EJPLT
European Journal of Privacy Law & Technologies • 2021/1 • ISSN 270

Facial recognition: a challenge for Europe or a threat to human rights?

KONSTANTINOS KOUROUPIS
Assistant Professor of European and Data Rights Law
at Frederick University, Cyprus

Abstract

This article deals with the issue of the use of facial recognition, mainly in the European Union. Its purpose is to provide a thorough and coherent analysis of its lawfulness in accordance with the European legislation. Even though there is a concrete legal background provided by European Directives and Regulations, many EU member states apply facial recognition without a solid legal basis. Therefore, the article pursues to offer valid answers to data rights issues that arise. For this purpose, the study is divided into three axes. The first chapter provides a wide analysis of the European legislation which governs the use of facial recognition. Into the second chapter, special emphasis is given to the application of this method at national level. A critical approach is attempted with the aim to define the legal basis and illuminate the legal gaps raised. The third chapter gives an alternative approach of the issue since it demonstrates the wide use of facial technology at international level and its different legal regulation. The final conclusions not only reflect the research's findings but also propose effective safeguards for the lawful application of the facial recognition in order to improve the European digital strategy.

Keywords: Data protection; Digital strategy; facial recognition; GDPR; privacy; Alicem.

Introduction.

A 'Europe fit for the digital age' is one of the top 6 Commission priorities for 2019-2024.[1] It focuses on the development of a high-level digital strategy which puts to the forefront the use of new technologies in order to create new perspectives for businesses, to enhance security and reliability in technology and to gain greater progress in society. As predicted, the EU's digital strategy aims to put new technology to the benefit social good, to produce a fair and competitive digital economy with benefits for both businesses and people and, finally, to bring an open, democratic and sustainable society. All these goals will be achieved by many actions, both at national and European level. One of those actions is the use of artificial intelligence which '*can bring many benefits, such as better healthcare, safer and cleaner transport, more efficient manufacturing, and cheaper and more sustainable energy. The EU's approach to AI will give people the confidence to embrace these technologies while encouraging businesses to develop them'*.[2]

Artificial intelligence consists of performing many functions that were traditionally executed only by humans. Its scope extends to all levels of social life, such as health, transport, business and the economy. It should also be noted that the EU invests significant amounts to increase benefits brought from artificial intelligence to our society and economy. In the White Paper of the European Commission, entitled 'White Paper on Artificial Intelligence- A European approach to excellence and trust'[3] it is explicitly highlighted that artificial intelligence is closely connected with European legislation on human rights, especially in relation to the protection of privacy and data rights. As the possibilities for monitoring and analyzing people's daily habits and actions increase, as indicated in the workplace environment, it is easy to conclude that significant risks arise related to the above issues.

Facial recognition is a representative example of the application of artificial intelligence. According to Opinion 3/2012 on developments in biometric

[1] Further details on European Commission's priorities for 2019-2024 can be found at its official site https://ec.europa.eu/info/strategy/priorities-2019-2024_en.

[2] See more details about the nature, the scope and goals of artificial intelligence at the official site of the European Commission https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en. In addition, see D.Fiott and G.Lindstrom, 'Artificial Intelligence: What implications for EU security and defence?', published by European Union Institute for Security Studies (EUISS), 1 November 2018, pp.1-8. A general approach regarding artificial intelligence can be also found on M.Medeiros, 'Public and Private Dimensions of AI Technology and Security', in the report 'Modern conflict and artificial intelligence', Centre for International Governance Innovation, 1 January 2020, pp.20-25.

[3] The White Paper on Artificial Intelligence was adopted on 19 February 2020 and is available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

technologies of the Article 29 Data Protection Working Party [4] facial recognition is defined as 'the automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals. It can be executed through various methods, such as video surveillance systems and smartphones, fingerprint readers, vein pattern readers or just a smile into a camera which might replace cards, codes, passwords and signatures. In the White Paper it is emphasized that facial recognition might have two dimensions, identification and authentication of the person. As noted, '*identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his or her image is stored there. Authentication (or verification) on the other hand is often referred to as one-to-one matching. It enables the comparison of two biometric templates, usually assumed to belong to the same individual. Two biometric templates are compared to determine if the person shown on the two images is the same person. Such a procedure is, for example, used at Automated Border Control (ABC) gates used for border checks at airports*'.

It can be easily concluded that the automated processing of biometric data included in the facial recognition method carries with it risks to privacy and the protection of fundamental rights[5]. Nevertheless, it is a technique that tends to be widely used in several countries, both in Europe and internationally. [6] Therefore, there is a strong interest in examining the special content of facial recognition, especially its legal regulatory framework at EU level (first chapter). Furthermore, we will examine various methods of facial recognition used in certain countries and their legal grounds (second chapter). An additional part of the study is consecrated on the rules that govern facial recognition at international level in order to provide a comparative study of the issues in question (third chapter). Finally, some personal thoughts will be shared regarding facial recognition's legal challenges.

