PRIVACY NETWORK

OBSERVATIONS TO THE PUBLIC CONSULTATION OF EDPB GUIDELINES 05/2022 ON THE USE OF FACIAL RECOGNITION TECHNOLOGY IN THE AREA OF LAW ENFORCEMENT

COMMENTS PROVIDED BY PRIVACY NETWORK

Co-authored by:
Gabriele Ientile, Riccardo Apa, Eleonora Bonel & Teresa Rizzi

TABLE OF CONTENT

1. BACKGROUND

Privacy Network is a leading Italian non-profit organisation promoting digital and fundamental rights related to technologies, automation and the internet. As an organisation, we firmly believe that **technology should be at the service of humanity**, and not a tool to exercise power, repress or discriminate against individuals or collectives. Our mission statement is to advocate for a new culture for the **defence of privacy and inviolable rights of people, towards a free and democratic technological society**. While advocacy is one of our core components, Privacy Network today has expanded to research and legal action, intervening in cases of legislation breaches and joining efforts in European campaigns such as EDRi's #ReclaimYourFace campaign.

Facial recognition is a category of biometric security or of biometric surveillance. Other forms of biometric software include voice recognition, fingerprint recognition, and eye retina or iris recognition, and they have in common the use of unique personal physical or behavioural characteristics. The use of Facial Recognition Technology ("FRT") is mostly used for law enforcement, while there is an increasing interest to apply it to other fields.

We believe that in the current state, Facial Recognition systems should be banned at least until these technologies can provide a sufficient level of trustworthiness. Nevertheless, we consider the **public consultation on Guidelines 05/2022** (the "Guidelines") as an opportunity to provide feedback to the European Data Protection Board and to make sure that the highest level of data protection is granted.

Indeed, the use of biometric surveillance technologies to process the indiscriminately or arbitrarily collected data of people in public or publicly-accessible spaces (for example, remote facial recognition) enables **mass surveillance** and creates a *'chilling effect'* on people's fundamental rights and freedoms. In this regard, it is important to note that any deployment of biometric mass surveillance in public or publicly accessible spaces amounts to, per definition, indiscriminate processing of biometric data. Such use of biometric mass surveillance by law enforcement authorities **intrudes on the psychological integrity and well-being of individual**s, in addition to the violation of a vast range of fundamental rights.

The key non-privacy concerns that emerge from Facial Recognition Technology are related to issues of bias, specifically regarding race and gender discrimination. Moreover, the use of facial recognition technologies ("FRT") in law enforcement can lead to violations of the citizens' rights in relation to the authority. For instance, people could be subjected to **unlawful investigations** that could lead to unjustified **limitations of personal freedom.** In the present document, we delve into our specific feedback to the European Data Protection Board, with the hope that the public consultation process enables a democratic and open conversation regarding the critical points of the proposed guidelines on the use of facial recognition technologies in law enforcement (and beyond).

2. GENERAL REMARKS

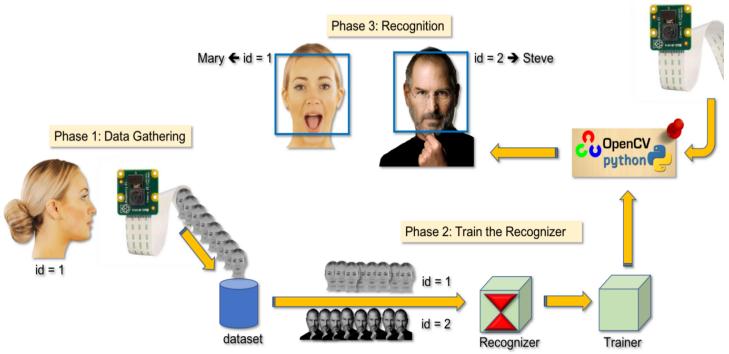
2.1. State of the art

Prior to delving into our specific points regarding the EDPB guidelines, we would like to provide the reader with a brief overview of the key definitions for the FRT. Indeed, a first distinction that ought to be underlined is the difference between **face matching** and **face recognition.** Both terms are within the umbrella term of 'Facial Recognition Technology' (FRT), which constitutes a broader category of facial recognition software, made up of many facial recognition programs available.

On one hand, **facial matching** occurs when the subject being tested is presented with two faces at the same time and asked whether they match without relying on the subject's memory. **Facial recognition,** on the other hand, occurs when the subject is presented with one face to learn and then presented large database, and then have to identify whether they are the same (without the comparison side to side)[1].Facial matching had already been done for decades in law enforcement. The way that facial recognition, using AI systems works, is typically identified in a series of 5 steps: (Bonsor and Jognson,)

1. **Detection**: The program tries to find something that is a face;
2. **Alignment**: Determining head position, size and pose. A face needs to be turned at least 35 degrees towards the camera for the software to be able to recognize it as a face;
3. **Normalization:** The image is rotated and scaled;
4. **Representation:** The data of the measurements and location of facial features translated into a unique code;
5. **Matching:** New facial data is compared to the stored data to determine if a match exists.

