologies for Environmental Monitoring and Environmental Law Enforcement

Technology has always been a threat to the right to privacy, in other words, to "the right to be le(f)t alone" (Warren and Brandeis 1890). In spite of several attempts that have been made to define privacy, no universal definition of privacy could be created. Although the claim for privacy is universal, its concrete form differs according to the prevailing societal characteristics, the economic and cultural environment (Lucács 2016). There are—among others—the following forms of privacy: information privacy and location privacy. Informational privacy indicates much more as informational seclusion, a refugium for the individual. Informational privacy rests on the premise that information about ourselves is something over which individuals may exercise autonomy. Location privacy refers to the right of individuals to move in their "home" and other public or semi-public places without being identified, tracked or monitored (Mitrou 2009). In this sense, the use of remote sensing technologies in the current era may interfere with the rights to informational and location privacy. Observation of private spaces with remote sensing technologies or the location of a person (even without collection of data) or even the correlation of collected data with other

[4] Available online: https://ec.europa.eu/environment/legal/compliance_en.htm (accessed on 5 April 2021).

[5] ESA Workshop Evidence from Space, Document ESA-ISPL/EO 47, 5 October 2010, Available on line: https://www.space-institute.org/wp-content/uploads/2010/10/Workshop-Information-Package-Final.pdf (accessed on 5 April 2021).

[6] Ibid.

data may reveal information about individuals' (private) life. Especially when using drones also the so called "bodily privacy" could be affected. As "bodily privacy" we understand also the right to keep bodily functions and body characteristics private (Mitrou 2009). Indicatively, regarding the use of remote sensing technologies for monitoring compliance with environmental legislation on vegetation clearance, in a survey of UK and Australian farmers about their attitudes to being monitored using satellite imagery, most farmers were happy to be monitored this way in principle, however, 58% of Australian respondents and 75% of UK respondents agreed that satellite monitoring was "an invasion of their privacy" (Purdy 2011). Similarly, even if people are aware that certain drones are used for conservation purposes, for example for combatting illegal hunting in South Africa, they may nonetheless feel aggrieved (Sandbrook 2015). The use of remote sensing technologies may interfere also with the right to data protection. Privacy and data protection are closely linked but they are not identical. Data protection serves the protection of private life but the relevant rules apply also to personally identified information, which does not fall under the scope of "private life" even in its broad interpretation. Data protection rules are applicable, whenever personal data are processed (Mitrou 2009). The right to data protection will only protect individuals when remote sensing technologies process personal data (which includes collection of personal data). The collection of images, videos, sounds, and the geo-localization data related to an identified or identifiable natural person (according to the definition of Article 4 (1) of General Data Protection Regulation—GDPR) that has been collected by remote sensing technologies and may also be processed by using suitable methods is subject to data protection legislation. According to CJEU case law, personal data are those that "allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them"[7].

In this sense, very high resolution (VHR) satellite imagery creates considerable challenges for personal data protection, since contextualizing satellite imagery in reference to geographical locations, such as neighborhoods or even houses, can transform an individual in an image from arbitrary to distinguishable (Coffer 2020). Additionally, interactive maps that integrate various types of data, including satellite Earth observation data, into GIS, as well as zooming function available when browsing GIS, may make available personal information linked to a specific geographic location or even an individual (Doldirina 2014). In addition, the application of facial recognition technology or big data analytical software in data collected by remote sensing technologies puts in danger the protection of personal data when it constitutes process of personal data. With regard to drones the threats are more direct, since they can easily observe persons and private spaces and collect personal data, such as persons' locations, relationships etc. Further, what is more: if data subjects are not informed about the use of remote sensing technologies for monitoring purposes their right to informational self-determination and to autonomous and informed decision making is affected. Furthermore, if they are not adequately informed about the data processing equipment, about the purposes of data collection and the identity of who is collecting data as well as the agency's or company's location, that would result in an increased feeling of being under surveillance and a subsequent possible decrease in the legitimate exercise of civil liberties and rights, best known as "chilling effect"[8].

For this reason, personal data protection law is applicable, so that personal data procession may be only under strict requirements allowed (see below under Section 4.2). Before applying personal data protection law, it must be first checked whether personal data concerns are raised by the use of remote sensing technologies in each particular case.

[7] C-293/12 and C-594/12 *Digital Rights Ireland* para 27, C-203/15 and C 698/15 *Tele 2* para 99 and C-207/16 *Ministerio Fiscal* para 60.

[8] On the chilling and panopticon effect syndrome arising from a large-scale use of drones, see Rachel L. Finn, David Wright and Anna Donovan (Trilateral Research & Consulting, LLP), Laura Jacques and Paul De Hert (Vrije Universiteit Brussel), 2014, Privacy, data protection and ethical risks in civil RPAS operations, 7 November 2014, Available online: http://ec.europa.eu\T1\textgreater{}translations\T1\textgreater{}renditions\T1\textgreater{}pdf (accessed on 5 April 2021).

For example, regarding the use of remote sensing technologies for the detection of planning breaches, it is remarkable that the Belgium Privacy Commission in its Opinion no. 26/2006 stated that: "The Privacy Commission considered that the satellite images, insofar as they concerned property of natural persons, constituted information about identified or identifiable natural persons which qualified as personal data for the purposes of privacy law, and that the processing of that information by the planning authorities had to be treated as processing of personal data within the meaning of privacy law" (Billiet 2012).

4. Setting the Limits between Conflicting Rights

It is clear so far, that the importance of remote sensing technologies as tools for environmental monitoring and environmental law enforcement is undoubtable, however, the same time their use may cause considerable threats to the rights for privacy and personal data protection. In the following section, it is examined how a fair and balanced reconciliation of all rights could be achieved before technology significantly outpaces legislation[9].

4.1. Specific Legislation on Remote Sensing Technologies

Satellite remote sensing is subject to international space law. The Outer Space Treaty and the four follow-on treaties consist the most important documents for international space law. They have not been recently modified. There is to observe a lack of relevant and precise guidance in the Outer Space Treaty on issues of privacy related to VHR satellite data. Further, in the four follow-on treaties on space no specific provision is included, as no consideration has been given to privacy aspects and the respective protection. This is due to the fact that at the time these major space treaties were drafted no consideration was given to privacy protection (Dunk 2013). Only the Convention on International Liability for Damage Caused by Space Objects rules in Article II that "A launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight[10]". Taking into account that the term "damage" in Article I (a) is defined as the "loss of life, personal injury or other impairment of health", it can be claimed that a violation of an individual's privacy right can be potentially construed as an impairment of health under this Convention. Such an interpretation is based on the World Health Organization's definition of health[11], according to which health is "a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity" (Santos and Rapp 2019). In this sense, targeted surveillance or even the fear of constant surveillance by satellite remote sensing may disturb people's mental and social well-being and cause "damage" under the Convention on International Liability for Damage Caused by Space Object. Finally, neither the Resolution 41/65 on the Principles of Remote Sensing of the Earth from Outer Space focuses at all on privacy matters.

International law regarding unmanned aircraft systems clearly states a need for harmonization comparable to that of manned operations, even though drones are subject to national civil aviation law of the member States[12]. However, in such international contexts there is again no clear reference to privacy and personal data matters.