1. The European regulatory framework on facial recognition.

In general, facial recognition is closely related to issues of private life. Privacy has a wide meaning and can take various dimensions.[7] Notably, it includes many terms of physical and social identity of the person, such as the name, the physical, ethical and psychological composition, the right to personal

[4] Article 29 Data Protection Working Party, 00720/12/EN,WP193, Opinion 3/2012 on developments in biometric technologies, adopted on 27th April 2012, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[5] A thorough analysis of the risks to human privacy due to facial recognition systems can be found in J.A.Lewis and W.Crumpler, 'Questions about Facial Recognition', published by Center for Strategic and International Studies (CSIS), 1 February 2021, pp.1-7, M Carey, Artificial Intelligence Facial Recognition Threat Detection Environment, CreateSpace Publishing, 2018, pp.1-58.

[6] S Ghaffary and R Molla, Here's where the US government is using facial recognition technology to surveil Americans, 10 December 2019, available at https://www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future.

[7] According to the European Court of Human Rights, privacy constitutes a wide term which cannot be defined exhaustively. See *Niemietz v. Germany* (CC), no 13710/88, ECHR, 16.12.1992, *Costello-Roberts v. United Kingdom* (CC), no 13134/87, ECHR, 25.3.1993.

development and self-determination.[8] In the strictest sense, considering the method by which facial recognition takes place, European legislation on personal data protection applies automatically. In particular, data collected by facial recognition technology is classified as biometric data, as information about facial features is collected, which constitutes 'special categories of personal data', according to the General Data Protection Regulation.[9] The GDPR divides biometric data into two distinct categories: those relating to the physical, physiological human characteristics, such as weight, dactyloscopic data, eye colour, voice and ear shape recognition and those relating to behavioral characteristics of a natural person, such as keystroke analysis, handwritten signature analysis and eye tracking. Both of these categories, allow for and/or confirm the unique identification of that natural person.

Therefore, processing special categories of personal data is lawful if one of the specific conditions of article 9§2 of the Regulation are applied. In that respect, the opinion of European Data Protection Supervisor who proceeds to a thorough legal and ethical examination of facial recognition should be noted.[10] Firstly, there is the aforementioned requirement to meet one of the conditions of Article 9§2 of the GDPR. Then, special emphasis is given to the content of the consent that should be required. Article 7 of the European regulation sets out the nature of the consent: '*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding*'. The question arises as to what extent it is possible to obtain a consent with those elements? How can we be sure that the subject of data gives his consent free and without any reservation?

Furthermore, accountability and transparency should be observed. As it is emphasized, '*it is almost impossible to trace the origin of the input data; facial recognition systems are fed by numerous images collected by the internet and social media without our permission. Consequently, anyone could become the victim of an algorithm's cold testimony and be categorised (and more than likely discriminated) accordingly*'. Regarding this issue, we should add the provisions of the GDPR regarding data protection by design and by default.[11] Under these provisions, '*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*'. In other words, any organization, natural or

[8] See ECHR *Pretty v. United Kingdom* (CC), no 2346/02, ECHR, 29.4.2002, *R.R. v. Poland* (CC), no27617/04, ECHR, 26.5.2011.
[9] Article 9 of GDPR.
[10] W Wiewiórowski, EDPS, 'Facial Recognition: A solution in search of a problem?', 28 October 2019, article available at the official site of the European Data Protection Supervisor https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.
[11] Regarding the privacy by design and by default see article 25 of the General Data Protection Regulation.

physical person who intends to process data rights is encouraged to adopt any necessary, appropriate and useful measure, at the earliest stage of the design of the processing operations as well as to ensure the accomplishment of all conditions demanded for the lawfulness of the processing, according to the article 6 of the GDPR. Additionally, in accordance with the special guidelines on article 25 of the GDPR,[12] '*a technical or organisational measure can be anything from the use of advanced technical solutions to the basic training of personnel, for example on how to handle customer data*'. Furthermore, '*data protection by default' refers to the choices made by a controller regarding any preexisting configuration value or processing option that is assigned in a software application, computer program or device that has the effect of adjusting, in particular but not limited to, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*'.

The European Data Protection Supervisor seems to be uncertain regarding compliance in relation to the principle of data minimization. As the method of facial recognition itself is not fully accurate and clear, the collection of the necessary data is called into question.

