unimc
UNIVERSITÀ DI MACERATA
l'umanesimo che innova

Collana del Dipartimento di Giurisprudenza
dell'Università degli Studi di Macerata

New technologies between security and the protection of fundamental rights: a zero–sum game?

a cura di
SVEVA DEL GATTO

Editoriale Scientifica

Collana del Dipartimento
di Giurisprudenza dell'Università
degli Studi di Macerata

NEW TECHNOLOGIES BETWEEN SECURITY AND THE PROTECTION OF FUNDAMENTAL RIGHTS: A ZERO–SUM GAME?

a cura di

Sveva Del Gatto

EDITORIALE SCIENTIFICA

Volume stampato con il contributo del Dipartimento di Giurisprudenza e della Scuola di specializzazione per le professioni legali delle Università degli studi di Macerata e Camerino.

Via San Biagio dei Librai, 39 - 80138 Napoli
www.editorialescientifica.com info@editorialescientifica.com

ISBN 979-12-235-0558-8

Indice

Sveva Del Gatto

FACIAL RECOGNITION TECHNOLOGIES, PUBLIC SAFETY NEEDS AND ADMINISTRATIVE SAFEGUARDS. A COMPLEX BALANCE.

1. *Introduction*

The actions of public administration, including those of an authoritative nature, and the relationship between public administration and private subjects, citizens and businesses, have long been affected by profound changes. These are gradually leading to a rethinking of the traditional "authority-freedom" relationship with a view, if not to equality, certainly to a fairer balancing. On the one hand, the reforms that in recent decades have affected the Italian administrative system and the judicial review of public administration helped transform the position of the citizen with regard to the actions of public power; on the other, they contribute to reducing the deep mistrust that characterised public opinion towards public administration until the recent past.[1]

In this process of change, which is still ongoing, a central and disruptive role is destined to be played, not necessarily with always positive outcomes, by the rapid spread of new technologies and artificial intelligence also in public decision-making and in the delivery of new digital public services to citizens. Public administrations have been affected, especially in recent years, by a significant digitization process, which has

[1] F. Benvenuti, *Appunti di diritto amministrativo. Parte generale,* IV ed., Padova, 1959, pp. 183 ff. As noted by the Author: if one wished to introduce a notation of a psychological-social nature, one could say that the citizen's hostility toward the administration, the deep distrust depends precisely on the fact that just as the citizen feels, in substance, unprotected, in the same way the authority feels itself absolved of all responsibility.

been accelerated thanks to the investments included in the National Recovery and Resilience Plan (NRRP)[2]. This process, which is changing the public administration, improving its tools is bringing a gain in efficiency internal to offices and external to citizens-users. The usefulness of algorithms as a new "operational mode of management of the public interest" is appreciated, as noted by the administrative judge[3], with particular reference to all those serial or standardized procedures that the public administration is faced with and that involve the processing of large amounts of instances and the acquisition of certain and objectively verifiable data. In these cases, algorithms appear to be the tools of choice for correcting the distortions and imperfections that typically characterize cognitive processes and choices made by humans, and for speeding up and improving the activity performed. However, the use of artificial intelligence software is possible even for discretionary choices, as indicated by the Council of State itself and long admitted in doctrine[4].

Nevertheless, with regard to the relationship between public authorities and citizens, the use of algorithms is not neutral especially when it pertains to the issuance of administrative measures likely to affect the legal sphere of the recipient. Important and different, depending on the type of technology used and the activity carried out, are the problems and critical issues that must be confronted. The many benefits (especially

[2] See Component 1, Mission 1 of the National Recovery and Resilience Plan. In this direction also, Artificial Intelligence Strategic Program 2022-2024 and 2024-2026. The goal of digitizing public administration aims to improve services and performance for users and simplify relations between citizens and public administration in the belief that public administration can and should be an engine of development for the country, an ally of economic operators and not an obstacle. On these profiles see D.U. Galetta, *Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal PNRR e problemi ancora da affrontare*, in *Federalismi.it*, 7, 2022. On the nature of the National Recovery and Resilience Plan, see M. Clarich, *Il PNRR tra diritto europeo e nazionale: un tentativo di inquadramento giuridico,* in *Corr. giur.*, 2021, pp. 1025 ff.

[3] Cons. Stato, Sec. VI, April 8, 2019, no. 2270. On the jurisprudential evolution on the subject M.C. Cavallaro, G. Smorto, *Transizione digitale della pubblica amministrazione in Italia e diritto ad una buona amministrazione: fra prospettive aperte dal PNRR e problemi tuttora da affrontare*, in *federalismi.it*, 2019, pp. 11 ff.

[4] Developments in case law, however, indicate the use of algorithms even in discretionary procedures as possible and useful. On this point the doctrine is divided. On the subject, see E. Carloni*, I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2020, pp. 271 ff.; see also L. Torchia, *Lo Stato digitale. Un'introduzione,* Bologna, Il Mulino, 2023*, passim*.

in terms of gaining efficiency) that can be derived from the use of artificial intelligence in the exercise of public functions and services are, in fact, counterbalanced by the concrete risk of a significant infringement for the principles and guarantees towards public administrations.

This is especially true when the technology used falls within the facial recognition technologies that are receiving great interest from public administrations, especially local governments, as well as scholars.

The following paragraphs will therefore focus on facial recognition technologies, characteristics and operation. The problems that such systems pose especially when used by public administrations will be also analysed. Possible corrective measures will then be critically discussed, taking a cue from the (few) solutions developed by case law, decisions by privacy authorities and the regulation, referring not only to the Italian system but also to other systems in which the issue of the risks posed by facial recognition has been raised. Finally, some summary considerations will be made.

2. *Facial recognition systems: brief description of their operation and uses*

Facial recognition technology extracts and processes an individual's biometric data[5] creating a "biometric template". The possible uses of this

[5] The definition of biometric data provided by Article 4(1)(14) of the GDPR shows that it is: '*personal data obtained by specific technical processing relating to physical, physiological or behavioural characteristics of a natural person that enable or confirm his or her unambiguous identification, such as facial image or dactyloscopic data*'; in essence, what is relevant is the way in which the data of a person's face image is processed. Images of people's faces represent biometric data, insofar as they are capable of communicating information such as an individual's ethnic or racial origins, fall under the GDPR into the 'special categories of personal data' or sensitive data, which are accorded greater protection and additional safeguards than other personal data. In addition to the observed definition in the GDPR, biometric data are defined as '*special categories of personal data*' by Article 1(1) of the EU - Law Enforcement Directive. A special category in that from these data one has peculiar information about the individual from whom the data are extracted they reveal important aspects such as the mentioned ethnic and racial origins, membership in a religious or political group. Data capable of uniquely and unequivocally identifying an individual, such as data concerning his or her health or, again, sexual orientation, as also suggested by a reading of Art. 9 para. 1 of the GDPR. Similarly, such categories of data are also considered "special" in other jurisdictions. See for example the Australian case: here facial images and facial fingerprints are considered as sensitive information covered by additional protections under the Privacy Act 1988 because they are "biometric information used for the purpose of automated biometric identification." Biometric data have been referred to as an "umbrella concept" because, within this definition, very different types of data are

technique[6] are many[7]: from identification (or one-to-many comparison)[8] to verification (or one-to-one comparison)[9]. In addition to verification and identification, facial recognition can also be used for profiling individuals, as it allows certain characteristics such as gender, age and ethnic origin to be extracted from facial images. In this case, it is referred to as "categorization" to mean that the technology is not used to identify or match individuals, but their characteristics[10].

