1 Facial Recognition Technology (FRT) in compliance with GDPR 2018 EU 2016

FRT is not some kind of a science work of fiction. Neither it is a technical wonder for next year nor a big threat. FRT is considered to be the reality of today that has been emerged as coherent evolution of something fascinating with the camera technology as well as the CCTV systems. Similar to the use of other hi-tech evolutions, FRT can also be used for both good or evil purposes. Keeping this in view, it would be unfair and misleading to overlook and flout the insinuation of this technology over society's privacy on the whole. Therefore, it is necessary to have some significant insights about ensuring the use of FR technology to comply with the GDPR.

Around the whole globe, several efforts have been made to implement the FRT into the majority of the public in a conventional way, but there remains a binding question that is it lawful to deploy this technological evolution in public? To put it another way, is it possible to make the exploitation of FRT in compliance with the "General Data Protection Regulation (GDPR) (EU 2016/679)"?

To begin with the groundwork, it is prominently known that the data taken or apprehended using the FR technology, that makes the companies and organizations detect and evaluate the particular person within the crowd, is the personal and private data of that individual. The thing that makes it more intricate from the perspective of GDPR is the same data that is considered to be eligible or licensed to be used as "biometric data" intending to specifically identify and recognize the actual person. As an outcome, FRT in its true essence will have the ability to fascinate and appeal the application of all the regime applying to distinctive categories of individual's private data.

This simply means that under the framework of EU data security regulations, the utilization of FRT is possible only or should be considered lawful if, at the minimum, one of all the existing legal bases fulfills the requirement. Besides this, one of the exceptions from the extensive interdiction affecting the handling of exclusive categories of private data or information applies. Since with the enormous majority of circumstances, where the utilization or the exploitation of private data is not directly involved to make interaction with the person, the most suitable and appropriate 'legal basis' to count on would be lawful and authentic interest ground. Stated otherwise, lest the implementation of FRT is to make an interaction directly with the person along with their information, for instance, to give the right to access the premises or make some kind of actions, neither the consent nor permission nor the contractual necessity, would be appropriate legal bases.

To count on the legitimate grounds, it is very essential for the system regulator to keenly observe and evaluate the person's preferred expectations i.e., what a person will preferably suppose or assume at the time of gathering its personal and private data. Considering more technically, it includes the process of

going through the assessment of lawful interests, that would look for the use of FRT to attain the desired purpose, and also to suggest some possible measures to curtail the intrinsic privacy imposition that FRT involves. It must be expected from the regulators to set a considerably high bar particularly focusing on setting out the range of liability measures visualized by GDPR.

Even though the use of FRT has incredibly increased from the past few years not only in public authorities but also in private organizations, but this, eventually, has flickered a forceful debate regarding its impact on ultimate human rights. The use of FRT along with surveillance CCTV cameras has led to pop-up several concerns about violations of fundamental rights. The threat of error in matching faces is considered to be the most outstretched concern regarding fundamental rights. These affected fundamental rights may involve, human dignity, respect for someone's personal life, data protection and security, non-discrimination, rights for those having disabilities, freedom of speech and expression as well as the right to a fair trial, effective remedy, and good administration.

2 FRT: Evaluating the risks of false identification

It might be a challenging task to determine the accuracy of FR software, depending upon the context, and purpose of its use. When this technology is implemented in places where millions of people visit on daily basis, for instance, airports, train or bus stations, the technical error even for a small portion makes hundreds of people to be wrongly identified.

Several ways are there to compute and analyze the error rates, therefore, it is necessary to avoid this kind of certain risk. Moreover, in terms of accuracy as well as errors, there arises a question regarding the possibility of the FR system being trapped, for instance, false face images are also known as spoofing, are considered to be imported specially for law enforcement.

FRT, similar to other AI and ML algorithms, represents binary outcomes, which means that there exist two possible outcomes. Hence, it might be helpful to differentiate among the "false positives and false negatives":

'False positive' is the condition where the image is matched with another image wrongly. As per the context of law enforcement, this false matching phenomenon means that the person is erroneously identified as another human being by the FRT system. This can lead to significant concerns regarding the fundamental rights of that individual. The "false identification rate" contributes greatly to the number of inaccurately identified matches. For instance, no. of individuals over the watch list being wrongly identified that are not present on the watch list.

