PENALISTI ASSOCIATI
STUDIO BLENGINO

AVV. CARLO BLENGINO
AVV. FILIPPO PERLO

AVV. ERNESTINA SACCHETTO

AVV. ERNESTINA SACCHETTO
sacchetto@penalistiassociati.it
ernestinasacchetto@pec.ordineavvocatitorino.it

To Capable Srl
Via Sacra di San Michele 101
10093 Collegno (TO)
PEO: rachele.didero@gmail.com

Turin, March 6th 2023

Legal Opinion on the Production, Marketing and Use of Knitted Garments that inhibit Automated Facial Recognition Tools under the European and Italian legal framework*[1]

LEGAL ISSUE

CAPABLE Srl (“C” collaboration; “A” awareness; “P” people), hereinafter CAPABLE, is a “benefit” Srl company (law No 208/2015)[2] operating as an innovative start-up within the design, sustainability, education and innovation sector.

The first CAPABLE’s project arose from a deep reflection on the increasingly widespread use of automated facial recognition tools[3]. This technology, based on the automated

[1] Translation by Avv. Ernestina Sacchetto from the legal opinion provided by Avv. Carlo Blengino, Avv. Filippo Perlo and Avv. Ernestina Sacchetto on January 12th 2023.

[2] CAPABLE Srl, Registro delle Imprese di Torino No 12726880011, head office in Collegno (TO), via Sacra di San Michele 101, 10093, as extracted from Registro delle Imprese di Torino on 8.7.2022.

[3] Facial recognition technology allows the automated identification of an individual, comparing two or more faces. This is possible by detecting and measuring several facial features, extracting these from the image and, in a second step, comparing them with features taken from other faces. From a picture or a video, it is possible to extract the facial features, generating the electronic template of a specific trait, which will be the subject of an automated comparison with another template or digital image, previously recorded. The software could be used in "static" (or ex post) or in "dynamic" (or real-time) modality. In the first case, the software compares an acquired image of a face with the profiles contained in databases of different sizes. In

comparison of digitized faces, is highly controversial, both on a technical level, due to the still uncertain reliability of results and eventual biases, and, on a political level, due to the high risks of the mass surveillance phenomenon and the potential violation of several fundamental rights of citizens.

CAPABLE's project consists in the transposition, on a particular type of polychrome fabric, of an "adversarial" image preventing the functioning of facial recognition tools. The aim is to raise awareness about several risks for fundamental rights involved with the use of facial recognition technologies.

More in detail, the garment reproduces the so-called "adversarial patches", able to "confuse" the algorithm from facial detection, in an imperceptible way for human eyes.

The main project's result is the production of various prototypes, part of the Manifesto collection. These garments reproduce "adversarial patches" generating a specific reaction to automated tools in "real-time" modality and preventing facial recognition. In this way, the subject's biometric data are not detected or extracted.

After several tests conducted at the Politecnico di Milano and at the Shenkar College of Engineering, Design and Art in Tel Aviv, the patent "*Method for Manufacturing a Knitted Fabric reproducing an adversarial image*" was registered with the patronage of Politecnico di Milano

One of the aims is the marketing of garments with these adversarial features. Due to the scientific and practical results obtained until now, the founders are thinking about new original applications in the field of design and computer science. In particular, one of the

the second hypothesis, the software examines "live" streams from cameras, selecting the "facial footprints" of the subjects, and finally searching for a match between them and the faces contained in a source archive. From 1970s, the discipline of computer vision has made relevant steps forward, enabling the development of sophisticated techniques for extracting information from images and thus giving strength to specialized study in the field of facial recognition. The availability of "big data" and the development of advanced algorithms allowed the exponential development of applications in the field of identification, authentication and categorization using biometric data.

main goals is to test this particular technique on different product categories, in order to extend the market for these products.

In general, facial recognition technologies and related applications have legitimate uses in several sectors. In particular, these tools are useful for law enforcement agencies.

This opinion addresses the legal issues, which may arise with the production, marketing and use of adversarial knitted garments for the functioning of facial recognition software. This legal opinion is on the production, commercialization and use of tools that guarantee anonymity with respect to a specific digital technology and prevent the extraction of personal data.

It should be clarified that, in order to raise awareness and stimulate the debate on the legitimate use of facial recognition technology, these knitted garments have been designed as reversible, without, in one side, the adversarial features that inhibit the operations of the software.