In recent years, facial recognition technology has spread rapidly in both the private and public sectors[11]: from object and person detection,

concentrated. J.D. Woodward, *Biometrics: A Look at Facial Recognition*, *Documented Briefing Rand Corporation*, DB-396-PSj, 293. Two main categories can be traced one referring to physiological and the other to behavioural data. Within the first classification we find devices capable of recognizing fingerprints, the geometry of our hands, and, again, smell, iris or face. The second, on the other hand, refers to the collection of information about behaviour, voice recognition, signature analysis (GDPR).

[6] Facial recognition belongs to the branch of deep learning and consists of automatic processing of digital images containing faces of individuals. In general, on facial recognition see E. Kindt, *Privacy and Data Protection Issues of Biometric Applications A comparative legal analysis* (1st edn. Springer, *Governance and Technology Series* 12, 2013); I. Iglezakis, *EU Data protection legislation and case-law with regard to biometric application*, Aristotle University of Thessaloniki, June 18, 2013.

[7] Art. 29, *Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services*, 00727/12/EN, WP 192, Brussels, March 22, 2012, 2; see also J.P. Woodward and Rand Corporation, *Facial Recognition: Defining Terms to Clarify Challenges*, November 13, 2019.

[8] Identification means that a person's facial image is compared with many other patterns stored in a database to find out whether his or her image is stored there. Facial recognition technology returns a score for each comparison and indicates the probability that two images refer to the same person. Sometimes images are matched against databases where it is known that the reference person is in the *database* (closed-set identification) and sometimes where this is not known (*open-set* identification). The latter operation would be applied when people are compared to *watchlists*.

[9] Facial recognition technology compares the two facial images, and if the probability that the two images show the same person is above a certain threshold, the identity is verified. Verification does not require biometric characteristics to be deposited in a central database. They can be stored, for example, on a card or in a person's identity/travel document. For a greater degree of detail on how this technology works, please refer to chapter 1 by Paolo Sernani in this book.

[10] If, however, the various characteristics are inferred from a face and potentially linked to other data (e.g., location data), identification of an individual could in fact be obtained as well.

[11] According to *The Global Expansion of AI Surveillance* study, edited by the *Carnegie Endowment for Institutional Peace*, 43 percent of states (precisely 64 out of a baseline sample of 176 states) used facial recognition technologies for surveillance purposes in 2019.

to access control to public and private buildings; from group demographic analysis to emotion analysis. The face can be used to unlock the *smartphone*, can be detected by CCTV cameras to enter offices or gyms, or to speed up *e-boarding* procedures at many airports. Of facial recognition there are known uses for commercial purposes, for example to record customer satisfaction levels, in the context of so-called *emotive marketing*, and also in the area of personnel where it can be used to identify, during a job interview, specific characteristics of the person for the purpose of recruitment.

Among the public administrations, facial recognition is now widely used: from schools, public housing, transportation to the public safety sector (in the species of public order, immigration and asylum).

In education, for example in Sweden and Marseille[12], facial recognition has been used to control and monitor student and visitor access and to quickly identify potential security risks. Still, the facial recognition technique is used to check attendance, assess students' attention or emotional state, and monitor examinations.

In the field of transportation, facial recognition technology is used to control access. In China, facial recognition systems are placed at bus stops and train entrances and are used to scan passengers' faces in place of physical tickets or digital ticket codes. Similar uses are being piloted in Kazakhstan.

In Russia, Face Pay is a system for accessing the Moscow subway simply by showing your face. In New York, facial recognition has been tested on bridges and tunnels to identify drivers with suspended licenses, to detect traffic violations, and to verify the driver's licenses of vehicle occupants.

Staying in the United States, facial recognition is being used in Detroit and New York City to monitor and regulate entry to public housing complexes. In Russia, Moscow's local government has announced the

East and Pacific Asia are the areas where there is-at least so far-the most widespread use of such technology (nearly 70 percent of states use it), while in the Europe and Eurasia region less than 40 percent of countries have adopted facial recognition technologies for surveillance purposes. Procuring this kind of technology and investing in its implementation are not only authoritarian systems. The interesting finding from the Report is that it is precisely liberal democracies that are the main users of facial recognition technologies, with a deployment rate of 51 percent of the total sample, compared with the lowest rate of 37 percent recorded in autocratic-type regimes. This means that one in two democratic states uses facial recognition devices for purposes-even in the broadest sense-of surveillance.

[12] See *infra* § 4.

citywide implementation of real-time facial recognition on public CCTV cameras and surveillance systems at entrances to most apartment buildings.

Facial recognition technology has been used to increase the deployment of national digital identity systems by offering help in digitizing public administration and improving the operation of digital services. For example, the State of Singapore has implemented SingPass facial recognition technology, one of the most advanced national digital identity programs in the world, which is used by residents to take advantage of numerous digital services, both private and governmental (including accessing tax returns and applying for public housing)[13].

However, the areas in which facial recognition technology appears to be most widely used are immigration and asylum and public safety. There are numerous examples in this field from different jurisdictions. In the United States, U.S. Customs and Border Protection uses facial recognition technology to screen people seeking admission to the United States. In the United Kingdom, the Home Office and the Ministry of Justice are reportedly planning to require immigrants convicted of criminal offenses to use facial recognition smartwatches[14]. The European Union uses facial recognition technology similar to the Biometric Exit Program at ports of entry to verify the identity of people applying for visas and asylum.

Facial recognition technology is used by law enforcement agencies in several countries to support investigations with the aim of making them faster and more effective, for example, in the search and capture of suspects or to find missing persons. In Italy, the S.A.R.I (automatic image recognition system) has been active since 2018. It allows the search for faces, otherwise unknown, by drawing on photos taken during mug shots (AFIS database) for comparison, automating the related search opera-

[13] The launch of the new feature, called *SingPass Face Verification*, is part of the government's US$2.4 billion (US$1.75 billion) *Smart Nation* initiative, launched in 2014, to digitize government services (from cashless payment systems to sensor-enabled street lighting). The new system was jointly developed by iProov, a UK-based biometric authentication provider and a Singapore-based digital government service platform provider. On the topic S. Del Gatto, *Riconoscimento facciale e uso dei servizi governativi. Numerosi benefici, ma quanti i rischi?,* su Osservatorio sullo Stato Digitale, IRPA, available at https://www.irpa.eu/riconoscimento-facciale-e-uso-dei-servizi-governativi-numerosi-benefici-ma-quanti-i-rischi/.

[14] The news reported by *The Guardian* newspaper can be read at https://www.theguardian.com/politics/2022/aug/05/facial-recognition-smartwatches-to-be-used-to-monitor-foreign-offenders-in-uk.

tions[15]. Facial recognition technology for law enforcement purposes is mainly used for face identification, whereby images obtained from police or private sources[16] are compared with a pre-existing database of images. Nevertheless, in some non-EU countries, facial recognition has also been used as an aid in interrogation techniques in order to understand from facial expressions whether or not the individual is telling the truth[17].