Nevertheless, especially for drones, there is to mention a recent trend for detailed regulation in European level. Regulation (EU) 2018/1139 clearly recognizes the threats for privacy and personal data protection by the use of drones: "The rules regarding unmanned aircraft should contribute to achieving compliance with relevant rights guaranteed under

[9] According to the Collingridge dilemma 'Regulators having to regulate emerging technologies face a double- bind problem: the effects of new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to change' (Collingridge 1980).

[10] Convention on International Liability for Damage Caused by Space Objects (1972), Available online: https://www.unoosa.org/pdf/gares/ARES_26_2777E.pdf (accessed on 5 May 2021).

[11] Preamble to the Constitution of the World Health Organization, reprinted in Final Acts of the International Health Conference, U.N. Doc. E/155, at 11 (1946).

[12] See: ICAO Cir 328, Unmanned Aircraft Systems (UAS), Available online: https://www.icao.int/meetings/uas/documents/circular%20328_en.pdf (accessed on 5 April 2021).

Union Law, and in particular the right to respect for private and family life, set out in Article 7 of the Charter of Fundamental Rights of the European Union, and with the right to protection of personal data, set out in Article 8 of that Charter and in Article 16 TFEU, and regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council[13]". Generally, the Regulation (EU) 2018/1139 serves for the protection of privacy in such use by setting what should be achieved. Recent Commission Delegated Regulation (EU) 2019/945[14] which applies since 1 July 2020 has divided drones into classes in terms of their technical characteristics (open, specific and certified category) and lays down the requirements for the remote identification of drones, which is very important in helping to determine the operator of the drone, serving thus for more effective privacy protection in the use of drones (Puraite and Silinske 2020). However, for classes C0 and C4, which are technically simpler and therefore more accessible to the majority of people, no requirement of a direct remote identification equipment is included. In addition, Commission Implementing Regulation (EU) 2019/947 of 24 May 2019[15] on the rules and procedures for the operation of unmanned aircraft, being in effect and applying since 1 July 2020, includes requirements for the implementation of three foundations of the U-space system, namely registration, geo-awareness and remote identification, which will need to be further completed. According to the Preamble of this Regulation par. 14 and 16: "Operators of unmanned aircraft should be registered where they operate an unmanned aircraft which, in case of impact, can transfer, to a human, a kinetic energy above 80 Joules or the operation of which presents risks to privacy, protection of personal data, security or the environment" ... "Considering the risks to privacy and protection of personal data, operators of unmanned aircraft should be registered if they operate an unmanned aircraft which is equipped with a sensor able to capture personal data". This is a clear safeguard clause but it is still questionable how alone the registration of operators would be effective for privacy issues if for classes C0 and C4, there is no requirement of a direct remote identification equipment. In addition, Article 11 of the Regulation 2019/947 states the rules for conducting an operational risk assessment while Article 18 (h) and (i) of the Regulation imposes the development of a risk based oversight system and an audit planning for certain drone operators, but it seems difficult to perceive how Article 35 GDPR[16] vis a vis Article 11 and 18 of the Regulation 2019/947 could complement each other (Pagallo and Bassi 2020). To sum up, the new legislation at EU level, namely Regulations 2019/945 and 2019/947, establish registration and remote identification requirements in the use of drones, making thus a huge contribution to the effectiveness of privacy and personal data protection, but with exceptions that could possibly undermine this goal, while there are still some unclear points of the risk assessment mechanism set.

4.2. Parallel Application of International and European Union Law on the Protection of Privacy and Personal Data

Apart from the above mentioned specific legislation on remote sensing technologies, it is important to assess the parallel application of International and European Union Law on the protection of privacy and personal data when using remote sensing technologies.

Protection of privacy on international level is ruled by Article 8 of the European Convention on Human Rights (ECHR): "Everyone has the right to respect for his private and family life, his home and his correspondence". According to Paragraph 2 of the Article 8 ECHR "There shall be no interference by a public authority with the exercise of this right

[13] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No. 2111/2005, (EC) No. 1008/2008, (EU) No. 996/2010, (EU) No. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No. 552/2004 and (EC) No. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No. 3922/91 Preamble para 28.

[14] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.

[15] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

[16] In Article 35 GDPR data protection impact assessment is ruled in 11 paragraphs. In particular, it is ruled when and how a data protection impact assessment is conducted in Member States.

except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". Therefore, the right to private life is not guaranteed in ECHR as an absolute right but it must be balanced against and reconciled with other legitimate interests, either private or public, while any interference with the right to privacy has to comply with the so—called "democracy test" (Mitrou 2009).

On European Union level, Article 16 of the Treaty on the Functioning of the European Union (TFEU) in accordance with Article 8 of the Charter of Fundamental Rights of the European Union, they rule together the protection of personal data. Article 7 of the Charter of Fundamental Rights of the European Union declares respect for private and family life. Furthermore, according to Article 52 (1) of the Charter of Fundamental Rights of the European Union, the principle of proportionality is introduced as a tool for balancing fundamental rights. According to the last Article, limitations on the exercise of the rights and freedoms recognized by the Charter must be necessary and appropriate.

In this sense, a limitation may be necessary if there is a need to adopt measures for the public interest objective pursued. If a limitation is proven to be strictly necessary, there must be also be assessed whether it is proportionate. Proportionality means that the advantages resulting from the limitation should outweigh the disadvantages the latter causes on the exercise of the fundamental rights at stake. To reduce disadvantages and risks to the enjoyment of the rights to privacy and data protection, it is important that limitations contain appropriate safeguards[17].

Furthermore, Union Law contains since very early specialized legislation on the protection of personal data. The current basic legislative acts for the protection of personal data in the EU is GDPR[18] on one hand, and Police and Criminal Justice Authorities Directive[19] on the other hand.

GDPR' s territorial scope according to Article 3 par. 2 b covers the processing of data (which includes collection) both from satellites and drones, as long as they collect or process data of EU residents, even if they collect or process such data from satellites under the jurisdiction and control of a non-EU country provided that processing activities are related to the monitoring of the behavior of EU residents as far as their behavior takes place within the Union. Police and Criminal Justice Authorities Directive applies to the processing of personal data by competent authorities of member states for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It also covers collected data both from satellites and drones, as long they are processed by competent authorities of member states.

Following the above mentioned legislation, and especially Article 52 (1) of the Charter and Article 8 (2) ECHR any limitation to the exercise of rights and freedoms recognized by the Charter must be provided for by law ("in accordance with the law"), made only if it is necessary and genuinely meets objective of general interest recognized by the Union or the need to protect the rights and freedoms of others ("in pursuit of one of the legitimate aims set out in Article 8 (2) of the ECHR and necessary in a democratic society")[20].

As a result, the police and other environmental authorities when using remote sensing technologies should first assure themselves that they have a valid legal basis for processing personal data. This also stems directly from Article 8 of Police and Criminal Justice

[17] Handbook on European data protection law. 2018. Available online: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed on 5 April 2021).

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[19] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[20] See also: Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilization of Drones. Available on line: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602 (accessed on 5 April 2021).