Finally, facial recognition is disputable from ethical point of view as well as its value in a democratic society. The treatment of the human personality as an 'object' clearly violates fundamental human rights, weakening the value of the individual.

For all these reasons, the European Data Protection Supervisor seems to take a more negative stance regarding the use of facial recognition technology, especially since it is often used in respect to vulnerable social groups. Furthermore, he is against automated recognition technologies in public spaces, suggesting their temporary ban. However, without prohibiting facial recognition in an absolute degree, he puts a special burden of responsibility on the national data protection supervisors, who are also called upon to decide on this issue. Hence, this advice sets out his opinion on artificial intelligence which clarifies the safeguards of artificial intelligence with respect to fundamental human rights and recommends national data protection authorities issue specific guidelines on this matter.[13]

In addition to the legal analysis performed by the European Data Protection Supervisor, the processing of personal data by the method of facial recognition shall meet some specific provisions of EU data protection legislation. In that sense, both Article 57§1c of the GDPR and Article 46§1c of Directive 2016/680 require the prior opinion of the national data protection supervisory authority for any measure restricting the protection of personal data. Certainly, the data protection impact assessment is needed in order to demonstrate the dangers to fundamental human rights and freedoms as well as to suggest efficient and appropriate solutions.

The European Union Agency for Fundamental Rights (FRA) seems to

[12] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted by the European Data Protection Board, on 13 November 2019, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

[13] EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, Opinion 4/2020, 29 June 2020, https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf.

approach the issue in question with more criticism. Through a paper published at the end of November 2019 focusing on the fundamental rights challenges involved when public authorities deploy live facial recognition technology for law enforcement purposes[14], FRA expresses the opinion that the use of facial recognition technology by public bodies causes (or can lead to) serious harms to fundamental rights and freedoms. It recognizes that the collection and storage of facial images corresponds to the procession of biometric data which, according to article 9 (2) (g) of the GDPR, the processing of biometric data is only allowed where processing is "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Consequently, the use of facial recognition must be lawful, fair and transparent, follow a specific, explicit and legitimate purpose and meet all the necessary provisions of GDPR. Special emphasis shall be given on the strong impact that the collection of facial images might have on the exercise of other fundamental rights, such as the freedom of expression and/or the freedom of assembly since when applied during demonstrations may prevent people from exercising the aforementioned rights. Therefore, that collection should be considered disproportionate or unnecessary. Furthermore, facial recognition systems affect the rights of children and violate certain provisions of both European and international binding legal texts, such as the EU Charter of Fundamental Rights and the UN Convention of the Rights of the Child. According to those texts, the best interests of the child must be a primary consideration in all actions public authorities and private actors take concerning children. Since there is a collection, of sensitive data, their further processing demands stricter necessity and proportionality test, compared to adults, since children are more vulnerable.

In addition, we should underline the Council of Europe's policy regarding the issue of facial recognition. Recently, on 28 January 2021, the Consultative Committee of the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data has issued a set of guidelines on facial recognition technology (FRT), addressed to governments, legislators and the private sector[15]. Those guidelines reaffirm the imperative need to meet the fundamental principles of necessity, proportionality, accuracy, lawfulness, fairness and transparency, as well as all the aforementioned requirements by the European legislation. It is explicitly mentioned that facial recognition systems could be considered as necessary and proportionate only if they intend to prevent an imminent and substantial risk to public security, which should be documented before their application. In that vein, facial recognition used by private companies in uncontrolled environments, like shopping centres, should not be allowed.

In conclusion, it becomes obvious that the European legislation, both at EU level in strict sense but also more widely under Council of Europe's guidelines,

[14]Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.
[15] Available at https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

sets quite strict requirements for the legality of the application of facial recognition. In this respect, Margrethe Vestager, the European Commission's executive vice president for digital affairs, is very critical regarding this method as it breaches GDPR provisions, especially those for the obtainment of clear consent without any reservation. However, she didn't exclude the possibility of the latter occurring in special occasions, such as in the domain of security, and invited national data authorities to review the legal grounds which will allow member states to make their own domestic decisions.[16] Hence, responding to recommendations of some members of the European Parliament, the EU executive of the European Commission's DG Connect, Mr. Kilian Gross, declared during the European Parliament's Internal Market Committee, which took place recently, that a future ban on the use of facial recognition technology in Europe should not be excluded. Therefore, he highlighted the findings of the White Paper on Artificial Intelligence which are related to the use of facial recognition.[17] It is maybe for this reason that many countries, both in EU and outside, apply facial recognition technology, calling for further and thorough analysis and fair balance of rights.