THE CONSTITUTIONAL BACKGROUND

The digital revolution and the "datafication" of our lives, constantly captured by digital devices, generated new kind of rights, i.e. the right of the protection of personal data, introduced as a fundamental right in Europe in 2011, creating new ways of exercising fundamental rights arose in a "pre-digital" scenario.

The right to protect data of natural persons and, more in general, the right to privacy[4] have assumed new shades generated by the intrusiveness of new technologies.

The Italian Constitution establishes the principle of confidentiality of communication and correspondence, while the supranational Charters of fundamental rights recall crucial principles that, at the state of the art, allow to make individual freedoms effective

[4] The right to privacy, having acquired the meaning of the right to data protection, is the right "to be alone": born in Boston, in the late 1800s, from the reflections of Warren and Brandeis with regard to the new technology of instant cameras created by Kodak, which - for the first time - allowed capturing the image of a person unconsciously.

and to trace the limits and conditions of eventual violations or interferences, in particular from the public authorities.

The right to privacy and the right to data protection derive directly from the art. 8 of the ECHR[5] and the art. 7, 8 of the Charter of Fundamental Rights of the European Union (Nice Charter)[6].

The right to respect for private life, established in the art. 8 ECHR and art. 7 of the EU Charter of Fundamental Rights, may be subject to a State interference only if there is an official legal measure providing for it, in specific hypothesis, and only if such interference is necessary, in a democratic society, for certain purposes, in compliance with the principles of necessity and proportionality[7]. In this way, the respect for private life is the prerequisite for the exercise of several rights, particularly the freedom of expression, movement, or assembly.

The right to data protection (art. 8 EU Charter) establishes that the treatment of automated decision-making is necessarily ruled by the principle of strict purpose based on an explicit consent or other legal basis.

Again, the protection for personal data provides certain rules for the correct exercise of several human rights, particularly when the legislation places strict preconditions for the

[5] Article 8 ECHR: "Right to respect for private and family life. 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

[6] Article 7 Charter of Fundamental Rights of the European Union: "Respect for private and family life. Everyone has the right to respect for his or her private and family life, home and communications. Article 8 Charter of fundamental rights of the European Union: Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".

[7] Article 52 of the Charter of Fundamental Rights of the European Union lays down such limits where it specifies that: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

processing of biometric data or when the processing is part of automated decision-making, such as profiling.

The constitutional guarantees balance each other in our hyper-connected society where several digital technologies actually produce and store information and personal data potentially subject of abuses.

Several digital technologies have generated exceptional and innovative forms of interferences into private lives by the States, whose need of information is related to the sovereign power. At the same time, these technologies offer legitimate solutions for the protection of fundamental rights, particularly for the protection of personal data.

Using technology preventing the capture of personal data and confidential information corresponds to the legitimate and clear exercise of fundamental rights in compliance with the EU legal provisions.

As Bobbio wrote, all freedoms arise from a non-freedom[8]; there is no freedom forever won, and history is a continuous rotation of freedom and oppression, of new freedoms as a reaction to new oppressions.

An end-to-end encryption system in communications is the actual expression of the exercise of the fundamental right to confidentiality of communications (art. 15 Italian Const.), even if it prevents legitimate interception by the judiciary power. Using antivirus or ad blocker is the expression of the right to privacy and computer domicile, even if it prevents requests of legitimate malware interception by the sovereign power.

Similar conclusions could be made with regard to CAPABLE technology.

It is therefore appropriate to elaborate further the issue and to address the much-discussed subject of facial recognition technology and its many applications.

THE EUROPEAN LEGAL FRAMEWORK

The automated face-based human recognition technology could be used for several applications and scopes. When employed in "authentication" or "verification" modality, the automated facial recognition software provides with "one-to-one" comparison and recognition with a previous consent for the treatment of biometric data (e.g. the

[8] N. Bobbio, Eguaglianza e libertà, Einaudi, 2009.

authentication through the most advanced smartphones)[9]. The use of biometric authentication is usually based on an express consent.