Authorities Directive as well as from Article 6 of GDPR. In this point, it is important to underline that Police and Criminal Justice Authorities Directive and GDPR supplement each other as they operate in different sectors but cooperate in the areas where they overlap (Pajunoja 2017). CJEU case law also identifies this relation between Police and Criminal Justice Authorities Directive and GDPR[21]. Therefore, police and the Criminal Justice Authorities Directive are applied when limitations to rights are imposed by the State for personal data collected directly by competent authorities only in order to serve their work (duty) for the prevention, investigation, detection or prosecution of environmental criminal offences. In cases when data are collected by third parties (private entities etc.) for other reasons but it happens them to be necessary also for the purposes of the prevention, investigation, detection or prosecution of environmental criminal offences, Article 23d of GDPR is applicable. Finally, Article 6e of GDPR is applicable, when administrative official authorities, such as forest services, environmental departments, environmental inspectors etc., that are authorized to protect the environment and impose administrative sanctions for law infringements, may according to a certain legal basis process personal data, for example inspect protected areas with drones.

Police and other environmental authorities when using remote sensing technologies should afterwards follow all principles stemming from Article 4 of Police and Criminal Justice Authorities Directive either from Article 5 of GDPR, namely their actions should comply with the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality (security), and accountability. This means that data subjects must be aware of the collection and processing of their personal data and therefore data controllers have the obligation to inform them according to the relevant Articles of Police and Criminal Justice Authorities Directive or of GDPR. Especially for drones, signposts or information sheets for an event could be easily used for drone operations in fixed locations, also social media, public display areas, flashing lights, buzzers and bright colors could be envisaged. Drone operators could also publish information on their website or on dedicated platforms in order to inform constantly about the different operations that take place[22]. In addition, remote sensing technologies shall be used from police and other environmental authorities when the necessity and appropriateness for the specific purposes is justified. A strict assessment of the necessity and proportionality of the processed data should take place.

Furthermore, data controllers and processors, where applicable, must implement the appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction according to the security principle (Article 29 of Police and Criminal Justice Authorities Directive or Article 32 of GDPR). Finally, it seems that a data protection impact assessment of Article 35 of GDPR is necessary (only when GDPR is applicable because such an impact assessment is not included in Police and Criminal Justice Authorities Directive), since remote sensing technologies, especially the use of drones, in the environmental law enforcement sector are likely to result in a high risk to the rights and freedoms of natural persons as stated above. Simultaneously, decisions that produce legal effects concerning the natural person, such as imposition of environmental administrative fines, can be based on processed remote sensing data, making a data protection impact assessment in these cases absolutely essential.

4.3. Relevant ECtHR and CJEU Case Law on Lawful Limitations of Privacy and Personal Data Protection

Under this rather complicated legislative background, finding relevant case law, seems to be more than vital for a successful interpretation of lawful limitations of privacy

[21] C- 623/17 *Privacy International*, para 47–48.

[22] WP29 apart from these also acknowledges the need for the creation of a national or cross-national information resource to enable individuals to identify the missions and operators associated with individual drones (Working Group on Data Protection in Telecommunication, Working Paper on Privacy and Aerial Surveillance, 54th meeting, Berlin, September 2013. Available online: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/ (accessed on 5 April 2021).

and personal data protection when using remote sensing technologies for environmental purposes. In this sense, relevant ECtHR and CJEU case law is of high priority.

A first observation is that the structure and wording of ECHR is different than that of the Charter. The Charter as already mentioned above does not use the notion of interferences with guaranteed rights, but contains a provision on limitation(s) on the exercise of the rights and freedoms recognized by the Charter. However, despite different wording, in their case law, the CJEU and the ECtHR often refer to each other's judgments, as part of the constant dialogue between the two courts to seek a harmonious interpretation of data protection rules[23].

According to the jurisprudence of ECtHR, interference is in accordance with the law if it is based on a provision of domestic law, which must be "accessible to the persons concerned and foreseeable as to its effects". Since very early the ECtHR had judged that the "notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued[24]. In its following jurisprudence the ECtHR considers further an interference "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient"[25]. More recently, the ECtHR interpreted the requirement of "necessity in a democratic society", as "including whether it is proportionate to the legitimate aims pursued, by verifying, for example, whether it is possible to achieve the aims by less restrictive means" while there is settled an obligation for domestic law for providing "adequate and effective safeguards and guarantees against abuse"[26].

The jurisprudence of the CJEU also recognizes the same necessity for adequate and effective safeguards and guarantees or in other words the "existence of clear and precise rules" and "minimum safeguards" to protect personal data against the risk of abuse and against any unlawful access and use of that data[27]. The CJEU also considers that only the objective of fighting serious crime is capable of justifying restrictions in personal data protection such as data retention measures or access to data protected by Articles 7 and 8 of the Charter[28]. However, the definition of what may be considered to be 'serious crime' is left to the discretion of the member states, since depending on the national legal system, the same offence may be penalized more or less severely. Therefore, it is finally the correlation between the seriousness of the interference and the objective pursued under certain criteria, such as the categories of data concerned and the duration of the period in respect of which access is sought, that is decisive for justifying a potential restriction[29].

In this sense, the CJEU often[30] refers directly to the principle of proportionality as the appropriate tool for properly balancing the objective of general interest against the rights at issue and underlines that exceptions that allow limitations on the protection of personal data must remain exceptions and not be transformed to the rule. Of special importance is C-73/16, *Peter Puškár* case, where the CJEU judged[31] that the processing of personal data by the authorities of a member state for the purpose of collecting tax and combating tax fraud without the consent of the data subjects is legitimate, provided that, those authorities were invested by the national legislation with tasks carried out in the public interest and

[23] Handbook on European data protection law. 2018. Available online: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed on 5 April 2021).

[24] ECHR *Leander v Sweden* No. 9248/81, 26 March 1987, para 50 and 58.

[25] *S. and Marper v the UK* (GC), 30562/04 & 30566/04, 4 December 2008, para 101.

[26] *Roman Zakharov v. Russia* (GC), 47143/06, 4 December 2015, Para 260, 236, *Szabo and Vissy v. Hungary*, 37138/14, 12 January 2016, para 57, *P.N v. Germany*, 74440/17, 11 June 2020, para 74.

[27] C-293/12 and C-594/12 *Digital Rights Ireland* para 54, C-203/15 and C 698/15 *Tele 2* para 109.

[28] C-203/15 and C 698/15 *Tele 2* para 102, C-207/16 *Ministerio Fiscal* para 56 and 57.

[29] C-746/18, *H. K. v. Prokuratuur* para 87–97.

[30] C- 623/17 *Privacy International*, para 64, 67, Joined cases C-511/18 *La Quadrature du Net and Others*, C- 512/2018 *French Data Network and Others* and C- 520/2018 *Ordre des barreaux francophones et germanophone and Others.*

[31] C-73/16, *Peter Puškár* para 112–117.

the principle of proportionality is respected. According to the decision such processing is proportionate only if there are sufficient grounds to suspect the person concerned for the alleged crimes. The court stated in this decision that the protection of the fundamental right to respect for private life at the European Union level requires that derogations from the protection of personal data and its limitations should be carried out within the limits of what is strictly necessary. In order to prove that such limitations are carried out within the limits of what is strictly necessary the CJEU requires from the national court to ascertain that there is no other less restrictive means in order to achieve the authority's objectives.