False negatives, on the contrary, are those who are not supposed to be matched because of not being present over the watch list but makes the matches. The “false negative identification rate” or considerably “miss rate” shows the amount of mistakenly not recognized among the ones that must be identified.

The challenges of both false positives and negatives are also linked to data processing accuracy as well as data quality. Addressing these issues needs a consistent correction and apprising of facial data and images to be stored in the watch list to certify the precise data processing.

Under Article 9(1) of GDPR, the biometric data establishes a “special category data”, whose data processing is not allowed until at least one of various explicit exceptions are implemented. Yet, not all the gathered data making use of FRT would be considered as “special category data”: Article 9(1) explicitly explains that biometric data will be taken under this term only it would be used to exclusively identify an individual. For instance, if FRT is utilized to identify that the person is either male or female, it may not certainly identify a person and would fall outside the range of “special category data”.

3 Key Principles for Implementing FRT under EU Legal Framework

While processing the personal and private data of the individual, some fundamental principles should be adhered to regarding the data protection stated under Article 5 of GDPR. These key principles of implementing FRT technology are as follows:

3.1 Purpose Limitation

It is necessary to collect the data with the individual’s consent. The data should be gathered for exclusive, explicit, and legal purposes and that must be defined at the time of collecting it from the person.

3.2 Data Transparency

Confirming the explicitness and comprehensibility facilitates the compliance with the principle of transparency, which further indulges the data regulator and controller to deliver the information as well as a data subject with clear info related to the data processing is the clear, comprehensible, and concise format, forming a legitimate data processing notice. The provision of ample notices can pretense a key challenge in terms of using FRT. For instance, persons may already be in the zone of FRT-enabled camera devices earlier before being aware of implications and signage.

3.3 Data Minimization

The principle of data minimization needs the data regulators to gather the least possible amount of information and data that is necessarily required for distinct purposes. In addition to that, the data processing should be stabled against the moralities and privileges of the data subject.

3.4 Data Protection and Security

Suitable procedural and organizational data security processes must be in a position to make sure that the data security is attained and acquired by implementing the FRT-based technological solutions. Here, describing the appropriateness that is required to assess several measures involves the scope, nature, purpose, and context of data processing, along with the risk and threat of varying severity and likelihood of rights as well as freedom of an individual. In several FRT-based techniques, fulfilling all the standards requires a high investment in data protection and security.

3.5 Non-automated Decision Making

Article 22 of GDPR provides the data subjects all the rights not to be incidental to decisions that are completely based on automated processing of FRT solutions i.e., without involving human interference. However, it is allowed to prompt consent, if it is deliberately legalized by the law, or for purpose of ample public interest.

4 FRT deployment concerning Public Interest

The legal basis for the public interest is more related to organizations that bring off the tasks as per the public interest. To solely depend on this, the data regulator should present that it is making efforts for officials regarding authority and mandatory powers. Furthermore, the responsibilities of the data regulators should be enacted by a member of the EU state's law. Although it is not mandatory to explicit the statutory provision, the tasks, responsibilities, functions as well as powers of the data controller must be accurately defined and should be clear. Thus, the ground of public interest becomes restricted to use for private companies. As per the "Irish Data protection commission (DPC)", public establishments, and the authorized individuals that are administered by public law, are the organizations that are most probably able to effectively depend on this public interest ground. This will involve the police that may use and implement FRT solutions to avoid and prevent the severity of the crime, or even the public authorities that may introduce the FRT technology and legalize it to access their amenities.

An official "Data Protection Impact Assessment (DPIA)" is essential to be fulfilled under Article 35 of GDPR in several situations where the data processing "is expected to result in a high risk to freedom and rights of natural persons", specifically when the technology of new data processing is being familiarized. The regulation issuance generated by the "European data protection board (EDPB)" particularly references the "groundbreaking utilization or implementation of novel technologies or the Hi-Tech solutions, such as merged use of FR and fingerprint for enhanced physical access control". If a greater risk to the data subject is analyzed by DPIA which may not be alleviated by the regulator, then the data protection authority and

supervisory of the related organization should be referred not only for GDPR but also the LAW Enforcement Directive purposes as well.