On the contrary, the use of automated facial recognition systems for "identification" and/or "categorization" purposes[10], both in "real time" or "post" modalities [11], raise doubts and concerns about the potential risks for fundamental rights. In particular, through the "identification" modality it is possible to perform a "one-to-many" comparison, in which the image captured is compared with all those present in a reference database. "Categorization", on the other hand, provides the extraction of general characteristics of an individual, in order to elaborate classifications with respect to certain reference categories (e.g., age, sex, gender, ethnic origin, humour, consumption habits, etc.). This application is generally part of a profiling process.

With regard to these latest modalities of facial recognition technologies, a specific attention is paid in Europe, where there is an effective necessity to investigate and prevent the potential violations of fundamental rights. In particular, the constant automated treatment of personal biometric data, inevitably risk becoming an unacceptable mass surveillance activity, showing also even serious discriminatory effects, particularly for ethnic groups and certain categories of individuals.

[9] "Authentication" or "verification" of data is the comparison between two images in a "one-to-one" modality. More in detail, the system verifies the analysed image matches another one stored within the same repository. An example of 1:1 comparison is employed to access an electronic device (smartphone) or a physical location (e.g., a bank).

[10] From a biometric-forensic perspective, through "identification" it is possible to perform a "one-to-many" comparison, by which the image is compared with all those contained in a reference database. For example, this modality is used for investigative purposes by law enforcement authorities to determine the identity of a particular unknown person. "Categorization", on the other hand, refers to the activity of extracting the general characteristics of an individual in order to develop classifications with respect to certain reference categories (e.g., age, sex, gender, ethnic background, mood, consumption habits, etc.).

[11] Article 3, paras. 37 and 38 of the Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence, COM/2021/206 final, defines: "'real-time' remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention. 'post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system".

With regard to the protection of personal data mentioned in the previous paragraph, with Regulation (EU) 2016/679 (the so-called RGPD) the European Union introduced a strict protection for the treatment of biometric data, establishing special requirements aimed at protecting data subjects from unlawful treatments[12].

Article 4(14) defines "biometric data" as «personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data»[13].

Both the "digitized" representation of a face and the template, considered as its vector representation, fall within the definition of this "particular category of personal data", in respect with the RGPD. Article 9(1) establishes a general ban for the processing of genetic and biometric data, unless the controller has given the consent[14].

The Directive 2016/680/EU "on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", authorizes the treatment of biometric data only if strictly necessary, in compliance with appropriate safeguards for the rights and freedoms of data subject and only if: a) authorized by Union or Member State law; b) in order to safeguard a vital interest of the data subject or another natural person; or c) if the said processing relates to data manifestly made public by the data subject.

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

[13] The same definition is in the Directive 2016/680/EU of the European Parliament and of the Council of 4/27/2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data, and by Italian Legislative Decree No. 51 of 5/18/2018.

[14] The treatment is also considered legitimate if it takes place for labour and social security purposes; when it is necessary to protect a vital interest; for the achievement of the purposes of foundations, associations or other non-profit bodies; if the particular personal data are manifestly made public by the person concerned; it is then allowed to process these data for the performance of defensive and investigative activities, for the achievement of a relevant public interest, and for the achievement of statistical and scientific purposes.

In this context, the European Agency for Fundamental Rights recently remarked that «*the rights to respect for private life and data protection are central to the deployment of facial recognition technology*»[15]. For both application modalities of facial recognition systems ("ex post" or "real-time"), taking into account their ability to «*collecting, comparing and/or storing facial images in an IT system for identification purposes*», is recognizable «*an interference with the right to protection of personal data set out in Article 8 of the Charter (embodying pre-existing EU data protection law) and the right to private life under Article 7 of the Charter and Article 8 of the ECHR*»[16].

Facial recognition systems, being able to extract «*of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances*»[17], can process information with an «*"intrinsically private" character that is not reduced because, for example, "the biometric data is derived from a person's facial features that are "manifest in public"*»[18].

With regard to "real time" modality, the European Union Agency for Fundamental Rights[19] reminds that the risks for individuals under surveillance are those to «*change their behaviour, withdrawing from social life, not visiting central places under surveillance, avoiding train stations or declining to attend cultural, social or sports events*»[20].

[15] European Union Agency For Fundamental Rights, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 23, available at https://fra.europa.eu/en/publication/2019/facial-recognition. European Parliamentary Research Service**,** *Regulating facial recognition in the EU*, September 2021, p. 10, establishes that «*FRT implies the processing of data for the purpose of identification, it constitutes an interference with the right to data protection, as set out in Article 8 CFR and the right to private life under Article 7 CFR*».