To sum up, it stems from all previous mentioned decisions of ECtHR and CJEU that limitations of privacy and personal data protection are lawful as long as they are proportionate to the legitimate aims pursued and they are imposed with sufficient safeguards against abuse or in other words as long as they are proportionate in so far as they apply only as it is strictly necessary under clear and precise rules with sufficient guarantees of the effective protection of privacy and personal data against the risk of misuse. Finally, it is obvious that although the objective of fighting serious crimes clearly justifies restrictions of privacy or personal data in areas of prevention, investigation, detection and prosecution of criminal offences, the condition of proportionality and strong safeguards to guarantee the rights are to be the same time fulfilled.

In regards with remote sensing technologies, although no ad hoc case law concerning the balance between the right for a high level of Environmental Protection and the rights for privacy and personal data exists, the use of the previously mentioned ECtHR and CJEU case law by analogy seems more than appropriate. Consequently, remote sensing technologies can be used for environmental purposes, especially for combatting serious environmental crime, however with sufficient guarantees for the effective protection of privacy and personal data, provided that no other less restrictive means exist.

In the following section, recent developments and first "concrete" steps in Greek legislation regarding the reconciliation of remote sensing technologies with personal data and privacy protection are presented, as well as their application perspectives in environmental law, in an attempt of a primary approach. However, it must be underlined even from this early point, that the new Greek regulatory framework is limited to certain crimes, covering thus only a small part of environmental crime, that is below analyzed. Police and Criminal Justice Authorities Directive (and its harmonization national law) as well as GDPR still regulate the majority of emerging legal issues from the use of remote sensing technologies for environmental monitoring and environmental law enforcement in Greece. Nonetheless, despite the limited scope of the new legislation, its value remains of great importance since it opens the path and the dialogue for a consistent regulatory framework of remote sensing technologies in national level.

5. The Case of Greece

5.1. The Special Features of Greece

Greece can be considered as a most interesting case for applying remote sensing technologies for environmental purposes. This is not only due to the natural features of Greece but also due to rules of constitutional protection of the environment, of privacy and personal data constitutional protection as well as due to the recent introduction of a specific regulatory framework for the use of remote sensing technologies in public places.

5.1.1. Natural Features and Remote Sensing Technologies

When it comes to the use of remote sensing technologies, Greece seems to be an "ideal" case study. This country is characterized by its unique relief, its alpine character, the great length of its coastline, its large number of islands, and its remarkable biodiversity, with habitats and species subject to a special protection status. Therefore, remote sensing technologies have great potential when it comes to covering the needs that arise from the purpose of environmental protection by replacing human physical presence, whenever such presence is inadequate or impossible.

The use of modern technological tools for the purpose of environmental protection is different from the former know-how employed by the Greek administration, which involved the "static" use of older technologies to address special technical issues (e.g., for purposes of public works[32] or for forest mapping[33]), and from the more recent one concerning the attainment of objectives of a wider range (National Cadastre[34], forest maps-Forest Register[35]) through modern technologies, which, however, are in these cases again used in a technocratic and mechanistic manner.

The usability of the most modern technologies, such as satellite imagery and UAVs, is nowadays examined in a 'dynamic' manner, i.e., for the purpose of systematically recording and using data where and when required, depending on the needs of an overall environmental protection strategy. Such a use, based on a real-time monitoring strategy, exceeds the existing administrative experience, on the one hand, and raises crucial questions about human rights and especially privacy and personal data protection, on the other hand.

5.1.2. Constitutional Protection of Conflicting Rights and the Principle of Proportionality as Counterbalance

Greek legal order has the particularity that provides a constitutional protection to the environment, and, especially to the forest environment, which is subject to a special status of enhanced constitutional protection (Article 24 par. 1 and Article 117 par. 3 of the Constitution) (Maria et al. 2020). At the same time, the rights of personal data, privacy, and personality protection are also constitutionally anchored (Articles 9, 9A, 5 of the Constitution).

Finally, any conflict between protected human rights in the Hellenic Constitution system is resolved through the implementation of the principle of proportionality (Article 25 par. 1 of the Constitution[36]), which is the essential counterbalance[37]. In the Greek legal order, the principle of proportionality was initially acknowledged by the Hellenic Council of State as a constitutional principle derived from the concept of State of justice[38], and after the constitutional revision of the year 2001, it was explicitly incorporated in Article 25 par. 1 of the Constitution.

5.2. Privacy and Data Protection in Greece

The inviolable nature of private and family life is explicitly guaranteed by Article 9 of the Constitution as well as by civil and criminal legislation, which protect these rights against infringements either by state authorities or by other citizens (Dagtoglou 1991). Moreover, the protection of privacy is further guaranteed by the Constitution through Article 19 (Confidentiality of letters, free correspondence and communication) and Article 21 (protection of family, marriage, motherhood and childhood, rights of persons with disabilities), while especially the confidentiality of letters and free correspondence and communication are supervised by the independent Communications Privacy Authority.

[32] Legislative Decree 3879/1958, PD 696/1974.

[33] Law 248/1976.

[34] Law 4512/2018.

[35] Law 3889/2010.

[36] Article 25 par. 1 "1. The rights of the human being as an individual and as a member of the society and the principle of the welfare state rule of law are guaranteed by the State. All agents of the State shall be obliged to ensure the unhindered and effective exercise thereof. These rights also apply to the relations between individuals to which they are appropriate. Restrictions of any kind which, according to the Constitution, may be imposed upon these rights, should be provided either directly by the Constitution or by statute, should a reservation exist in the latter's favor, and should respect the principle of proportionality".

[37] About the principle of proportionality and its adoption and evolution by the different national legal orders, the European Law, the CJEU case law and the ECHR case law: see Scaccia G. Proportionality and the Balancing of Rights in the Case-law of European Courts. 2019. federalismi.it, 4/2019, Available on line: https://www.sipotra.it/wp-content/uploads/2019/03/Proportionality-and-the-Balancing-of-Rights-in-the-Case-law-of-European-Courts.pdf (accessed on 5 April 2021).

[38] Hellenic Council of State 1341/1982, 2112/1984, 2261/1984, 3682/1986.

Personal data protection, which is inextricably connected to remote sensing technologies[39], is established in Article 9A of the Constitution[40] and currently regulated by Law 4624/2019, through which national law has been harmonized with Directive (EU) 2016/680. Privacy and personal data are also protected through criminal law, in Chapter 22 of the Penal Code regarding "infringements of personal confidentiality and communication" (Manoledakis 2008) and through civil law in Article 57 of the Civil Code regarding the protection of personality (Alexandropoulou-Egiptiadou 2007). Personal data protection in Greece is simultaneously directly subject to GDPR regulation.

Proper implementation of the personal data protection framework is under the supervision of the independent Data Protection Authority (hereinafter DPA). In the event of conflict between the necessity of safeguarding the environment and the protection of personal data, the necessary balance shall be pursued through the implementation of the principle of proportionality. In this sense, DPA in its Opinion 2/2010 considers that restrictions in personal data protection for the purpose of protecting the environment (as a whole, not only with regard to environmental crime), which is an explicit constitutional provision, are legitimate, as long as requirements set by the principle of proportionality (necessity, appropriateness, stricto sensu proportionality) are met.