2. Facial recognition in EU member states.

Despite the fact that facial recognition seems to be contrary to European legislation, at national level this method is often applied in several ways. There are different reasons for its application, such as for reasons of security (in airports), protection of public health or personal entertainment (these issues will be considered in more detail below).

France is the first country in the European Union where biometric data processing techniques are applied via the extensive use of cameras in the city of Nice, following the terrorist attack.[18] Furthermore, with the aim to prevent the expansion of the pandemic due to covid19, French police use cameras with speakers to reprimand people who break coronavirus rules.[19] However, French firm Datakalab whose software is used for video surveillance in many towns in France ensures the protection of personality and personal information as no image is stored or transmitted. In that sense, there is no facial recognition. Certainly, it should be noticed that both European Union and United Nations

[16] T Macaulay, 'Automated facial recognition breaches GDPR, says EU digital chief', 17 February 2020, https://thenextweb.com/neural/2020/02/17/automated-facial-recognition-breaches-gdpr-says-eu-digital-chief/.

[17] S Stolton, 'Commission will 'not exclude' potential ban on facial recognition technology', 3 September 2020, article available at https://www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology/.

[18] M Meeker, 'Nice has Europe's most sophisticated police surveillance, but it failed to stop a new terror attack', 30 October 2020, available at https://www.telegraph.co.uk/technology/2020/10/30/can-anti-terrorism-tech-protect-french-cities-residents-nice/, N Silbert, 'Vidéoprotection: jusqu'où iront les villes', 9 January 2019, available at https://www.lesechos.fr/idees-debats/editos-analyses/videoprotection-jusquou-iront-les-villes-347536, A Bellier, Nice, 'La ville la plus surveillée de France, pourtant vulnerable', 15 July 2017, available at https://www.ouest-france.fr/societe/faits-divers/attentat-nice/nice-la-ville-la-plus-surveillee-de-france-pourtant-vulnerable-4369155.

[19] E Braun, 'French police use cameras with speakers to shout at people who break coronavirus rules', 8 April 2020, available at https://www.politico.com/news/2020/08/04/french-police-coronavirus-cameras-speakers-shout-391320.

encourage the use of digital tools and new technologies with the aim to fight against Covid19. In any case, it is explicitly declared that any contact tracing and modern digital application shall meet all the safeguards for the respect of fundamental rights, especially of data privacy.[20] Hence, in the EU, member states must adopt a necessary and proportionate data retention policy, which conforms with the European regulation on data rights (GDPR) as well as establishes strong safeguards to prevent stigmatization of infected persons or close contacts of infected persons.

In the context of digitalization of services and e-government, we should highlight that France is the first country in the EU with a facial recognition ID system. In fact, the French government through its law on facial recognition, launched a project called 'Alicem' (Authentification en LIgne CErtifiée sur Mobile).[21] It aims to include facial recognition on users' smartphones to allow them to connect to government services applications. Its primary goal is to provide to French citizens and legal residents with a secure and valid digital identity. According to the *Ministry of Interior,* Alice will comply with the "high" security level defined by the European eIDAS (electronic IDentification, Authentication and trust Services) regulation and is in the process of certification by ANSSI (Agence nationale de la sécurité des systèmes d'information – National agency for information systems security). However, France's data regulator condemns this project as it violates the provisions of the GDPR, in particular those of requiring the consent of the subject.

It should also be noted that the method under consideration has been considered for use at airports for security and crime prevention purposes. However, there is no particular legislation which regulates the legality of the use of facial recognition. The opinion of the French Data Protection Agency (CNIL) is enlightening on these issues, as it provides a clear legal framework under which facial recognition can be considered legitimate.[22] CNIL indicates that the GDPR should govern the application of facial recognition in airports. The principles of necessity and proportionality should be taken into account in order to prevent any damage to public security. Of course, the protection of

---

[20] K Panetta, 'How Technology Can Curb the Spread of COVID-19', 18 May 2020, available at https://www.gartner.com/smarterwithgartner/how-technology-can-curb-the-spread-of-covid-19/, United Nations Division for Public Institutions and Digital Government, '*UN/DESA Policy Brief #61:* COVID-19: Embracing digital government during the pandemic and beyond', 14 April 2020, available at https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-61-covid-19-embracing-digital-government-during-the-pandemic-and-beyond/, E-Health Network, 'Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States', 15 April 2020, available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[21] Ministère de l'Intérieur de la République Française, 'Alicem, la première solution d'identité numérique régalienne sécurisée', 16 December 2019, available at https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee, ' France, First Country in EU With Facial Recognition ID System', 6 October 2019, available at https://www.telesurenglish.net/news/France-First-Country-in-EU-With-Facial-Recognition-ID-System-20191006-0011.html.