[16] European Union Agency For Fundamental Rights, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 23.

[17] High Court of Justice*, Queen's Bench Division, Divisional Court*, [2019] EWHC 2341 (Admin), § 57.

[18] [2019] EWHC 2341 (Admin), § 57.

[19] European Union Agency For Fundamental Rights, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 27.11.2019, pp. 29 e ss., available at https://fra.europa.eu/en/publication/2019/facial-recognition.

[20] European Union Agency For Fundamental Rights, *FRA Focus. Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 20.

For this reason, the European Commission, before with White Paper[21], and later, with the proposal for a Regulation «*on a European approach for Artificial Intelligence*» (*Artificial Intelligence Act*)[22], highlighted the risks of the use of remote biometric identification systems used in public spaces because they potentially affect fundamental rights. In the proposal, "real-time" and "post" remote biometric identification systems are classified as "high risk" for their potential to generate harm to the health, safety and fundamental rights of individuals, since the «*technical inaccuracies (...) can lead to biased results and result in discriminatory effects*»[23].

The use of remote biometric identification systems, in publicly accessible spaces, for law enforcement purposes is considered particularly intrusive for the rights as far as it could affect the private lives, make citizens feel constantly under surveillance, and indirectly discourage the exercise of freedom of assembly and other fundamental rights.

So, according with the proposal, the use of "real time" biometric identification systems by law enforcement authorities, in publicly accessible spaces, is prohibited, with few exceptional hypotheses[24].

The use of “post” remote biometric identification systems would be allowed when several mandatory requirements are satisfied, in order to ensure that such tools «*do not present unacceptable risks to important public interests of the Union, as recognized and protected by Union law*»[25].

[21] WHITE PAPER on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065&from=EN.

[22] Proposal for a Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence, COM/2021/206 final, available at https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206.

[23] See recital No. 33, 2021/0106(COD).

[24] Article 5, par. 1, lett. d) specifies: “(i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State”.

[25] See recital No. 27, 2021/0106(COD).

Once obtained the certification, the system could circulate in the market, but it remains that any processing of biometric data or other personal data, affected by the use of AI systems for biometric identification purposes, should continue to be compliant with all requirements of article 9(1) of the Regulation (EU) 2016/679, article 10(1) of the Regulation (EU) 2018/1725 and article 10 of the Directive (EU) 2016/680[26].

According with the proposal, the remote biometric identification systems for categorization purposes are defined as AI tools «*assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data*»[27].

Since they are not classified as "high-risk" systems, they should be in compliance with only transparency rules concerning the information to be provided to individuals who are exposed to the system. However, the use of biometric categorization systems in publicly accessible spaces could have an equal negative impact on the fundamental rights of individuals.

In this regard, these systems could be used by law enforcement authorities to «*classify people in public places as of a certain ethnicity or political orientation*», because «*they are under no obligation to include human oversight, or to notify people that the system is in use*»[28].

In this regard, the European Data Protection Supervisor (EDPS) argues that a more strict approach should be followed in order to protect the use of automated recognition, in publicly accessible spaces, regardless the application in a commercial, administrative, or law enforcement context[29].

For this reason, the European Data Protection Supervisor, together with the European Data Protection Board (EDPB), proposed a «*general ban on any use of AI for an*

[26] See recital No. 24, 2021/0106 (COD).

[27] See art. 3, par. 35, 2021/0106 (COD).

[28] C. Kind, "*Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics*", in *Ada Lovelace Institute*, 2021, available at https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/.

[29] European Data Protection Supervisor, *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*, 2021, available at https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context»[30], because the «*problem regarding the way to properly inform individuals about this processing is still unsolved*»[31]. Furthermore, «*the intrusiveness of the processing does not always depend on the identification being done in real-time or not. Post remote biometric identification in the context of a political protest is likely to have a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy. Second, the intrusiveness of the processing does not necessarily depend on its purpose. The use of this system for other purposes such as private security represents the same threats to the fundamental rights of respect for private and family life and protection of personal data*»[32].