3. *The use of facial recognition technologies between guarantees of efficiency and risks of breaching fundamental rights*

The spread of facial recognition technologies brings with it many benefits as the examples just given suggest. Biometrics, in which facial recognition falls, provides higher levels of assurance that the person trying to access a service or perform a transaction is real. In addition, unlike the face, passwords, PINs and other personally identifiable information can be compromised by data breaches, allowing illegal access to accounts using traditional authentication methods. This is an undoubted advantage when we think about the digitization of services offered by public administrations.

States that take advantage of emerging technologies can provide more efficient services, reducing costs and freeing up resources to invest precisely in new digital infrastructure. This is coupled with the significant

[15] SARI is able, from a photographic image (taken from cameras on the street and videos made by officers) of an "unknown subject", to perform a computerized search both in the A.F.I.S. database (the law enforcement identification system) and on social media (where some of the boys in the pack posted comments the day after the attacks in the square in Milan). And thanks to two facial recognition algorithms, it is able to provide a list of images according to a degree of similarity. On the SARI system see V. Bontempi, *Un'interrogazione parlamentare sull'uso del riconoscimento facciale in Italia: il caso S.A.R.I.,* su Osservatorio sullo Stato Digitale, IRPA, available at https://www.irpa.eu/uninterrogazione-parlamentare-sulluso-del-riconoscimento-facciale-in-italia-il-caso-s-a-r-i/.

[16] Consider the well-known *Clearview* case on whose multiple events we refer to C. Ramotti, *Clearview A.I. approda in Italia?*; Ead., *Il caso Clearview e il Primo Emendamento alla Costituzione americana;* Ead., *Clearview A.I. cita in giudizio i dissidenti,* all of which can be consulted *online* on the Digital State Observatory, IRPA.

[17] As reported by A. M. Ousmane, T. Djara, W. Zoumarou, et al, *Automatic Recognition System of Emotions Expressed through the Face Using Machine Learning: Application to Police Interrogation Simulation*, 2019 *3rd International Conference on Bio-engineering for Smart Technologies (BioSMART)*, 1-4.

benefits that such techniques can generate in the public safety sector, where, for example, the use of facial recognition can help in identifying suspects and finding missing persons. For these reasons, in recent years, we are witnessing the exponential spread (further driven by the pandemic emergency) of facial recognition and verification systems.

The positive effects of using these technologies do not stop at speeding up and making existing tasks more effective and efficient, but also take the form of enabling the performance of tasks and obtaining results previously not even imagined[18].

On the other hand, facial recognition raises significant ethical and legal questions[19].

The main critical issue with facial recognition is the risk that the use of this technology could seriously infringe on people's fundamental rights (such as the right to privacy)[20] and freedoms and degenerate, as has hap-

[18] As noted by M.M. Young, J.B. Bullock, J.D. Lecy, *Artificial Discretion as a Tool of Governance: A Framework for Understanding the Impact of Artificial Intelligence on Public Administration*, in *Perspectives on Public Management and Governance*, 2019, 1-13 "*This presents questions for scholars of governance as to how the governance tool of artificial discretion will affect the effectiveness, efficiency, and equity of governance, and for the manageability and legitimacy of the tool. But in cases of many emergent technologies, the challenge in predicting impact comes from new tasks that are made feasible, not the rationalization of existing tasks. For example, AI can be used to generate massive new data sets by automating the processing of images and sensors or by standardizing unstructured data such as social media posts or text*."

[19] On these issues see the monographic works of C. Grieco, *Intelligenza artificiale e tutela degli utenti nel diritto dell'Unione europea,* ES, Napoli, 2023; G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative.* ES, Napoli, 2021.

[20] On the issues that facial recognition techniques raise about respect for fundamental rights, *ex multis* M. O'Flaherty, *Facial Recognition Technology and Fundamental Rights*, in *European Data Protection Law Review (EDPL)*, vol. 6, no. 2, 2020, pp. 170-173; E.J. Kindt, (2013). *Privacy and Data Protection Issues of Biometric Applications, Dordrecht, Heidelberg*. Springer; N. Taylor, (2002), *State Surveillance and the Right to Privacy*, in *Surveillance & Society, 1*(1), 66-85. See also European Union Agency for Fundamental Rights (2019), *Facial recognition technology: Fundamental rights considerations in the context of law enforcement, November 21, 2019* available at https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law and P. Alston, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/74/493, October 11, 2019, available at https://undocs.org/A/74/493.

pened in some jurisdictions, into forms of mass surveillance[21] used to control the population and repress dissent[22].

Precisely in urban contexts, as mentioned above, there is great interest in this technology, the use of facial recognition in open places and even more so during demonstrations, can give rise to the so-called chilling effect, a 'chilling effect'[23], affecting an individual in such a way that, for fear of being watched, they choose to give up exercising their fundamental rights, from freedom of assembly to freedom of expression, even to the point of giving up, returning to the topic of smart cities, the right to experience the city for fear that their private sphere may be irreparably violated[24].

A second problem, also typical of other artificial intelligence systems, is the risk of mistakes and biases related to race or gender. The NIST

[21] Risk this made particularly real in the period of public health emergency due to the spread of Covid-19 (think of the use of facial recognition techniques to monitor the spread of the virus).

[22] Evident in this regard are the drifts that such tools can have, as witnessed by some examples from overseas: think of China's social scoring system or what occurred during the Hong Kong protests when authorities used facial recognition systems to identify protesters and repress freedom of expression and assembly. On which K.L.X. Wong and A.S. Dobson, *We're Just Data: Exploring China's Social Credit System in Relation to Digital Platform Ratings Cultures in Westernised Democracies*, in *Global Media and China*, 4(2), 220-232. See also Z. Doffman, *Hong kong exposes both sides of China's relentless facial recognition machine*. *Forbes*, August 26, 2019. On the topic see the chapter by Fulvio Costantino in this book.

[23] EU Commission, *White Paper on Artificial Intelligence - A European Approach to Excellence and Trustworthiness*, Brussels, 19.2.2020 COM(2020) 65 final. For an initial commentary S. Del Gatto, *Una regolazione europea dell'AI come veicolo di eccellenza e affidabilità. Gli obiettivi del Libro bianco della Commissione europea sull'intelligenza artificiale,* Osservatorio sullo Stato Digitale, IRPA, available online at https://www.irpa.eu/una-regolazione-europea-ai-delgatto/.

[24] On the risks that facial recognition could degenerate into forms of mass surveillance, last January the International network of civil liberties organizations, a network that brings together fifteen independent human rights organizations, published the report "In Focus", documenting thirteen cases of the use of facial recognition collected in as many states, from Hungary to India, South Africa and Russia. The report denounces how the spread of this tool ends up normalizing public surveillance practices, undermining not only privacy but also the rights to freedom of expression, protest and equality. On this topic, A. Mascolo, *Riconoscimento facciale e sorveglianza pubblica: una tecnologia in cerca di regolamentazione*, Osservatorio sullo Stato Digitale, available online at https://www.irpa.eu/riconoscimento-facciale-e-sorveglianza-pubblica-una-tecnologia-in-cerca-di-regolamentazione/.