4.1 Legitimate Interest

This phenomenon provides the extent of flexibility for a private organization desiring to implement FRT, without relying on the public entities. This legitimate perspective might be counted on if the gathered data has not been categorized as "special category data". Reliance and dependence are provisional and restricted on stabilizing the recognized and classified lawful interests along with data subject interests. These legitimate interests enclosed within this aspect involve the interest of the controller as well as the third parties. It has considerably a larger scope, and DPC refers not only to the individual, commercial interests but also public and communal benefits. The article of GDPR regarding legitimate interest also recommends that it is probably to be present where there occurs a "relevant and appropriate relationship" among the controller as well as the data subject, for instance, among the client and the service provider. One thing that should be mentioned essentially, is that being dependent on legitimate interest, a vigilant assessment of this must be undertaken against the interest of data subjects, freedom as well as rights. This stable implementation must contemplate that if the data subject can probably expect that processing of its private data may happen for the use of legitimate interest. The example for this case would be the retailer who would cast off FRT solution for speeding up its payment processes.

4.2 Consent

Provided the restrictions applied over public and legitimate interest under GDPR, reliance on the consent is occurs to be the accurate legal basis for several private organizations that have implemented FRT. Dependence on consent is complex because of the practical complications in acquiring it and conditions that must be fulfilled to be lawfully valid. All of this may occur to be in contrast to several other regions of the world like Asia, where expressing the obvious consent is the vital requirement to validate the data collection, disclose and use it under several frameworks of data protection, and unlike in Europe, no challenging issues are there to prove consent has been given.

As stated in the data protection article of GDPR, it is necessary for the individual to express its consent using the statement "clear affirmative action" without any unambiguity. Hence, it can be said that consent should not be incidental or contingent on silence, pre-ticked boxes, or inactivity, rather it should be well informed and specified. The person or the individual must be familiarized with what they are compliant or consenting to. Most exclusively, "consent" should be "freely given". Smartphones are the perfect examples of freely given consent, that provide the availability to its features via FR technology. In smartphones, consent is necessarily desired by the person to use the face-scanning feature while unlocking the screen or other features like password protection feature, etc.

It is necessary to keep in mind that public and local authorities, including law enforcement entities and the police, cannot solely count on grounds of legitimate interest or consent at all for their data processing. In reality, law enforcement is taken as the subject to several distinct regimes completely under its directives of data security and protection, which provides the accountability for instituting the related situations to every member of the state. For instance, in the UK, police pursuing to utilize the FRT solution for law enforcement will require to validate the compulsion of this technology for the purpose of the task being performed.

To the degree that processing of the (biometric) data is concerned as a "special category" of private information, the accessibility of exemptions to general proscription is quite restricted in practical terms.

As far as the implementation and exploitation of FRT are concerned to be used as public safety measures, the only exemption would be that processing should be essential for causes of substantial and exclusive public interest. If the bar for lawful interest is high, then that of public interest is certainly higher as it stems from the law which is fair, and proportionate, as well as respects the crux of accessing the data in terms of its protection and safety and also provides the specific and suitable measures to protect the rights of the individuals.

Concerning the way GDPR relates to FRT, it is now clear that FRT is implemented under strict observations and is legal to implement. It is now unlikely that FRT would vanish or fade away from our cities or devices completely. However, the controllers of implementing this technology should take some proper security steps to make sure that FR and other alike technologies are compatible and adhering to law enforcement regulations. FRT complies with the GDPR, but concentrating on acquiring this in practical terms is crucial like ensuring the functionality and working operation of the technology.

5 References

[1]https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

[2] https://www.dataguidance.com/opinion/international-making-facial-recognition-gdpr

[3] https://www.avocats-mathias.com/actualites/facial-recognition

[4] https://www.datagovernance.org/files/research/NIPFP_Smriti_FRT_-_Paper_5.pdf

[5]https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

[6] https://www.dlapiper.com/en/asiapacific/insights/publications/2020/05/facial-recognition-technology/