Real time facial recognition diagram (Rovai, 2018)



[1] Stacchi, L., Huguenin-Elie, E., Caldara, R., & Ramon, M. (2020). *Normative data for two challenging tests of face matching under ecological conditions. Cognitive Research: Principles and Implications,* 5(1). https://doi.org/10.1186/s41235-019-0205-0

2.2. Necessity and proportionality

Observations

The evaluation of proportionality should take into account several factors, such as the accuracy of the FRTs and the categories of personal data involved.

Many studies enlighted a low level of accuracy of these systems and a high risk of bias flawing the algorithms[2]. As noted by the board, due to the large number of people involved in facial recognition practices, "*a relatively small proportion of errors (e.g. 0.016 %) still means that hundreds of people are wrongly flagged*"[3]. Also, CCTV position, light conditions and other features could increase the error percentage of error.

In addition, data collected through video recording devices raise serious risks of secondary use and misuse[4]. Any activity carried out thanks to the result of facial recognition techniques goes far beyond the reasonable expectations of data subjects. Moreover, as noted by the board at paragraph 35 of the Guidelines, usage of FRT "*allows conclusions to be drawn concerning the private lives of the relevant persons. Those conclusions may refer to the racial or ethnic origins, health, religion, habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".*

In other terms, such conclusions could be used to discriminate against minorities and political opponents. In some countries of the Union, rule of law and human rights are in crisis and abuse cannot be excluded[5].

Any limitation on the exercise of the rights and freedoms, In order to respect Art. 52(1) of the Charter, shall be designed in such a way that "***the advantages resulting from the measure should not be outweighed by the disadvantages***"[6].

As noted at paragraph 43 of the commented Guidelines, the law that provides for a limitation should be accessible and foreseeable[7]. The notion of foreseeability "refers to the quality of domestic law must be **sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public**

[2] European Digital Rights, *EDRI Ban Biometric Mass Surveillance* (13/05/2020) https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf ;
[3] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* ,(21/10/2019), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf
[4] European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video* (10/07/2019), https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf
[5] https://www.europarl.europa.eu/doceo/document/TA-8-2018-0340_EN.pdf https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0722&from=EN https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0714&from=EN
[6] European Digital Rights, *EDRI Ban Biometric Mass Surveillance*, (13./05/2020) https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf ;
[7] European Data Protection Supervisor: *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19/12/2019), https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf ;

authorities are empowered to resort to any such measures[8]" . Moreover ***"the lack of clarity and did not offer sufficient safeguards against arbitrary interference*** *with Article 8 rights"*. As further explained by CJEU in the Digital rights judgement: "*where interferences with fundamental rights are at issue, the extent of the EU* ***legislature's discretion may prove to be limited, depending*** *on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter,* ***the nature and seriousness of the interference and the object pursued by the interference****"*[9]

The proportionality principle became a helpful tool also to address the risk of secondary uses and dangerous inferences on the private life of the data subject since it "*requires that a measure which interferes with an ECHR right* ***should go no further than needed to fulfil the legitimate aim being pursued***."[10]

Concerning the necessity principle:

WP 29 clarified that "*necessity implies the existence of* ***a pressing social need***", taking into account "the public concern, **nature of the issue to be tackled** and so on"[11]. Moreover, it "*implies the need for a combined, fact-based assessment of the* ***effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal*** […] *If the proposed measure includes the* ***processing of sensitive data, a higher threshold should be applied in the assessment of effectiveness*****"**[12].

Considering what was stated above, the necessity and proportionality of a legislative measure involving a limitation of fundamental rights to privacy and personal data protection are **two essential requirements** that any proposed measure involving the processing of personal data must comply with. The principle of proportionality requires, therefore:

1. first, that measures in various ways restrict the right to be limited to only those cases supported by specific and differentiated needs, thus making massive measures generally illegitimate;

---

[8] European Data Protection Supervisor: *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19/12/2019), https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

[9] CJEUJoined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238;European Data Protection Supervisor: *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19/12/2019), https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

[10] Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (27/02/2014), https://www.pdpjournals.com/docs/88168.pdf ; European Data Protection Supervisor, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit 11/04/2017)* https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

[11] Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (27/02/2014), https://www.pdpjournals.com/docs/88168.pdf ; European Data Protection Supervisor, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit 11/04/2017)* https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf; *The Sunday Times v United Kingdom Appl. No. 6538/74 (ECtHR 6 November 1980) par. 59.* https://www.ucpi.org.uk/wp-content/uploads/2018/03/The-Sunday-Times-v-The-United-Kingdom-A30-1979-80-2-E.H.R.R.-245.pdf

[12] Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (27/02/2014), https://www.pdpjournals.com/docs/88168.pdf

2. second, the principles of necessity and proportionality lead to the conclusion that right-restrictive measures are illegitimate whenever it is possible to adopt equally effective but less invasive measures.

It is our opinion that any processing involving the recognition of individuals in public spaces will never be proportionate as it could be used to carry out mass surveillance activities by public authorities and reduce the right to demonstrate.