[22] A thorough analysis of the issue can be found at the official site of CNIL https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter. Further examination is available at K V Quathem and A Oberschelp de Meneses, 'French Supervisory Authority Releases Strict Guidance on the Use of Facial Recognition Technology at Airports', https://www.insideprivacy.com/data-privacy/french-supervisory-authority-releases-strict-guidance-on-the-use-of-facial-recognition-technology-at-airports/, 21 October 2020.

privacy and the completion of data protection impact assessments are required. Furthermore, all the principles of legal processing of data must be applied, such as those of accuracy, storage limitation, integrity and confidentiality and accountability. CNIL's position regarding obtaining prior valid consent is of great interest. According to the guidance in case, consent should be the legal basis for processing, and thus should meet the requirements for consent under the GDPR. Furthermore, there are some special additions:

- *airports should provide an alternative to individuals who do not consent to the use of facial recognition technology;*
- *airports should also allow individuals to withdraw their consent;*
- *consent should not be tied to or mixed with the acceptance of the terms and conditions of a ticket;*
- *individuals should receive enhanced information about the use of facial recognition technology and its alternative(s); and*
- *facial recognition technology should be used only on individuals who have provided their prior consent (for example, it should blur the picture of other individuals in the background and indicate the control zones).*

In our opinion, the requirement of prior valid consent should be fundamental. In fact, a balance between the right to privacy and the need to prevent criminal acts could be based on the optional use of facial recognition by the passenger. Anyone has the right to opt out and if someone refuses to be scanned, he will have his boarding pass and passport checked manually instead. not necessary for the lawfulness of facial recognition. Apparently, the principle to prior consent is respected and gives an adequate solution to the problem[23].The prior information of passengers could constitute the right legal basis as 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller', according to article 1(e) of the GDPR. Moreover, there is in force the Directive 2016/681, widely known as Directive Passengers Name Record (PNR), which provides for the transfer by air carriers of passenger's name records (PNR) data of passengers of both extra-EU and intra-EU flights.[24] With respect to the protection of fundamental rights of passengers and safeguards to their lawful processing, purposes of security and prevention of criminal acts take precedence. However, comparing the extent of the invasion to privacy by the two aforementioned methods, it can be deducted that is greater and more direct in case of facial recognition. Thus, the requirement of prior valid consent is necessary and cannot be substituted by the prior information.

It becomes obvious that GDPR provisions offer safe guidance for the application of facial recognition. Under those conditions, French courts declared school facial recognition illegal due to the GDPR, regardless of whether or not the prior consent of students had been obtained. CNIL also

[23] Facial recognition technology is already used at many airports in USA. A short but well-structured description and analysis on how is applied can be found on F.Street, 'How facial recognition is taking over airports', article published in https://edition.cnn.com/travel/article/airports-facial-recognition/index.html, 8 October 2019.
[24] Articles 1 and 2 of the Directive.

reaffirmed the decision by drawing attention to alternative less intrusive means, such as badge control.[25] In the same vein, the Swedish DPA has fined a municipality 200 000 SEK (approximately 20 000 euros) for using facial recognition technology to monitor the attendance of students in schools.[26]

However, facial recognition seems to be legitimate and legal for the purposes of public security. Hence, in October 2019, the Swedish Data Protection Authority (DPA) approved its use for criminal surveillance, finding it legal and legitimate (subject to clarification of how long the biometric data will be kept). Similarly, the UK DPA has advised police forces to 'slow down' due to the volume of unknowns – but have stopped short of calling for a moratorium. UK courts have failed to see their DPA's problem with facial recognition, despite citizens' fears that it is highly invasive. In the only European ruling so far, Cardiff's high court found police use of public face surveillance cameras to be proportionate and lawful, despite accepting that this technology infringes on the right to privacy.[27]

In accordance with the aforementioned rationale, Greece has recently issued the presidential decree 75/2020 which authorizes the installation and operation of surveillance systems which capture or record audio or video, in public places.[28] The prevention of criminal acts as well as traffic management that includes dealing with road network emergencies, regulating vehicle traffic, and preventing road accidents are defined as legal grounds for the installation and use of surveillance systems. Furthermore, the principles of justification and proportionality are required. Therefore, sufficient indications are required in order to demonstrate either the present or the possible future commitment of criminal offenses. The contribution of sufficient evidence is justified by the reporting of factual data such as, in particular, statistical or empirical data, studies, reports, testimonies, information on the frequency, type and specific characteristics of crimes committed in a particular area, as well as on the basis of the above elements, probable spread or transfer of crime to another public place. Surveillance is deemed necessary when, in the light of the above facts, a reasonable belief is formed that serious public safety risks are posed in these public areas. The prior authorization of judicial authorities is also necessary in case of public gathering. The data collected are erased 48 hours after the end of the event, unless there are serious reasons for