In this scenario, most recently, the European Parliament, with the Resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, called for a moratorium on the use of facial recognition systems for law enforcement purposes «*until the technical standards can be considered fully fundamental rights compliant, results derived are non-biased and non-discriminatory, the legal framework provides strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence of the necessity and proportionality for the deployment of such technologies*»[33].

In other words, regardless the actors/users involved and its more or less legitimate purposes, facial recognition technology is potentially very intrusive and able to cause interferences and violations of several fundamental rights. This assumption is crucial for the evaluation of the legitimacy of any solution, including technological ones, aimed at

[30] EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, p. 3, available at https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

[31] EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, p. 12.

[32] EDPB – EDPS, *Joint opinion 5/2021*, 18.6.2021, p. 12.

[33] «[…] *unless strictly used for the purpose of identification of victims of crime*». European Parliament resolution of October 6th 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

exercising, preserving and protecting the same rights of the person subject to potential violations.

ITALIAN LEGAL FRAMEWORK

Italy, trying to be in compliance with the abovementioned European principles, shows a legal framework characterized by uncertainty.

With the aim to restrict the use of facial recognition software in compliance with the European regulatory approach, the Decree-Law No 139/2021 (so-called "Capienze") called for a moratorium in order to suspend the use of facial recognition systems in public places or open to the public, by both public and private entities, with the exception of law enforcement purposes, which will still be subject to a positive opinion of the Italian Data Protection Authority[34].

The provision, on the one hand, prohibits until December 2023, the use of automated facial recognition; on the other hand, it excludes from the moratorium certain specific purposes as well as the use of this technology by the judicial authority[35].

The unlucky formulation of this provision generated several interpretative doubts, as it has been misread as a kind of an authorization for uses excluded by the moratorium.

[34] Art. 1 co. 9, D.L. No 139/2021: "9. In considerazione di quanto disposto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nonché dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dell'esigenza di disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale, nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea, l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici di cui all'articolo 4, numero 14), del citato regolamento (UE) 2016/679 in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023. (...)"

[35] Paragraphs 9, 10, and 11 do not apply to the treatments processed by law enforcement authorities after the positive opinion of the Authority in accordance with Article 24, paragraph 1, letter b), of the same Legislative Decree No. 51 of 2018. If the same activity is carried out by a judicial authority in the exercise of judicial functions as well as judicial functions of the public prosecutor, the treatment of personal data is allowed without a mandatory positive opinion by the Italian data protection Authority.

However, the provision must be read in light of a recent opinion given by the Italian Data Protection Authority, who considered non-compliant with the RGDP, the Ministry of the Interior's Automatic Image Recognition System (S.A.R.I.)[36], applied in "real time"[37], for the clear violation of the regulation to protect personal data.

According to the Italian Data Protection Authority opinion, the "real-time" modality represents a systematic mass surveillance activity that allows to process and to treat, without an appropriate legal basis[38], the digital representations of faces of a multitude of citizens in order to compare them with a watch list of subjects[39].

Beyond the interpretative issues of L.D. No 139/2021 - which can hardly be considered a valid legal basis - it seems clear that even in our legal system the use of a technology based on the automated comparison of faces for "identification" purposes ("one to many" comparison), particularly in "real time", must be qualified as illegitimate. In the absence of a consent and a suitable legal basis, it represents an inevitable and unjustified

[36] No. 127, March 25th 2021.

[37] The "real time" modality allows automated real-time analysis of faces captured in multiple live video streams from cameras installed in the same geographical area. The faces in the frames of the different video streams are compared using a recognition algorithm that draws the elements of comparison from a database whose size is approximately hundreds of thousands of images. Once the frame is captured, the software "reviews" at very high speed the images held in the archive looking for a match. At the end of this activity, the algorithm returns a list of profiles ordered according to a probability score based on similarity to the image of the subject to be identified. The match of the unknown face with the filed face is made known to the operator by an alert signal generated by the algorithm. If the search does not generate any alert, the image remains stored within the SARI platform so that any future matches can be flagged, thereby increasing the possibility of next matches. At the end, for both program application modes, the result will be analysed by the specialized operators of the forensic police in order to verify the outcome processed by the automatic system.