Interagency 8280 report[25], dated December 2019, found that most facial recognition algorithms still have a high rate of false positives as well as, although to a lesser extent, false negatives, especially when referring to people from West and East Africa and East Asia. Algorithms developed in China show the same effect, but reversed, with low false positive rates on East Asian faces. In the United States, algorithms used by law enforcement reveal higher false positives in American Indians, with high rates in individuals of African descent[26]. In this regard, emblematic and well known was the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) case. Used in several U.S. jurisdictions, COMPAS was produced by a commercial company and designed to quantify the risk of recidivism of individuals undergoing criminal proceedings, to calculate the likelihood of commission of further offenses over the next two years, and to decide the type and *quantum* of punishment to be imposed. With reference to it, by analysing more than 10,000 criminal defendants in Broward County, Florida, and comparing their expected recidivism rates with the rate that actually occurred over a two-year period, some scholars have verified that black defendants were far more likely than white defendants to be wrongly adjudicated at higher risk of recidivism[27].

4. *Facial recognition governance attempts*

While waiting for the European legislator to take action, the matter of facial recognition has been the object of interesting acts of so-called

[25] Viewable at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[26] The reason often lies in the very design and initial testing of facial recognition systems. Indeed, in Western countries, experimentation, prior to actual use, takes place with "white" men with Western features. RF systems therefore are "untrained" to recognize individuals with different facial features thus generating, an error rate that then results, in de facto discrimination. On this topic, A. Najibi*, Racial discrimination in face recognition technology, science policy blog, Special Edition: Science policy and social justice*, October 24*,* 2020.

[27] The study is reported in J. Larson, S. Mattu, L. Kirchner, J. Angwin, *How We Analyzed the COMPAS Recidivism Algorithm*, May 23, 2016, available *online* at https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. See also S. Barocas, A.D. Selbst, *Big Data's Disparate Impact*, *California Law Review*, *June* 2016, Vol. 104, No. 3, p. 671 ff. and G. M. Haddad, *Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom,* in *Vanderbilt Journal of Entertainment and Technology Law, 23,* 891-918.

soft law: in 2021, the Advisory Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) adopted the "Guidelines on Facial Recognition" with the aim of outlining a set of measures that not only governments, but also facial recognition system developers, manufacturers, service providers and user organizations should apply to ensure that this technology does not undermine the human dignity, human rights, including the right to protection of personal data, and fundamental freedoms of any person[28].

Subsequently, in May 2022, the European Data Protection Board (EDPB) issued Guidelines on Facial Recognition by Law Enforcement[29]. In this document, the EDPB, while recognizing the undoubted benefits that such techniques can bring in the area of law enforcement, stressed that such tools must be used in strict compliance with the applicable legal framework and only in cases where the requirements of necessity and proportionality are met, as stipulated in Article 52(1) of the European Charter for Fundamental Rights. In providing its guidelines, the Board also considered that the use of facial recognition technologies in public settings, indiscriminately and in all cases where these technologies can determine the classification of individuals by sex, race, religion or political affiliation, should be prohibited, in the same way as technologies that can also determine a subject's state of mind from the physiognomy and physiology of the face. Unfortunately, the solutions indicated, while appreciable, suffer from the lack of legally binding effects inherent in acts of so-called "grey legislation".

Case law and privacy public independent authorities have also attempted to identify principles and criteria aimed at preventing the violation of the fundamental rights of those affected by the use of facial recognition technologies by public administrations.

Among the first cases to be decided by a judicial authority was that on the use of automatic facial recognition technology in public places by the Wales Police[30].

[28] The text is available *online* at https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html.

[29] The text is available online at https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

[30] The lawsuit originated from an appeal brought by a civil rights activist who was unknowingly caught on camera in a shopping mall and, a second time, during an exhibition. According to the plaintiff, the Wales Police, on those occasions and, in general, during the testing phase of AFR technology, violated the *Data Protection Act*, the Human

After analysing the type of technology employed by the Wales Police and the concrete ways in which it was used, the lower courts dismissed the appeal and concluded that the authorities' actions were lawful[31]. According to the court, there was no conflict with paragraph 2 of Article 8 of the ECHR, according to which interference by a public authority is permissible only if it is provided for by law and constitutes a necessary measure for the protection of specific public interests (such as national security, or the protection of health)[32]. Furthermore, in the view of the

Rights Convention, and the *Equality Act*. In particular, the Police's processing of sensitive data (the biometric data collected by cameras in public places) was challenged as relating to ordinary people, not suspects, suspects or wanted persons, and as not strictly necessary for law enforcement purposes, as required by the regulations. The use of AFR technology would also violate Article 8 of the ECHR, which protects private and family life, as the power exercised by the Wales Police would lack a legal basis and consequently lack the requirements of "foreseeability, predictability, and hence of legality". Finally, the software used could result in erroneous *matches* due to the presence of *bias* and programming errors. On the matter see B. Davies, M. Innes, and A. Dawson, (2018), *An Evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, September 2018.

[31] See High Court of Justice Queen's Bench Division, Case No. CO/4085/2018, September 4, 2019 on which reference may be made to S. Del Gatto, *Quali regole per le nuove tecnologie di riconoscimento facciale? La Corte di giustizia di Cardiff si pronuncia per la legittimità dell'uso di tecniche di Automated Facial Recognition da parte della Polizia del Galles,* Osservatorio sullo Stato Digitale, IRPA, available online at https://www.irpa.eu/quali-regole-per-le-nuove-tecnologie-di-riconoscimento-facciale-la-corte-di-giustizia-di-cardiff-si-pronuncia-per-la-legittimita-delluso-di-tecniche-di-automated-facial-recognition-da-parte/.

[32] The use of facial recognition technology also, according to the judges, passes the so-called. *Bank Mellat test* under which an interference with rights under Article 8(1) ECHR can be justified only if the objective of the measure being pursued is sufficiently important to justify the restriction of a fundamental right; if there is a rational connection between the measure and the objective; if a less intrusive measure could have been used without unacceptably compromising the objective; and if, taking into account these aspects and the seriousness of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community. For the Court, in fact, AFR technology is aimed at crime prevention and its use in practice "struck a fair balance and was not disproportionate". Similar arguments were used by the British judges to reject the complaint regarding the alleged violation of personal data processing regulations. According to the judges, Section 35 of the *Data Protection Act* would be complied with because the AFR "*i*s strictly necessary to prevent and detect crime*"*. The court also found that the principles governing the actions of public authorities, contained in the Equality Act*,* were not violated: it was, in fact, affirmed that there is no valid reason to argue and prove that the accuracy of the *software* results may have been affected by factors such as gender or race.

judges regarding the necessary existence of a legal basis, there would exist "a clear and sufficient legal framework" represented by the primary law rules governing the powers and actions of the police, secondary legislative instruments, such as, for example, codes of conduct issued on the basis of primary law, and, ultimately, local policies adopted by the Wales Police[33]. The High Court of Justice thus concluded that the procedure followed by the police in using the data was "open and transparent" having, moreover, offered as an additional safeguard for the subjects filmed without their knowledge, the fact that, in the absence of a match between the captured image and a person on a checklist, all data corresponding to that image had been "immediately and automatically deleted".