[25] Further details on this matter can be found in L Pascu, 'French high court rules against biometric facial recognition use in high schools', available at https://www.biometricupdate.com/202002/french-high-court-rules-against-biometric-facial-recognition-use-in-high-schools, 28 February 2020, T Christakis, 'First ever decision of a French court applying GDPR to facial recognition', available at https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/, 27 February 2020, O Kagan, 'France Prohibits Use of Facial Recognition Technology to Control School Entry', available at https://dataprivacy.foxrothschild.com/2019/11/articles/european-union/gdpr/france-prohibits-use-of-facial-recognition-technology-to-control-school-entry/, 4 November 2019.

[26] European Data Protection Supervisor, Facial recognition in school renders Sweden's first GDPR fine, available at https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en, 22 August 2019.

[27] A Daly, 'The use of live facial recognition technology through a comparative lens', available at https://infolawcentre.blogs.sas.ac.uk/2020/04/30/the-use-of-live-facial-recognition-through-a-comparative-lens-angela-daly/?fbclid=IwAR2mUlEMu5AHMYPXW_rhx_1vsCMvpfNsji_47GRqqIvWwQyLV_89T1rb9jU, 30 April 2020.

[28] The presidential decree is available (in Greek) at the official site https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/proedriko-diatagma-75-2020-phek-173a-10-9-2020.html (in Greek).

investigation of criminal acts. In that case the period of erasure can be extended up to 15 days.

3. The regulation of facial recognition outside European Union.

Contrary to the strict European Union's regulation on facial recognition and its restrictions, things are not the same at international scope. In China technologies based on artificial intelligence are widely used. Therefore, Facial recognition technology has become an integral part of people's daily life and is applied not only for private purposes (eg for home security or payment solutions) but also for public interest (eg police surveillance systems and traffic controls). Furthermore, many companies and organizations are also using facial recognition to improve their customer experience and increase business efficiencies. That phenomenon is favored by the lack of a relative regulatory framework on data facial rights. Considering that, personal information covers the sense and content of the aforementioned term and is defined as 'information that can identify the individuals and that involves privacy of individuals' under the Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks ('NPC Decision') effective as of 28 December 2012.[29] This definition has known several amendments through specific laws. Special emphasis shall be given on the Cybersecurity Law 2016 which offers, implicitly, a special provision on facial recognition; In particular, according to Article 76 of the CSL, '*'personal information' refers to various kinds of information recorded by electronic or other means which, whether independently or combined with other information, can be used to identify a natural person, including personal biochemical information*', which then implicitly covers personal facial information. In addition, the updated Personal Information Security Specification ('the Personal Information Specification') pointed out the concept of 'sensitive personal information' which can be derived from such procession of data rights and so can cover facial recognition issues. Of course, there are imposed strict restrictions on controllers when processing sensitive personal information, such as encryption when transmitting and storing sensitive personal information and a separate disclosure and consenting process. Since then, Face recognition cameras have been deployed in many parts of China to target security checks in public places, such as subway stations and shopping malls. The Minister of Public Security and Chinese police are using those systems of electronic monitoring of human behavior in streets in order to prevent illegal acts. Furthermore, companies such as ZTE, Dahua and China Telecom propose the adoption of new rules and international standards for the integration of face recognition, video surveillance and license plate registration.[30] However, many concerns have

[29] See more details about the regulation of facial recognition in China in C A Parsa, AI, 'Trump, China and the weaponization of robotics with 5G', The AI Organization, 2019, pp.22-28, 133-137. Also see M Tan, China : facial recognition and its legal challenges, 6 May 2020, published in China: facial recognition and its legal challenges (taylorwessing.com).

[30] According to J Kynge and N Liu, 'From AI to facial recognition: how China is setting the rules in new tech, article published in Financial Times', From AI to facial recognition: how China is setting the rules in new tech | Financial Times (ft.com), 7 October 2020.

been raised regarding the lawfulness of facial recognition. Several Chinese cities have imposed stricter laws and requirements on that technology since there are clear risks for human privacy.[31]