[38] The Italian Data Protection Authority, with a previous opinion on the application modality of SARI "real time", analysing the relevant legal provisions (i.e. Italian Code of Criminal Procedure, Presidential Decree No 15, 15.1.2018), established that it was not possible to identify any legal basis, pursuant to Article 7 of Italian Legislative Decree No. 51/2018, in order to allow the processing of biometric data aimed at the identification in "live" mode.

[39] See GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere sulla valutazione di impatto del Ministero dell'Interno relativo ad un sistema di telecamere indossabili (body-cam), da Reparti mobili della Polizia di Stato, per la documentazione audio e video di situazioni critiche per l'ordine e la sicurezza, in occasione di eventi , manifestazioni pubbliche*, 22.7.2021, p. 7, available at https://www.asaps.it/downloads/files/Garante%20Privacy%20provvedimento%20bodycam%20Polizia%20di%20Stato%20luglio%202021.pdf, in which the Authority established that these tools could not be used for the «*identificazione univoca […] o autenticazione di una persona fisica (facial recognition)*».

interference in the private life of citizens and a violation for unlawful treatments of the protection of personal data.

There could be not an obligation in the Italian and European regulation to be subjected to an automated biometric identification system, such as facial recognition technology, for the use of which, even by law enforcement authorities, there are not clear prohibitions but certainly great uncertainties and considerable caution.

Furthermore, even if - in the next future - the use of this specific technology were regulated and authorized for specific purposes, a mandatory and pervasive automated identification of persons could not derive from this provision.

This hypothetical obligation or an eventual ban on wearing clothes as CAPABLE's, would be, in the declared and institutionalized practice of mass surveillance, a transformation of our democratic societies into the most classic of nightmares in dystopian literature.

*

The same conclusions could be reached analysing the Italian legislation on the verification of identity by judicial or public security authorities.

With regard to articles 495, 496 and 651 of the Italian Criminal Code, law enforcement and judicial authorities must be able to identify citizens by providing information about his or her personal identity, status or other personal qualities.

Article 495-ter of the Italian Criminal Code punishes who, in order to avoid his or her own or others' identification, modifies parts of his or her own or others' body useful to determine the identity or other personal qualities.

These provisions assign to public authorities a legitimacy to identify an individual in order to exercise his or her office: there is a formal obligation to be identified just with a request of the public authority.

In any case, this obligation is completely apart from the hidden, non-consensual and automated identification performed by facial recognition technologies.

The legal framework arose during the Italian terrorism period and the fascist period is more complex and apparently insidious. The so-called “police-laws” prohibit wearing masks in public spaces[40], e.g. protective helmets or any other means to make it difficult for a person to be recognized, in a public place or open to public, without a formal reason[41].

These provisions, dating back to Italian fascist period (1931) and the emergency legislation of terrorism (1975), cannot be applied to the different circumstances of this legal opinion and with regard to a specific identification technique.

People wearing CAPABLE are clearly recognizable and identifiable, in compliance with all the above-mentioned provisions regarding the proper identifiability of citizens by law enforcement authorities[42]: the last scope is just to avoid a specific intrusive technology, which represents a potential violation to the protection of personal data.

A broad interpretation of these provisions would imply a generalized obligation to submit to facial recognition technologies, for identification and categorization purposes; this approach would be clearly in conflict with Articles 7, 8 and 52 of the EU Charter of fundamental rights and Article 8 of ECHR.

FINAL REMARKS

- In conclusion, the production, marketing and use of CAPABLE's adversarial garments does not seem - at present - to be in conflict with any European and Italian legal provisions. There is not, and it should not be, in compliance with the current constitutional legal framework, a general duty for citizens freely circulating in public spaces or open to the public, to be subjected indiscriminately to the capture of their biometric data by automated facial recognition tools.

- The use of CAPABLE products constitutes the legitimate exercise of constitutionally protected fundamental rights in most democratic countries.

[40] Art. 85, R.D. no. 773/1931.

[41] Art. 5, Law No. 22.5.1975, n. 152

[42] Of course, people wearing CAPABLE do not intend to refuse or decline their identity if expressly prescribed by the law.

- CAPABLE's technology helps to safeguard privacy and the protection of personal data, defending citizens who choose to wear its garments from abuse and unlawful intrusion into the individual's life.

- Regarding the marketing, it should be clarified that a garment that shields facial recognition software does not fall into any of the categories set forth in the Regulation (EU) 2021/821 on "*for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*".