5.3. The National Implementation of the Principle of Proportionality

5.3.1. The National Legal Framework on the Principle of Proportionality

Although Article 25 par. 1 of the Constitution establishes the principle of proportionality horizontally, namely in all cases of individual rights' restrictions, without any further distinctions or clarifications, the implementation of the principle itself is related to the particular characteristics of each restricted right and its specific legal frame. As foresaid, the protection of personal data is ensured by specific legislation, at international, EU and national level and the proper implementation of this legislation is supervised by DPA. Any derogation to the protection of personal data is subject to special strict rules, because personal data are connected to elements of human personality and in particular the private sphere of the individual. Therefore, collection and procession of such data is permitted only exceptionally, when and to the extent necessary to serve another legitimate interest, in accordance with the principle of proportionality[41].

Particularly in the monitoring technologies context, DPA issued the Directive No. 1/2011 regarding the use of video surveillance systems. Article 5 of this Directive, entitled "the principle of proportionality", provides that the lawfulness of personal data procession is examined with regard to the legitimate aim pursued as well as in accordance with the principle of proportionality. Video surveillance systems must be thus appropriate and necessary in relation to the aim pursued. This aim should the same time not be possible to be achieved by means equally effective but less restrictive for individual rights.

With regards to environmental protection, the principle of proportionality intervenes with an ecological role, allowing the restriction of other rights for the sake of environmental protection, and preventing any disproportionate infringement of the environment in the course of pursuing other lawful purposes[42]. Furthermore, it ensures the protection of other public or private interests against an intensive implementation of the precautionary

[39] The reason for the creation of a special legal framework for personal data protection lies on the special nature of the information produced by modern technologies, which may relate to certain individuals as well as important aspects of their identity (Wagner De Cew 2004; Solove 2003; Akrivopoulou 2011).

[40] Article 9A: All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law.

[41] DPA, Opinion 4/2020, Decision 31/2019.

[42] Thus, when examining compliance of distortion of forest vegetation with the Constitution, while pursuing a lawful purpose, the protection of forest vegetation must be weighed against the objective pursued, and it must be examined whether the specific goal can be achieved by other means (Hellenic Council of State 293/2009, Perivallon and Dikeo (In Greek) 2009, p. 494, Hellenic Council of State 2763/2006, Perivallon and Dikeo (In Greek) 2007, p. 70), since even if the change of the forest form is deemed to be permitted, it must be implemented with the "least possible loss of forest wealth" (Hellenic Council of State 3816/2010, Perivallon and Dikeo (In Greek) 2011, p. 123), and only to the "absolutely necessary extent" (Hellenic Council of State 2972/2010).

principle, which would systematically exclude the protection of other rights in the name of environmental protection, as well as the avoidance of excessive sanctions in case of violation of environmental protection measures[43] (Veinla 2004; Thomas 2000; McNelis 2000; Siouti 2018; Nikolopoulos 2000).

In particular, with regard to environmental crimes, the Greek environmental criminal laws, and especially, both Law 4042/2012[44] transposing Directive 2008/98/EC into the Greek legislation, and special statutes[45] respect the principle of proportionality, aiming at the implementation of preventive, effective, and proportionate sanctions, which will safeguard environmental protection more effectively.

5.3.2. The National Case Law on the Principle of Proportionality

Greek case law on the principle of proportionality is quite rich. According to national case-law, no right is absolute, not even the constitutional ones, therefore even a constitutional right, such as the right to personal data protection, may be restricted for reasons of public interest, such as the protection of other constitutional rights, in accordance with the criteria imposed by the principle of proportionality[46].

Particularly, in the monitoring technologies context, the Council of State considers in line with DPA's guidelines, that personal data may only be lawfully taken and processed when a legal interest is to be satisfied, provided that this legal interest obviously outweighs the rights and interests of the personal data subject and only if the legal order does not provide any other way for satisfying the specific legal interest[47].

Individual rights' restrictions for environmental protection is a special case of implementation of the principle of proportionality particularly important for national case law. Due to the paramount importance of environmental protection, due to environmental degradation throughout the planet and natural phenomena described as "climate change" as well as due to the need for decisive measures to ensure the effective protection of the environment, measures restricting other rights that are considered proportionate to this purpose may be very intensive, reaching even "the core" of restricted rights. In this sense, the substantial deprivation of the use of a property by its owner for environmental purposes, may be considered lawful, but the same time may lead to lawful compensation claim by the owner in proportion to the imposed deprivation[48]. Similarly, an absolute prohibition of hunting in an area of the Natura 2000 network, as long as there is a need for such a strict prohibition as an appropriate measure to protect wildlife in that area, is in line with the principle of proportionality[49]. Moreover, the Hellenic Supreme Court applies the principle of proportionality in order to resolve the question of procedural use, before civil and criminal courts, of evidence obtained through illegal means, despite Article 19 par. 3 of the Constitution which explicitly prohibits the use of illegal evidence. According to national case law, securing the exercise of the right to judicial protection of a party (Article 20 par. 1 of the Constitution) consists a legal reason for the use of evidence obtained through illegal means in accordance with the principle of proportionality, i.e., if the data collected are absolutely necessary and appropriate for the recognition, exercise or defense of a right before the court, to the extent absolutely necessary and insofar as this purpose cannot be achieved by other less restrictive means[50].

[43] Hellenic Council of State 1393/2016, which ruled that in determining the environmental fine, while determining the unified fine, the principle of proportionality is applied, through the co-assessment of the elements determining and restricting the amount of the fine, which are provided for in the substantive provisions of the environmental laws.

[44] Government Gazette, Series I, No. 24/ 2012.

[45] e.g., in accordance with article 94 §§ 1 and 8a' of law 4495/2017 for administrative and criminal sanctions in case of illegal constructions, it is considered that during the measurement of the imposed penalty, the value of the illegal construction and the degree of environmental degradation are to be taken into account.

[46] Hellenic Supreme Court (Plen. Sess.) 1/2017, Hellenic Council of State 1616/2012, 2254/2005.

[47] Hellenic Council of State 265/2017, 2254/2005.

[48] Hellenic Council of State 488/2018, 2428/2016, 2133/2016, 2601/2005.

[49] Hellenic Council of State 875, 876/2019.

[50] Hellenic Supreme Court (Plen. Sess.) 1/2017, Hellenic Supreme Court 901/2019, 653/2013.

5.4. The Establishment of a Modern Legal Framework

In view of the aforementioned parameters, and in the light of the CJEU case law, the current EU laws (GDPR, Directive 2016/680) and the opinions and guidelines of the national Independent Data Protection Authority) and pursuant to Law 3917/2011 (regarding the use of surveillance systems with sound and picture recording in public places), innovative legislation on the use of monitoring technologies in public places has been recently established in Greece, via the Presidential Decree 75/2020[51] (hereinafter PD). The PD 75/2020 does not provide for a general monitoring policy or a specific policy for environmental purposes, it only provides rules for the use of such technologies for crime prevention and repression and for traffic management. However, these provisions despite not aiming at the special regulation of the use of monitoring technologies for environmental purposes, contain, inter alia, rules applying on environmental crime prevention and repression. Therefore, even though the scope of the new legislation may be limited, it is important that these provisions, reflect all current European and national trends and needs regarding the exploitation of remote sensing technologies. Therefore, the analysis of these new specific rules can be the axis for the establishment of an integrated monitoring national legal framework for environmental purposes.