The ruling[34] was reformed in August 2020. According to the Court of Appeal, the use of facial recognition technologies by the Wales Police was unlawful because it was not supported by an adequate legal basis and was adopted in violation of the Equality Act. The Court, in particular, censored what the judges called "fundamental deficiencies" in the legal framework for the use of facial recognition technology and in the policies that governed its use[35]. These deficiencies resulted in the police having "impermissibly wide" discretion[36], also producing negative consequences on the results of the DPIA conducted. According to the Court of Appeals, due to the legislative deficits, the DPIA, while correctly carried out by the police, would have led to the erroneous finding of compliance with Article 8 of the ECHR[37].

[33] As noted in the ruling, while these are already existing regulations, they can well be used for the regulation of the use of these new technologies and that applied as a whole they make the actions of the Police in the case "predictable and accessible" As noted by the Court, "[w]hat is important is to focus on the substance of the actions that use of AFR Locate entails, not simply that it involves a first-time deployment by SWP of an emerging technology. The fact that a technology is new does not mean that it is outside the scope of existing regulation, or that it is always necessary to create a bespoke legal framework for it".

[34] The conclusions of which immediately appeared to be criticized. See S. Del Gatto, *Quali regole per le nuove tecnologie di riconoscimento facciale?.,* cit., e Ead., *Potere algoritmico,* digital welfare state *e garanzie per gli amministrati.,* cit., 839, *sub* note 24.

[35] Royal Courts of Justice Strand, London, WC2A 2LL Date: 11/08/2020, available *online* at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[36] As noted by the English lower courts, "the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law".

[37] The Court of Appeals has, specifically stated that: "The unavoidable consequence

The Court, then, upheld the last ground of appeal concerning compliance with Section 149 of the Equality Act of 2010, arguing that the NSW Police "never sought to ensure, either directly or through independent verification, that the software program had not caused unacceptable prejudice on grounds of race or sex". Finally, the Court concluded with the hope that "as AFR is a novel and controversial technology, all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias".

On the legality of the use of facial recognition, national privacy independent authorities have since ruled on several occasions.

In Italy, for example, the "Garante per la protezione dei dati personali (GPDP)" has rejected SARI Real Time, deeming it not in line with the standards imposed by the legislation on the matter. According to the Authority, SARI Real Time, insofar as it is installed in public places open to the public, would carry out large-scale automated processing that would extend even to those who are not included in the police watch-list, since the identification of the suspected person would require the biometric processing also of all other people who happen to be circulating in the monitored public space. This would result – in the view of the Authority – in an evolution of the very nature of surveillance activity, bringing about a shift "from targeted surveillance of certain individuals to the possibility of universal surveillance for the purpose of identifying certain individuals". It would, in essence, give rise to "a new surveillance model" that would introduce "*de facto*, a non-reversible change in the relationship between individual and authority"[38].

of these deficiencies is that, despite the DPIA's attempt to address the Article 8 issues, the DPIA failed to adequately assess the risks to the rights and freedoms of data subjects and failed to address the measures provided to address the risks arising from the deficiencies we found, as required by Article 64(3)(b) and (c) of the DPA 2018".

[38] Opinion, March 25, 2021, No. 127. Precisely because of the incisive interference with people's private lives – with the correlated risk of compression of certain individual and collective prerogatives of an essential nature, including the right to respect for personal life and freedom of expression – the Garante believes that such a device must be justified by an adequate regulatory basis that identifies the conditions of admissibility and limits. According to the GPDP, in order to be satisfactory, such a normative basis should take into account all the rights and freedoms involved and define the situations in which the use of such systems is possible, avoiding conferring "such a wide discretion that its use depends in practice on those who will be called upon to dispose of it, rather than on

Outside national borders, Canada's Federal Privacy Commission has observed that the use of facial recognition technologies by police for mass surveillance should be banned as overly intrusive to the privacy of individuals, also highlighting the need for legislation.

The privacy Commissions of Canada, France, the United Kingdom and Italy have, then, sanctioned the company *Clearview* for creating a database with billions of personal images, collected *online* without consent, in order to sell a biometric identification service to law enforcement agencies.

The issue of consent in relation to the use of facial recognition systems has also been the subject of other decisions. In Sweden, Datainspektionen (the National Data Protection Authority), fined a high school in Skellefteå for introducing a facial recognition system to check student attendance. Swedish legislation that implemented the GDPR includes an express prohibition on the processing of biometric data, such as those used in facial recognition. Although the school had stated that it had obtained the consent of the students, Datainspektionen found that in that specific case consent could not constitute an appropriate legal basis, given the position of subjugation in which the students find themselves in relation to the school (a public administration) and therefore decided to impose the sanction.

A similar case was decided by the Administrative Court of Marseille[39] where the local school office, after entering into a contract with the private company Cisco International Limited, had facial recognition cameras installed on students in a high school. Following an appeal filed by the parents' association, the Court censored the school office's decision, finding that there was a violation of the GDPR because the students could in no way provide free consent to the processing of their biometric data due

the enacted normative provision". Regulatory foundation considered by the *Privacy Authority* to be non-existent in national law to date, as no adequate legal basis for the processing of biometric data can be found either in Legislative Decree No. 51/2018 (which regulates the processing of personal data for the purpose of prevention, investigation, detection and prosecution of crimes) or in the Code of Criminal Procedure. On this topic, see A. Mascolo, *Riconoscimento facciale "in tempo reale": il Garante per la privacy boccia S.A.R.I. Real Time*, Osservatorio sullo Stato Digitale, IRPA, available *online* at https://www.irpa.eu/riconoscimento-facciale-in-tempo-reale-il-garante-per-la-privacy-boccia-s-a-r-i-real-time/.

[39] Tribunal Administratif de Marseille, February 3, 2020, No. 1901249, available online at https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf.

to the position of power in which the school authority holds over them. Such a surveillance system represented, according to the judges, an opt-out adherence, devoid of the possibility of withholding consent since the student who did not wish to be subjected to such processing would not be able to access the school building thus suffering an infringement of his or her right to education.

Referring to regulatory solutions, a significant watershed in the governance of facial recognition technologies was the entry into force in 2024 of the Artificial Intelligence Act[40] before which, Italy, choosing a solution of utmost caution, had banned the use of facial recognition systems *tout court*[41].

[40] Regulation (EU) 2024/1689 of the European Parliament and of the Council – June 13, 2024. The long gestation is partly due precisely to the tensions that the gradually proposed solutions on facial recognition have caused. In the long period between the proposal for a Regulation put forward by the Commission in 2021 and its final approval, positions on facial recognition technologies have, in fact, changed several times due to the attempt to hold together the different positions on the subject brought forward by individual states and European institutions. After an initial move away from the position of total closure immediately expressed by the European Parliament (on October 6, 2021, the European Parliament had voted by a majority vote a resolution calling on the European Commission to ban, by a general regulatory act, facial recognition as a general prevention tool throughout the European Union. See https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.pdf), subsequent versions of the *AI Act* appeared to be more cautious until the final version in which we see a substantial compromise such that, it was said, it bans facial recognition technologies, but with some openings explainable by the need to consider the position of some member states opposed to the full ouster of this technique.