Like China, in USA does not exist any specific regulation on Facial Recognition Technologies. Nevertheless, many states use them for purposes of public interest. The Los Angeles Police Department has widely used, during last decade, facial recognition software via surveillance cameras in order to detect suspects of law infringements.[32] Despite that, many states demonstrate their strong fears about the dangers for human privacy due to the use of facial recognition technology. At this point it should be noticed a controversial facial recognition bill in California which finally didn't come into force since it met a huge criticism. Introduced as Assembly Bill 2261, the bill would provide a framework by which companies and government agencies could legally engage in facial recognition, provided they give prior notice. The utility of facial recognition was never questioned. Especially, in the era of Covid19 the aforementioned technology is widely applied and offers great services in health environment via several measures, such as tracking potential patients of Covid19 via specific masks. However, that method would lead to an uncontrolled and undefined surveillance in the workplace since the prior consent was not necessary. For that reason, many California cities did not finally proceed to the adoption of the bill.[33] According to the latest evolutions, facial recognition technology meets strong criticism at legal level since Portland, Oregon became the first jurisdiction in the country to ban the private-sector use of facial recognition technology in public places within the city, including stores, restaurants and hotels. Through the adoption of specific regulation which will come into force on 1st January 2021 'private entities' will be prohibited from using 'face recognition technologies' in 'places of public accommodation' within Portland, except (1) to the extent necessary to comply with federal, state or local laws; (2) for user verification purposes to access the user's own personal or employer-issued communication and electronic devices; or (3) in automatic face detection services in social media applications.[34]

Russia is another country where facial recognition technology is lawful and is widely used. In particular, in Moscow, a network of 100,000 cameras equipped with facial recognition technology are being used to make sure anyone placed under quarantine stays off the streets.[35] A Russian court

[31] T Qu and Y Xue, 'Chinese cities target facial recognition to curb abuse of personal data, article published in South China Morning Post', Chinese cities target facial recognition to curb abuse of personal data | South China Morning Post (scmp.com), 3 December 2020.
[32] K Rector, R Winton, 'Despite past denials, LAPD has used facial recognition software 30,000 times in last decade, records show', LAPD widely used controversial facial recognition software - Los Angeles Times (latimes.com), 21 September 2020.
[33] S Pont, 'On facial recognition, the U.S. isn't China-Yet', On Facial Recognition, the U.S. Isn't China—Yet - Lawfare (lawfareblog.com), 18 June 2020, R Johnston, 'Facial recognition bill falls flat in California legislature', Facial recognition bill falls flat in California legislature (statescoop.com), 4 June 2020.
[34] See more details on that issue in the article entitled Portland, 'Oregon First to Ban Private-Sector Use of Facial Recognition Technology', published in Portland, Oregon First to Ban Private-Sector Use of Facial Recognition Technology | Privacy & Information Security Law Blog (huntonprivacyblog.com), posted on September 10, 2020.
[35] See further details in P Reevell, 'How Russia is using facial recognition to police its coronavirus lockdown, article published in How Russia is using facial recognition to police its coronavirus lockdown - ABC News (go.com), 30 April 2020.

reaffirmed in its decision the lawfulness of such technology ruling that it does not causes any breach of privacy rights. [36] Certainly, there are several requirements for the conformity of facial recognition with data protection principles. Therefore, the cameras are controlled from a purpose-built coronavirus control centre. Images and personal details of those under quarantine are put on a database so they can be recognised by the cameras. The centre can also be used to monitor social media for 'fake news' on the coronavirus, according to officials, and track international arrivals from virus hotspots. However, serious concerns are raised since Russian national authorities seek to expand facial recognition technology. In particular, many privacy groups and digital rights lawyers allege that the national data protection legislation which enables the undefined procession of data rights for the purposes of protection of public security is unproportioned and incompatible with fundamental rights and freedom. According to those allegations, since there is no judicial or public oversight over the surveillance methods in Russia, including facial recognition, there is a potential infringement of the European Convention of Human Rights, mainly of the article 8 regarding the protection of private life. [37] The principles of proportionality, necessity and accountability are violated so facial recognition should be limited. At this point, it should be noticed that the European Court of Human Rights in Strasbourg has already ruled[38] that Russia's legal provisions governing communications surveillance did not provide adequate safeguards against arbitrariness or abuse, and that therefore a violation took place of Article 8 of the European Convention of Human Rights. Consequently, Moscow's use of facial recognition could be contested at the European Court of Human Rights.

Facial recognition is also legitimate and legal practice in Canada where it has been initially used for purposes of border controls. Therefore, in order to guarantee public and national security, the police authorities proceeded to the expansion of the facial recognition technology without any special requirements for the protection of human privacy. That expansion can be easily explained but not justified by the fact that Canada doesn't have a policy on the collection of biometrics, which are physical and behavioral characteristics that can be used to identify people digitally. Because of that, there are no minimum standards for privacy, mitigation of risk or public transparency, according to the Office of the Privacy Commissioner of Canada's website.[39] Consequently, facial recognition systems can be used. Due to the strong criticism regarding the lawfulness of the technology in case, the Canadian Commissioner of the Office of Privacy has recently outlined necessary actions for privacy and data

36 C Stephens, 'Russia court rules facial recognition technology does not violate privacy rights', article published in Russia court rules facial recognition technology does not violate privacy rights - JURIST - News - Legal News & Commentary, 4 March 2020, Reuters, Russian Court Rules in Favor of Facial Recognition Over Privacy Claims, article published in Russian Court Rules in Favor of Facial Recognition Over Privacy Claims - The Moscow Times, 4 March 2020.