In this point, it must be noted that PD 75/2020 is a very recent law and therefore no related national case law has been produced yet, so its present analysis is only theoretical and cannot be based to any case law interpretation.

5.4.1. Overview of the Provisions of the Presidential Decree 75/2020

PD 75/2020 governs all the surveillance systems installed and operating at public spaces, provided that they process personal data, regardless of their technical specifications (Articles 1 and 2).

The restrictively designated public authorities that are competent for the prevention, investigation, detection, or prosecution of crimes, or the enforcement of criminal sanctions, namely the Hellenic Police, the Hellenic Fire Service, and the Hellenic Coast Guard, are considered as data controllers (Article 4).

The installation and operation of surveillance systems in public spaces is permitted only to the extent necessary, and when the objectives pursued cannot be achieved equally effectively using less restrictive means, in a specific place and for a specific period of time, following a reasoned decision of the competent authority. This decision has a validity term of no longer than three years, is subject to periodical evaluation and is issued following the conduct of an impact assessment study. Finally, it is promptly sent to the competent public prosecutor for district court judges. In particular, with regard to crime prevention or repression, it is required that there is adequate evidence that the offences subject to the PD were committed (Articles 5 and 12).

The collection and processing of sound data is only exceptionally allowed, following a specifically reasoned decision of the data controller, which is approved by the competent public prosecutor, for the purpose of detecting and recognizing the persons involved in specific punishable acts, including forest arson by negligence (Article 7).

Strict rules have also been established concerning the retention period, the complete and automatic destruction of the data without the right to retrieve them, and the anonymization of the data kept exceptionally for educational purposes (Article 8), the data recipients, and the safe and unimpeachable transfer of data (Article 9), and the rights of the data subjects, especially the right of information (Article 10).

Furthermore, organisational and technical safety measures are imposed with regard to the technical specifications and the operation of the surveillance systems, for the purpose of minimizing the impact on the right to personal data protection, in accordance with the accepted international standards, as well as the minimum safety measures (users' training,

[51] Government Gazette, Series I, No. 173/ 10 September 2020.

creation of separate accounts, and user authentication, data encryption, etc.) are explicitly provided for (Article 11).

Harmonisation of the Presidential Decree 75/2020 with the GDPR and the Police Directive

PD 75/2020 makes explicit reference to the general application of Regulation (EU) 2016/679 (GDPR) and Directive (EU) 2016/680 (Police and Criminal Justice Authorities Directive), but it further specifies special rules, which are harmonised with the principles derived from Article 5 of GDPR and Article 4 of the Directive, as analysed above.

Firstly, as far as the principles of lawfulness, fairness, and purpose limitation are concerned, the PD limits the collection and processing of personal data exclusively to the purposes restrictively specified by the authorising legal provision of Article 14 of Law 3917/2011 (Articles 1 and 3). Such a procession is subject to a decision provided by the competent public authority (Article 12) when the above objectives cannot be achieved equally effectively using less restrictive means, and, in particular, with regard to crime prevention or repression, provided that there is adequate evidence that the crime was committed, and, in any case, provided that the collection and processing is necessary (Articles 5 and 6).

Secondly, referring to the implementation of the principle of transparency, according to the PD, data collection and processing is contingent upon the prior notification to the public prosecutor, the gathering organiser, the data subjects, and the public, as appropriate, with any expedient means, and primarily with the means explicitly specified in its provisions (Articles 6 and 10). The foregoing obligation to notify the public prosecutor and the public also includes the notification of the decision of the competent public authority on the operation of a surveillance system (Article 12). Data subjects always have the right to request and receive information about the data concerning them and any recipients of the processing (Article 10 par. 3).

Thirdly, data minimisation principle is clearly reflected in the PD, which limits the installation and operation of surveillance systems to the specific necessary space, and prohibits expansion thereof to a broader area and collection of data from non-public spaces or homes, image focus is allowed only for the detection of crimes (Article 5), while sound data collection and processing is in principle prohibited (Article 7).

Furthermore, specific provisions have been set in order to ensure storage limitation. According to the PD, the maximum data retention period is, in principle, 15 days, with certain exceptions that serve the needs of the criminal court procedure, while specifically in the case of public gatherings, the maximum data retention period is 48 hours. In addition, integrity and confidentiality (security) are pursued through specific provisions in the PD. The automatic destruction of personal data is provided in a manner that precludes retrieval thereof, and in the case of their exceptional retention for educational purposes. The PD includes also provisions for data anonymization and compliance with the confidentiality obligation (Articles 6 and 8), and for ensuring, using suitable technical means, not only secure transfer of data, but also that the transferred data cannot possibly be distorted in an unperceivable manner (Article 9). Moreover, the data controller is subject to all the necessary organisational and technical security measures (Article 11), which are aligned with Article 25 of the Regulation, or Article 20 of the Directive.

Finally, the designation of the public authorities acting as data controllers, the establishment of the legislative framework of their liability (Article 4), and the establishment of special requirements for the issuance of a decision on the installation and operation of surveillance systems (Article 12) integrate the principle of accountability in the PD.

Critical Assessment of the Provisions of Presidential Decree 75/2020

The draft PD 75/2020 was submitted to the DPA, in accordance with the law, which issued its Opinion No. 3/2020, where, presenting an analysis of the Greek and European legal framework on personal data protection, and having particularly focused to ECtHR and CJEU case law, it stressed that certain provisions needed to be amended in order

to be compatible with the International and European Union Law. Compliant with the recommendations of the DPA, the final text of the PD constitutes a strict set of rules that integrate the principles of modern protection of personal data at an international and EU level.

Although the principle of proportionality is not explicitly mentioned at any point in the text of PD 75/2020, Article 5, which sets the conditions and criteria for the installation and operation of surveillance systems, introduces the special condition of implementation of the principle of necessity and the principle of appropriateness, as manifestations of the principle of proportionality. In addition, Article 8, with respect to the retention period and the destruction of data, also follows the recommendations of the DPA regarding the respect of the principle of proportionality[52]. Besides, the authorizing legal provision of PD 75/2020 explicitly stipulates that this PD should aim at setting the criteria for complying with the principle of proportionality[53].

It is also to underline that Articles 11 (Organizational and Technical Security Measures) and 12 (Decision on the Installation and Operation of Surveillance Systems) provide not only for the conduct of an impact assessment study at the stage of personal data processing, but also for the conduct of an impact assessment study concerning the installation, commissioning, and procurement of the surveillance systems, the software, and the additional equipment in general. Therefore, impact assessment accompanies the surveillance system and any accompanying item or equipment already from the stage of procurement thereof until installation, operation, and processing of the collected material. Such a provision is of great importance, since impact assessment at the time of the determination of the means for processing is essential for data protection by design and by default. In this sense, legal framework set by the PD not only follows in a timeliest manner current European trends on personal data protection but also forms the necessary legal background for any other future laws regarding the use of remote sensing technologies, including possible specialized legislation for environmental protection.