[41] See Decree Law Oct. 8, 2021, No. 139 "Urgent provisions for access to cultural, sports and recreational activities, as well as for the organization of public administrations and in the field of personal data protection" aimed at introducing provisions on the management of the pandemic emergency from Covid 19. The deadline initially set for Dec. 31, 2021 was first moved to Dec. 31, 2023 and lastly postponed to the end of December 2025 by Article 8 of Decree Law "Public Entities," May 10, No. 51. The prohibition therein is not, however, absolute: processing carried out by the competent authorities for the purpose of preventing and suppressing crimes or enforcing criminal sanctions is excluded, provided that there is a favourable opinion from the Data Protection Authority. The opinion is not, however, necessary where the processing is carried out by the judicial authority in the exercise of judicial functions as well as judicial functions of the public prosecutor. The solution adopted by the Italian legislature appears inadequate to deal with the new challenges posed by the use of facial recognition, particularly by public authorities, and on closer inspection does not meet either the expectations of those in favour of the use of these technologies in public places or those open to the public, or those against it. The rule banning facial recognition, specifically, appears short-sighted, not very courageous, and not decisive. Timid and short-sighted because it takes into ac-

The AI Act, on the contrary, adopts a compromise solution that bans facial recognition technologies but with some openings due to the position expressed by some member states opposed to the full ouster of this technology: in accordance with the risk-based approach underlying the entire Regulation, real time facial recognition systems, as qualified high-risk artificial intelligence systems, are banned except for law enforcement reasons and under certain prerequisites and limitations[42].

5. *Conclusions*

How does this reflect on the nature of public power and the relationship between "authority" and "freedom" and between public administrations that use facial recognition in the exercise of their functions and the recipients of measures taken? Does the use of these technologies by public power result in a significant change in the existing model, starting with the Italian constitutional model, of the relationship between public administration and citizens?

In our system, in the pursuit of the interests of public safety and public order, citizens' freedoms represent a logical and legal *prius*, from

count neither inevitable technological progress nor the actual needs of citizens to be able to take advantage of the benefits made available by facial recognition technologies. It is unhelpful from a fundamental rights protection perspective because the ban introduced is subject to very broad limits. See S. Del Gatto, *Facial Recognition in Italy: legal problems and perspective, in European Review of Digital Administration & Law-ERDAL*, 2025, *forthcoming.*

[42] Art. 5(2). Art. 5(d) prohibits the use of *real time* biometric identification systems in spaces open to the public for law enforcement purposes, unless strictly necessary for the targeted search of potential victims of criminal actions, such as missing children, for the prevention of a specific, substantial and imminent danger to a person's life or safety or a terrorist attack, or, finally, for the detection, location or incrimination of a person suspected of crimes under Art. 2(2) of Council Framework Decision 2002/584 for which the member state concerned provides for a prison sentence of three years or more. Where facial recognition is intended to achieve these objectives, the draft regulation stipulates that the authority must consider the concrete situation, and in particular the severity, likelihood, and extent of the harm that would be caused by not using the identification system, and the consequences that the use of the identification system might have for the rights and freedoms of the persons involved. The individual use of facial recognition requires in any case, a prior authorization issued by the judicial authority or an independent administrative authority following a reasoned application and in accordance with national law.

which the limits to the exercise of power are set[43]. The system outlined by the Italian Constitution, places fundamental freedoms at the centre from which to conform and limit authoritative power. This adopted angle of view is emblematic of a broader choice in favour of a precise way of understanding the relationship between public powers and the citizen, even when it is the so-called *puissance publique*[44] that is exercised.

Compared to this model, the use of facial recognition, particularly by police forces or municipalities with a surveillance function in cities, seems to lead, by contrast, to a reversal of this setup with the risk of again placing some fundamental freedoms of individuals in a subordinate position.

Indeed, what was observed in the preceding paragraphs (§§ 3 and 4) offers a not very reassuring picture of algorithmic administrative power when it makes use of such intrusive technologies as facial recognition. A power that is opaque, less accountable, that presents accentuated characters of authoritativeness and unilateralism, and that indicates a clear imbalance in favour of the public administrations with reference to the relationship between "authority" and "freedom"[45].

This is aggravated by the increasingly broad delegation of decision-making to third parties (in some cases private parties) with respect to the public administration, to whom the latter entrusts the processing of the software[46] (not always fully transparent or knowable to the public

[43] See Articles 13, c. 3, 16, c. 1, 17, c. 3 and 21, c. 4 Const. On the subject, G. Corso, *L'ordine pubblico,* Bologna, Il Mulino, 1979, *passim.*

[44] A. Pubusa, *Riflessioni sulla pubblica amministrazione rileggendo la Costituzione,* in *Studi in onore di Feliciano Benvenuti*, VI, Mucchi Editore, 1996, pp. 1471 ss.; AA.VV., *Valori costituzionali e pubblica amministrazione*, 1993, *passim*; V. Allegretti, *Amministrazione pubblica e Costituzione*, Padova, Cedam, 1996, *passim.*

[45] Garante per la protezione dei dati personali, Opinion March 25, 2021 No. 127. According to the Garante, *Real time* facial recognition realizes large-scale automated processing that can affect, among others, those who are present at political and social events, which are not the subject of 'attention' by the police forces.

[46] This delegation can also be direct, as, for example, has happened in Australia, where the government has outsourced the power to issue certain benefits under *welfare* policies, without, among other things, complying with public evidence procedures. On the Australian case of the debit card (whereby benefits are loaded onto that card, which, however, cannot be used for certain purchases, e.g., alcohol or gambling, or in certain establishments) S. Tilley, *In the Name of 'Digital Inclusion': The true cost of the automation and privatization of Australia's social security system*, in *Social Alternatives*, vol. 39, 1, 2020, pp. 28 ff. The points criticized are compulsoriness, lack of consent, and decision-making based only on the use of data. According to the Author, the government is abdicating its responsibility for what citizens' needs are to be met, putting the choice back to the algorithm. This form of exercising power would also alter the very position of

authority) *de facto* outsourcing the care of the public interest. This generates important questions: the imputability[47] of the algorithmic administrative choice, its explicability and the responsibility[48] with regard to the decisions made. With respect to which, moreover, there is also the fear of a risk of flattening of the decision maker to the findings of the machine, which goes far beyond the subordination of the administrative decision to the technique[49].

In these cases, there is a risky "reintermediation" of public authority[50], realizing the eventuality whereby in discretionary activities the use of new technologies determines an "unconscious constraint" such that the decision is "not simply anticipated, but replaced by technique"[51].