37 See S Zhumatov, 'Russia Expands Facial Recognition Despite Privacy Concerns', article published in Russia Expands Facial Recognition Despite Privacy Concerns | Human Rights Watch (hrw.org), 2 October 2020.

38 *Roman Zakharov v. Russia* (GC), no 47143/06, ECHR, 4 December 2015.

39 H Solomon, 'Canada should stop using facial recognition at border crossings, says legal clinic', article published in Canada should stop using facial recognition at border crossings, says legal clinic | IT World Canada News, 7 October 2020.

protection in an annual report to parliament. Through the emission of two specific recommendations on artificial intelligence and its legal requirements, the Commissioner admits the necessity and the great value of the use of facial recognition platforms, especially in the era of the pandemic due to Covid19. Those platforms offer significant help and support in order to prevent the expansion of the pandemic and to protect public health. Nevertheless, stricter rules governing their use should be adopted in order to guarantee human privacy. In that vein, governments must cooperate with data protection authorities to ensure compliance with legal frameworks in the development and use of AI systems, keeping in mind consequences for human rights.[40]

Conclusions.

The thorough analysis which preceded demonstrated some useful conclusions. First of all, it is evident that European Union's policy on data privacy and artificial intelligence seems to provide more efficient and safe guarantees for the protection of fundamental rights in comparison to relevant international legislations. European Union continues to be the safeguard of fundamental rights and freedoms and consolidates the European area of justice. Regarding the legal treatment of the challenges produced by the rapid and ongoing evolution of the technology, it is clear that the facial recognition constitutes an inherent action of the EU digital strategy. Without any doubt, it includes processing of special categories of personal data. Despite the fact that existing European legislation on data rights could be applied, such as the General Data Protection Regulation, the Directive 2016/680[41] and the Directive PNR, the adoption of specific regulatory frameworks at national level is urgent. Certainly, all safeguards for the protection of fundamental rights must be implemented. However, due to the special nature of facial recognition and the continuous evolution of technology, all EU member states should adopt new laws on this issue. Therefore, national data protection authorities must cooperate and issue safe guidelines which would lead to the later adoption of laws.

Regarding the material scope of the proposed legislative package on facial recognition, it should be noticed that, in accordance with the relevant provisions of the GDPR[42] its use could be legal and legitimate for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security. A typical example of this use of facial recognition systems could be applied at airports, as it has been already

[40] K Pivcevic, 'Government facial recognition policies updated in Canada, Sweden and China', article published in Government facial recognition policies updated in Canada, Sweden and China | Biometric Update, 29 October 2020.
[41] 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.
[42] See Article 2 of GDPR.

thoroughly examined, due to the great extent of security risk and the high risk of criminal acts. Furthermore, due to the rapid expansion of the pandemic caused by Covid19, facial recognition technology could be used for the purposes of protection of public health. In all those cases, the establishment of strict conditions of application of facial recognition is of primary interest. In summary, the duration of use should be defined, the recipients of the act should not be children as well as it must be ordered by national authorities, such as police and judicial authorities. Furthermore, adequate and effective safeguards must be put in place against the abuse of power, in accordance with the European Court of Human Rights. [43] Such adequate and effective safeguards would require prior authorization by the competent Minister. In addition, the lawfulness of the measures should be examined either by a judicial authority or by an independent legal body. Under those specific conditions, facial recognition can meet not only the requirements set out under the European legislation on data rights but also the challenges posed by the EU digital strategy. Otherwise, uncontrolled facial recognition will lead to a new form of Orwellian society where technology will not serve the person but will eliminate human dignity[44].

[43] *Klass v. Germany* (CP), no 5029/71, ECHR, 6 September 1978, *Leander v. Sweden* (CC), no 9248/81, ECHR, 26 May 1987.

[44] Concerns have been already raised about the huge extent of mass surveillance due to face recognitions systems. See Senior, W Andrew, 'Privacy Protection and Face Recognition' in S Z Li, A K Jain (eds.), *Handbook of Face Recognition*, Springer-Verlag London Limited 2011, pp.671-691, J Stanley, *The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy*, American Civil Liberties Union, 2019, p. 5.