However, there are some points in which PD 75/2020 did not fully comply with the recommendations of the DPA. Thus, contrary to DPA's recommendations, Article 5 (installation and operation of surveillance systems) did not encompass any provision specifying clearly the criteria based on which surveillance in a specific space is evaluated as necessary, or the precise procedural requirements and the necessitated guarantees of supervision and control of the relevant measure. Similarly, Article 9 (data recipients) did not incorporate DPA's recommendation for a procedure of control and supervision by an independent authority in the case of transfer of data (except for the cases of transfer to administrative authorities acting as third parties where the transfer is approved by the public prosecutor). Finally, in Article 10 (Rights of data subjects), DPA's recommendations for special provisions for each surveillance system, and for persons who have lost their eyesight, so that the obligation of informing data subject could be most successfully achieved, were not taken into account.

Moreover, even at the points where the PD conforms to the DPA's recommendations, it is not certain that the final wording of the provisions is always correct. Thus, despite adding to Article 8 (Data retention period and destruction) the criteria on which the justified suspicions for preparing or committing in the future offences are assessed, pursuant to the Authority's recommendations, as a reason for exceptional extension of the data retention period, the criteria encompass the wording "any kind of relevant information[54]", which is rather ambiguous, and possibly leaves room for unauthorized extension of the data retention period. These shortcomings are indicative of the necessary adjustments for the lawful use of remote sensing technologies for all purposes and especially for environmental purposes.

[52] DPA, Opinion 3/2020, Available online: https://www.dpa.gr/sites/default/files/2020-07/gnomodotisi%203_2020.pdf (accessed on 5 April 2021).

[53] Law 3917/2011, Article 14 (4).

[54] Article 8 of the PD: " . . . justified suspicions for preparing or committing in the future the above criminal acts may stem from witnesses' testimonies or from any kind of relevant information".

5.4.2. Application of PD 75/2020 in Environmental Crimes

As already mentioned, PD 75/2020 does not specifically regulate the use of surveillance systems for the prevention and repression of environmental crime, however, its purpose, as described in Article 3, includes a large number of environmental offences, referring to the relevant provisions of the Criminal Code.

In particular, the scope of PD 75/2020 encompasses:

- organized environmental crime, in particular, felonies and misdemeanors committed for the purpose of pursuing financial gain (Article 187 of the Criminal Code);
- assault by a large crowd against environmental goods (Article 189 of the Criminal Code);
- arson in forests, forest and reforestable areas (Article 265 of the Criminal Code);
- flooding (Article 265 of the Criminal Code);
- destruction or damage to works or installations intended for protection from natural disasters (Article 273 of the Criminal Code);
- poisoning of sources, wells, and water tanks (Article 279 of the Criminal Code);
- destruction or damage to public environmental goods (Article 378 of the Criminal Code).

Therefore, PD 75/2020 offers, to a large extent, the possibility of using modern remote sensing technologies for environmental protection, since its scope primarily involves the protection of public environmental goods, including public forests, coastal and riparian zones, rivers, large lakes, sea, as well as the protection of all forest and reforestable ecosystems from arson. Furthermore, such technologies can be used both for preventive and for repressive protection of the above areas and elements (Article 3a).

5.5. Concluding Remarks for Greek Legislation and Future Perspectives in Environmental Law

Although the regulatory framework of PD 75/2020 includes many and significant offences of environmental relevance in its scope, it is found to be inadequate for facing emerging legal issues from the use of remote sensing technologies for environmental monitoring and environmental law enforcement. This is because it not only addresses certain environmental offences but also addresses them in a fragmentary manner. From this point, it even fails to regulate effectively issues related exclusively to environmental crime. It is a telling sign that Article 4 does not designate the competent environmental protection authorities as data controllers. Similarly, the provisions of Article 10 on information to the data subjects fail to take into account and to respond to the particularity of supervision of broad and freely accessible areas such as forest and coastal zones. In addition to this, the scope of PD 75/2020 is limited to the use of remote sensing technologies in public spaces, leaving private environmental goods (e.g., private forests, lakes, private coastal areas) unprotected.

Thus, it is recommended that a special legislative and regulatory framework is established, which will adjust the technical features offered by modern remote sensing technologies not only to the preventive and repressive treatment of environmental crime in its whole but also to their use in environmental monitoring and all aspects of environmental law enforcement. Lessons learned from the regulatory framework of PD 75/2020 for the protection of the infringed human rights, in accordance with the principle of proportionality, which calls for a special weighting based on the particular features of each environmental good, the special enhanced constitutional protection of forest ecosystems, and human rights' risks emerging from the use of technical means for environmental surveillance, should be taken into account, when forming such a special framework.

6. Conclusions

Remote sensing technologies provide tools for gathering data, which are extremely useful for ensuring a high level of environmental protection and the improvement of the quality of the environment. However, the same time they raise new difficult challenges,

such as their interference with the rights of privacy and personal data, which are also protected fundamental rights.

It stems from existing legislation and case law interpretation that remote sensing technologies in the European Union can be used for environmental purposes, especially for combatting serious environmental crime, however with sufficient guarantees for the effective protection of privacy and personal data, provided that no other less restrictive means exist.

The case study of Greece clearly shows that despite recent developments in the field of surveillance systems' legislation, there is still a gap in special legislative and regulatory framework which will envisage the lawful use of remote sensing technologies in the environmental sector.

However, the path has been opened and the great demand for a wider use of remote sensing technologies for supporting environmental law enforcement, for combatting environmental crime and for collecting environmental monitoring data will inevitably lead to a consistent regulatory framework in European and national level.

Author Contributions: Conceptualization, M.M. and E.-A.M.; Funding acquisition, M.M., A.P., E.-A.M. and L.M.; Investigation, M.M. and A.P.; Project administration, E.-A.M.; Supervision, E.-A.M. and L.M.; Writing—original draft, M.M. and A.P.; Writing—review & editing, M.M., A.P., E.-A.M. and L.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research is co-financed by Greece and the European Union (European Social Fund-ESF) through the Operational Programme "Human Resources Development, Education and Lifelong Learning 2014-2020" in the context of the project "Legal issues derived from the use of monitoring and earth observation technologies to ensure environmental compliance in the Hellenic legal order-HELLASNOMOSAT" (grant number MIS 5047355).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

Akrivopoulou, Hristina. 2011. The right to personal data protection through the lens of the right to privacy. *Theoria kai Praxi Diikitikou Dikeou* 7: 2. (In Greek).

Alexandropoulou-Egiptiadou, Evgenia. 2007. *Personal Data*. Athens-Komotini: Ant. N. Sakkoulas, p. 115. (In Greek)

Almar, Rafael, Erwin W. J. Bergsma, Philippe Maisongrande, and Luis Pedro Melo de Almeida. 2019. Wave-derived coastal bathymetry from satellite video imagery: A showcase with Pleiades persistent mode. *Remote Sensing of Environment* 231: 111263. [CrossRef]

Anderson, Chris. 2012. Here Come the Drones! August Issue: *Wired Magazine*. Available online: https://www.wired.co.uk/article/here-come-the-drones (accessed on 5 April 2021).