The question then arises as to whether in the face of such risks and problems the choice initially followed by the Italian legislature which, it has been said, has banned the use of facial recognition systems[52] (as in many other non-EU legal systems[53]) should be endorsed, or, motivated by

welfare recipients, whom the A. defines as "actors necessarily conforming to the market". In this vein also M. Langford*, Taming the Digital Leviathan: Automated Decision-Making and International Human Rights*, AJIL Unbound, 114, p. 141-146 according to which "*The digital welfare state, unwittingly or not, provided a useful "neutral" cover for long-standing neoliberal policies that challenged the right to social security, whether by reducing welfare budgets, narrowing the beneficiary pool, or enhancing sanctions*".

[47] M.C. Cavallaro, *Imputazione e responsabilità delle decisioni automatizzate*, in *European Review of Digital Administration & Law – Erdal*, 2020, pp. 69 ff.

[48] See on this topic the interesting reflections on the increase of freedom at the expense of responsibility in the "digital society" carried out by L. Violante, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in *BioLaw Journal,* 2022, pp. 145 ff. On these issues already S. Del Gatto*, Potere algoritmico.,* cit., pp. 829 ff.

[49] S. Stacca, *Potere algoritmico. Profili organizzativi del rapporto tra amministrazione e automazione,* in *Dir. pubbl.,* 2024, pp. 365 ff.

[50] That is, the risk noted is that we are not simply witnessing the "cancellation of mediators" but a "discreet replacement of them". Thus L. Violante*, Diritto e potere.,* cit., 145 ff.

[51] The reference is again to S. Stacca*, Potere algoritmico.,* cit., pp. 365. See already A. Cassatella*, La discrezionalità amministrativa nell'età digitale*, in Scritti per F.G. Scoca, Napoli, E.S., 2020, pp. 681 ff. as also cited by S. Stacca.

[52] *See supra sub* note 20.

[53] In the United States, for example, some states have decided to ban facial recognition *tout court* or to introduce specific sectoral bans, for example, in schools or public housing. Facial recognition is banned, with specific reference to police functions, in Boston, San Francisco, Minneapolis, Oakland, and California. In the State of Maine, the law prohibits state, county, and municipal departments, employees, and officials from using or possessing facial recognition technology or entering into an agreement with a third

the positive benefits that such technology can determine in the performance of certain public functions and services[54], whether it would not be preferable to investigate the possibility of finding appropriate correctives capable of restoring a fair balance between public power and individual rights and freedoms when using facial recognition systems.

However, the solutions reviewed above do not seem satisfactory.

At the regulatory level, the AI Act leaves (too) wide discretion to member states on the law enforcement assumptions that allow the use of this technology. There is also evidence of excessive vagueness, too much leeway given to member states to implement the exception to the ban on remote facial recognition systems for law enforcement purposes, and a lack of adequate public oversight of the proposed standardization and self-assessment processes[55].

Insufficient, too, seem to be the safeguards, identified by case law and privacy authorities and linked to the granting of consent to the processing of biometric data: it is doubtful that consent can ever be considered freely given and therefore effective when there is such an imbalance of positions as that between public administration and the administered. "Voluntary" subjection to a surveillance system that makes use of facial recognition by a public authority translates in fact into opt-out adherence, lacking the real possibility for the individual to deny his or her consent[56].

party to obtain, access, or use facial recognition technology in most public areas, including schools, and for surveillance purposes. There is also a strict regulatory framework as to the specific ways in which law enforcement agencies can exploit the relevant technology for crime suppression and investigation.

[54] Also having in mind the reconstruction of Feliciano Benvenuti who observed that the justification of power is instrumentality to social utility and general interest. The duties of security police are directed to the service of the community and citizens by providing to enable individuals to live peacefully in the community and to act in it for the manifestation of their individuality and the satisfaction of their interests F. Benvenuti, *Appunti di diritto amministrativo*, *Parte generale*, cit., 183.

[55] The *summa divisio* made in the AI Act between low-risk and high-risk biometric systems does not seem, in general, entirely convincing, and the choice to give private companies themselves the task of assessing the compliance of the software produced with security and quality standards without public intervention, for example by an independent authority established ad hoc, raises strong concerns C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento in materia di intelligenza artificiale*, in *BioLaw Journal*, 3/2021; G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. informaz. e informat.,* 2022, pp. 303 ff.

[56] Significant in this regard are some cases that occurred in Sweden and France. With

Not very decisive is also the guarantee indicated by the Italian judge and now transposed into the new Italian law on artificial intelligence [57]of the so-called "reservation of humanity" or non-exclusivity of the algorithmic decision[58]. The reasons inherent in the criticality of the corrective offered by the so-called human in the loop lie in the very character of the algorithms used[59] whose functioning can be difficult to understand even for the programmers themselves[60]. Consequently, a serious problem of

reference to the latter, see the decision of the *Tribunal Administratif de Marseille*, Feb. 3, 2020, No. 1901249, available *online* at https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf.

[57] Article 14, L. n° 132/2025 on 'Use of artificial intelligence in public administration' establishes that public administrations shall use artificial intelligence for the purpose of increasing the efficiency of their activities, reducing the time required to complete procedures, and increasing the quality and quantity of services provided to citizens and businesses, ensuring that interested parties are aware of how it works and that its use is traceable. The use of artificial intelligence can only be allowed for an instrumental and supportive capacity to the decision-making process, respecting the autonomy and decision-making power of the person who, according to the provision referred to, remains solely responsible for the measures and procedures in which artificial intelligence has been used.

[58] Human involvement, so-called human in the loop, while not sufficient is considered a necessary element for the legitimacy of the use of facial recognition software by public authorities. For a definition of human in the loop, see the Ethical Guidelines for Trustworthy Artificial Intelligence, developed by the High-Level Panel on Artificial Intelligence, published in April 2019 and laid the foundation first for the AI White Paper and then for the *AI Act*. On this topic extensively G. Gallone, *Riserva di umanità e funzioni amministrative*, Padova, Cedam, 2023, *passim.* Also interesting is the analysis from a sociological perspective by B. Marchetti, *La garanzia dello Human in the loop alla prova della decisione amministrativa algoritmica*, in *Biolaw Journal*, 2021, pp. 367 ff.

[59] Reference is made to so-called *machine learning* algorithms and algorithms that generate predictive and decision-making *output* from their learning system. These are, in fact, algorithms that transform the huge amount of incoming data (even heterogeneous to each other and unstructured), into new information, generating correlations and predictive models not on the basis of a deductive logical process, but based on probabilities. In other words, the interweaving of data by these systems is able to learn by other means, what is not known directly. The prediction mechanism underlying machine learning can, however, realize discriminatory and stigmatizing effects: relying on time series, they work out a trend on which they make a prognostic judgment that tends to "freeze" pre-existing situations, with the consequence of perpetuating and exacerbating inequalities, regardless of the initial will of those of the programmer.

[60] G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza,* in *Pol. dir.*, 2019, p. 217; F.Z. Borgesius (ed.), *Discrimination, Artificial Intelligence, and Algorithmic Decision Making*, Council of Europe, Strasbourg,

transparency and comprehensibility of the assumptions of the "algorithmic decision" arises[61]. When the basis of the decision is an output produced by artificial intelligence software, as in the case of facial recognition, transparency, even in the strengthened version affirmed by the Council of State[62], risks offering only "a snapshot" of the functionality of the system[63], which favours "vision" to "understanding", significantly limiting the benefits attributable to its operation[64].