Billiet, Carole. 2012. Satellite Images as Evidence for Environmental Crime in Europe: A Judge's Perspective. In *Evidence from Earth Observation Satellites Emerging Legal Issues*. Edited by Leung Denise and Purdy Ray. Leiden: Brill, pp. 321–55.

Coffer, M. Megan. 2020. Balancing Privacy Rights and the Production of High Quality Satellite Imagery. *Environmental Science and Technology* 54: 6453–55. [CrossRef] [PubMed]

Collingridge, David. 1980. *The Social Control of Technology*. Birmingham: The University of Aston, Technology Policy Unit, New York: St. Martin's Press.

Dagtoglou, Prodromos. 1991. *Individual Rights*. Athens-Komotini: Sakkoulas, vol. 1, p. 323. (In Greek)

di Vimercati, Sabrina De Capitani, Angelo Genovese, Giovanni Livraga, Vincenzo Piuri, and Fabio Scotti. 2013. Privacy and Security in Environmental Monitoring Systems: Issues and Solutions. In *Computer and Information Security Handbook*. Edited by John R. Vacca. Burlington: Morgan Kaufmann, pp. 835–53.

Doldirina, Catherine. 2014. Privacy, earth observations and legal ways to reconcile the two. Paper presented at the 65th International Astronautical Congress, Toronto, ON, Canada, September 29–October 3.

Dunk, Frans G. 2013. Outer Space Law Principles and Privacy. In *Evidence from Earth Observation Satellites: Emerging Legal Issues*. Edited by Leung Denise and Purdy Ray. Leiden: Brill, pp. 243–58.

Finn, L. Rachel, and David Wright. 2016. Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Computer Law & Securty Review* 32: 577–86.

Harris, Ray, and Ingo Baumann. 2021. Satellite Earth Observation and National Data Regulation. *Space Policy* 56: 101422. [CrossRef]

Kuriyama, Ikuko. 2005. Supporting multirateral environmental agreement with satellite Earth observation. *Space Policy* 21: 151–60. [CrossRef]
Laituri, Melinda. 2018. Satellite Imagery Is Revolutionizing the World. But Should We Always Trust What We See? Available online: https://theconversation.com/satellite-imagery-is-revolutionizing-the-world-but-should-we-always-trust-what-we-see-95201 (accessed on 5 April 2021).
Lucács, Adrienn. 2016. What Is Privacy? The History and Definition of Privacy. Available online: https://www.semanticscholar.org/paper/What-is-Privacy-The-History-and-Definition-ofAdrienn/430bfacbabb89c0033b6dceddc18ba9bbc02c5f (accessed on 5 May 2021).
Manoledakis, Ioannis. 2008. Penal protection of personality. *Piniki Dikeosini*, 334. (In Greek)
Maria, Efpraxia-Aithra, Athanasios Papathanasopoulos, and Maria Maniadaki. 2020. Natura 2000 Forest areas in Greece: A national implementation review. *Zeitschrift fur Europäisches Umwelt-und Planungsrecht (EurUP)* 18: 68–85.
McNelis, Natalie. 2000. EU Communication on the Precautionary Principle. *Journal of International Economic Law* 3: 545. [CrossRef]
Mertikas, P. Stelios, Panagiotis Partsinevelos, Constantine Mavrocordatos, and Nikolai A. Maximenko. 2021. Environmental applications of remote sensing. In *Pollution Assessment for Sustainable Practices in Applied Sciences and Engineering*. Edited by Abdel-Mohsen O. Mohamed, Evan K. Paleologos and Fares Howari. Oxford: Butterworth-Heinemann, pp. 107–163. [CrossRef]
Mitrou, Lilian. 2009. The Commodification of the Individual in the Internet Era: Informational Self-determination or "Self-alienation"? Paper presented at the 8th International Conference Computer Ethics: Philosophical Enquiry, Corfu, Greece, June 26–28.
Nikolopoulos, Takis. 2000. The Principles Of Community Environmental Law. Available online: https://nomosphysis.org.gr/7034/oi-arxes-tou-koinotikou-dikaiou-periballontos-noembrios-2000/ (accessed on 5 May 2021). (In Greek).
Pagallo, Ugo, and Eleonora Bassi. 2020. The Governance of Unmanned Aircraft Systems (UAS): Aviation Law, Human rights, and the Free Movement of Data in the EU. *Minds and Machines* 30: 439–55. [CrossRef] [PubMed]
Pajunoja, J. Lauri. 2017. The Data Protection Directive on Police Matters 2016/680 Protects Privacy-The Evolution of EU's Data Protection Law and Its Compatibility with the Right to Privacy. Master's thesis, University of Helsinki, Helsinki, Finland. Available online: https://core.ac.uk/download/pdf/84363684.pdf (accessed on 5 April 2021).
Patias, Petros, Georgios Mallinis, Vassilios Tsioukas, Charalampos Georgiadis, Dimitrios Kaimaris, Maria Tassopoulou, Natalia Verde, Mario Dohr, and Michael Riffler. 2020. Earth observations as a tool for detecting and monitoring potential environmental violations and policy implementation. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences* 43: 1491–96.
Puraite, Aurelija, and Neringa Silinske. 2020. Privacy Protection in the New EU Regulations on the use of unmanned aerial systems. *Public Security and Public Order* 24: 173–83. [CrossRef]
Purdy, Ray. 2011. Attitudes of UK and Australian farmers towards monitoring activity with satellite technologies: Lessons to be learnt. *Space Policy* 27: 202–12. [CrossRef]
Sabins, F. Floyd. 1978. *Remote Sensing: Principles and Interpretation*. San Francisco: W. H. Freeman.
Sandbrook, Chris. 2015. The social implications of using drones for biodiversity conservation. *Ambio* 44: S636–47.
Santos, Cristiana, and Lucien Rapp. 2019. Satellite Imagery, Very High-Resolution and Processing-Intensive Image Analysis: Potential Risks under the GDPR. *Air and Space Law* 44: 275–96.
Siouti, Glikeria. 2018. *Manual of Environmental Law*. Thessaloniki: Sakkoulas, p. 58. (In Greek)
Solove, J. Daniel. 2003. *Information Privacy Law*. New York: Aspen Publishers, pp. 47–51.
Thomas, Robert. 2000. *Legitimate Expectations and Proportionality in Administrative Law*. Oxford: Hart Publishing, p. 78.
Veinla, Hannes. 2004. Determination of the level of Environmental Protection and the Proportionality of environmental measures in Community Law. *Juridica International* 9: 89. Available online: https://www.juridicainternational.eu/public/pdf/ji_2004_1_89.pdf (accessed on 5 April 2021).
Wagner De Cew, Judith. 2004. Privacy and Policy for Genetic Research. *Ethics and Information Technology* 6: 5–14. [CrossRef]
Warren, D. Samuel, and Luis D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4: 193–220. [CrossRef]
Watts, C. Adam, Vincent G. Ambrosia, and Everett A. Hinkley. 2012. Unmanned aircraft systems in remote sensing and scientific research: Classification and considerations of use. *Remote Sensing* 4: 1671–92. [CrossRef]