2018; Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability, Washington*, 2014, pp. 10 ff.; S. Del Gatto, *Potere algoritmico.,* cit., pp. 829 ff.

[61] On the black box character algorithms see F. Pasquale, *The black box society,* Harvard University Press, 2015 in which the A. points to a number of examples to support the thesis that while companies and institutions are increasingly subject to the "logic of secrecy," people's lives are increasingly transparent and open. Also on the subject is I.M. Delgado, *Automation, artificial intelligence and public administration: old conceptual categories for new problems?, Institutions of Federalism*, 3, 2019, pp. 643 ff. As noted by the A. with reference to self-learning systems, "[t]*he machine learning* possesses three well-known characteristics that distinguish it from other types of techniques: it is based on the use of algorithms that learn autonomously, these algorithms are *black box* in nature, and the system has the ability to produce results that could potentially exceed human prediction. The first relates to "explainability": if information is transformed into predictions through a *black box* in a way that is not fully knowable, how do we motivate the measure? […]". On the problem of transparency in AI systems and possible solutions also in light of the principles of the new Public Contracts Code, see E. Carloni, *Transparency within the artificial administration, principles, paths, perspectives and problems,* in *Italian Journal of Public Law*, 2024, pp. 8 ff.

[62] As noted by the administrative judge, "the use of computerized procedures cannot be a reason to circumvent the principles that conform our system and regulate the conduct of administrative activity". Cons. St., VI, Dec. 13, 2019, No. 8472, § 10. See also *Décision* n° 2018-765 DC, June 12, 2018 of the *Conseil Constitutionnel*, which recognized the legitimacy of the use of algorithms in administrative proceedings, provided that the full intelligibility of the algorithmic procedure is ensured and-if the decision is based on or concerns sensitive data-that the final decision is not fully automated. The importance of having an adequate discipline of algorithmic procedure has also been highlighted by C. Harlow, R. Rawlings*, Proceduralism and Automation: Challenges to the Values of Administrative Law*, in E. Fisher, J. King, A. Young (eds.), *The Foundations and Future of Public Law* (in honor of Paul Craig), LSE Legal Studies Working Paper No. 3/2019; J. Cobbe, *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making*, in *Legal Studies*, 39 (4).

[63] This is especially true for adaptive systems that learn as the amount and types of data they draw on increases, and for platforms with mobile interfaces, settings, features, and number of users.

[64] Doubts as to whether transparency in decisions using algorithms can be guaranteed have been raised by D. Runciman, *How Democracy Ends*, UK, 2018. According to the A., algorithms in decisions would prevent a balanced system of checks and balances and

In addition to transparency, the enhancement of two other typical principles of administrative law then appears important: the principle of legality and the principle of proportionality. While respecting the principle of legality to be understood, as suggested by the Italian GPDP, in a strict way and to be scrutinized in "qualitative" terms, the use of facial recognition by the public administration should always be based on an *ad hoc* legal basis. Therefore, a generic provision allowing the public administration to use such technologies cannot be said to be sufficient, but it is necessary, because of the intrusiveness and characteristics of such tools, the existence of a detailed discipline[65] that does not merely attribute the power, leaving the administration free in the choice of means to exercise it, but that indicates with a high degree of detail the prerequisites for its exercise and formulates the limits to the exercise of discretion[66]. In the

offer only unidirectional transparency-that is, that of the administration that makes use of the algorithm-about the data subject. On the risks of achieving transparency that is "fuzzy" or in other respects harmful, P.B. de Laat, *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, *Philos. Technol.,* 31, 2018, p. 525.

[65] This is also the direction taken by the Personal Data Protection Authority, which has deemed the SARI *real time* tool illegitimate because it is used in the absence of an adequate legal basis. According to what the Data Protection Authority said, the implementing decree of the Personal Data Protection Code regarding the processing of data carried out for public security purposes by police organs, offices and commands cannot be considered an adequate and sufficient legal basis because it lacks the degree of detail necessary to meet the need for predictability that is fundamental when police use real-time facial recognition technologies. In the decree referred to by the Guarantor there is in fact, only a specific regulation for the processing of data collected through video surveillance and photographic, audio and video recording systems, which, however, as noted by the Guarantor, are "ontologically different systems from those for biometric data processing". The importance of a regulatory prerequisite indicating in detail assumptions and limits was recently affirmed with reference to facial recognition technologies by the EDU Court, which affirmed the fundamental importance-when using such technologies-of having sufficiently detailed rules governing the scope and application of the measures taken and, at the same time, strong safeguards against the well-founded risk of possible abuse. See ECHR, III, July 4, 2023, Case 11519/20, *Glukhin v. Russia.*

[66] One of the first cases of police use of facial recognition technologies to come under judicial review is that of the Wales Police. The Court of Appeal has overturned the decision of the lower courts, which had declared the actions of the Welsh Police to be lawful. According to the Royal Courts of Justice, the use of AFR technology, violates Article 8 of the ECHR, which protects private and family life because the power exercised by the Welsh Police appears to lack a specific and sufficiently detailed legal basis and consequently such power would lack the requirements of "foreseeability, predictability, and hence of legality". The police who had made use of such technologies would, in the

narrow cases permitted, moreover, the use of facial recognition should always be preceded by a scrutiny of compliance with the principle of proportionality. The mere, albeit essential, presence of a public interest that, screened by the legislature, allows the use of a video surveillance system with facial recognition software is, in fact, insufficient if not accompanied by a judgment on the proportionality of the measure, in particular, on its tolerability (also called "proportionality in the strict sense"). This element (which together with those of suitability and necessity concurs to fill with content the principle of proportionality), often little investigated in the judgments of the administrative judge, in this case should have instead, a central role.

However, in the face of the rapid evolution of new technologies even these correctives may not be sufficient making it necessary to identify an insurmountable limit, an intangible core of rights that benefits from an absolute protection against intrusion by public administration[67], in order to ensure a fair relationship between "authority" and "freedom" put at risk by the use of some technologies considered too intrusive.

Court's view, have enjoyed an "*impermissibly wide*" discretion due to the lack of an adequate legal basis. Royal Courts of Justice Strand, London, WC2A 2LL, August 11, 2020, available *online* at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. On the matter see B. Davies, M. Innes and A. Dawson, *An Evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, September 2018.

[67] The existence of intangible core of private life (*Kernbereich privater Lebensgestaltung*) as an insurmountable limit in the face of certain public interference was affirmed by the German Constitutional Court in 2016, which declared the illegality of state-of-the-art covert surveillance tools used in the context of counterterrorism. *Bundesverfassungsgericht*, April 20, 2016, 1 BvR 966/09 and 1 BvR 1140/09, at www.bundesverfassungsgericht.de. According to the court, the more substantial the measure's interference in an individual's private life, the more stringent the legal requirements for its implementation must be. For the judges, a relationship of direct proportionality between the degree of intrusiveness of the measure and the level of intensity of the legal safeguards must, in essence, be affirmed. See paras 105 and 108 of the judgment.