However, at least it should be (i) carried out for specific purposes different from the generic need to detect criminals (i.e., FRTs should be used only for a limited catalogue of crimes) and (ii) the impossibility to use ordinary law enforcement techniques (i.e., ordinary CCTV systems) is demonstrated.

Proposal

Considering *(i)* the high error rate risk of FRT applications at the current stage, (ii) the intrusiveness of FRT technologies if compared to others, and (iii) the risk of secondary use of data collected, It appears to be very difficult to comply with the proportionality and necessity principles as intended by the EDPB and the stated jurisprudence.

On behalf of these considerations, extreme caution is needed in the applications of FRT. In particular, any real-time live surveillance in public places should be avoided, given that is impossible to reach a proper balance between advantages and disadvantages

In order to ensure compliance with principles of necessity and proportionality, as explained above, our opinion is that more specific indications on the level of seriousness of crimes that could justify the application of FRT systems, should be provided, having regard to specify:

- for each crime, under which conditions it could be prosecuted once it is perpetrated or before. in the latter case, specifying further circumstances under which an FRT system can be deployed;
- under which conditions a secret surveillance system could be deployed;
- under which conditions an FRT system could be deployed only on the base of existing law and when, instead, a prior judicial authorization is needed, in particular, to tackle the risk of arbitrariness

2.3. Two different data processing

Observations

It is our opinion that the Guidelines do not distinguish properly between the different data processing of which facial recognition for law enforcement is made. This activity implies at least two different data processing:

a. creating and managing databases storing biometric data, and
b. identification of a person.

The latter cannot be pursued without the first one and both of them should be taken into account by the Guidelines.

Proposal

The requirements settled down about the identification of natural persons should be extended with appropriate modifications to database management. For example, specific measures should be taken to ensure transparency (that is, when biometric data are entered into a database, data subjects should be properly informed), proportionality (i.e., only biometric data of people who committed major crimes should be entered in the database) and any other relevant safeguard. This consideration also impacts third-party management (please, see the relevant section)[13].

3. SPECIFIC ISSUES

3.1. Introduction

Observations

Paragraph 1 of the Guidelines: The current version of the text, in certain instances, is non-inclusive because it does not take into account minorities such as non-binary people.

Proposal

We suggest the EDPB adopts a more inclusive terminology, as for example replacing "his/her" with "their" in Paragraphs 1 and 6 of the text. This sets the correct tone for the anti-discriminatory considerations which the text later adopts, as suggested by the guidelines of the High-Level Group on Gender Equality and Diversity.[14]

3.2. One biometric technology, two distinct functions

Observations

Paragraph 14 of the Guidelines: Limiting the notion of FRT to technologies of this type leaves out all other applications related to large-scale surveillance or predictive policing functions. For example, emotion facial recognition or the application of algorithms associating sexual orientation to facial traits.

Moreover, the text states that: *"These examples are however not completely unrelated to facial recognition and are still subject to personal data protection rules"*, and therefore does not rule out that emotional recognition is to be considered as a type of facial recognition application.

[13] Serious concerns about how databases containing biometric data are made up have been raised by the European Data Protection Supervisor with regard the proposal for Prum II regulation.: *EDPS issues opinions on the Police Cooperation Code proposals with a set of recommendations* (11/03/2022), https://edps.europa.eu/system/files/2022-03/EDPS-2022-07-Opinions-on-Prum-2_EN.pdf

[14] Stacchi, L., Huguenin-Elie, E., Caldara, R., & Ramon, M. (2020). *Normative data for two challenging tests of face matching under ecological conditions. Cognitive Research: Principles and Implications,* 5(1). https://doi.org/10.1186/s41235-019-0205-0

Proposal

While the definition of the two-fold functions may be useful for clarification purposes, they ought to present more specific details on each separate function. Moreover, the applications of FRT ought to be expanded to include the controversial practices of emotional facial recognition and other forms of FRT-based applications such as detection of sexual orientation[15].

3.3. A wide variety of purposes and applications

Observations

Paragraph 22 of the Guidelines: Privacy Network welcomes the efforts in ensuring that data controllers are made part of the accountability obligation and in their undertaking of regular and systematic evaluation of algorithmic processing. However, it is our opinion that the current list of cases is not flexible and does not match all the possible applications of such technologies.

Proposal

The list of cases of facial recognition identification ought to be made more flexible in order to make it future-proof, for example by adding "*these particularly include **but are not limited to** the uses listed below, currently observed, experimented or planned in the EU [...]*"

In particular, section 2.2. of the LED[16] does not include a crucially important, and equally vulnerable case of facial recognition identification: Emotional recognition.

Emotional recognition is a highly invasive form of surveillance that involves "the mass collection of sensitive personal data in invisible and unaccountable ways, enabling the tracking, monitoring and profiling of individuals, often in real-time". Several studies show that facial expressions do not always reflect one's actual emotions, yet some technologies have been developed to infer the emotional state of individuals through a range of technologies. For example, 'face-based' emotion recognition may be based on Ekman's "basic emotions" theory, which assigns universal categories of human emotion and claims to objectively be able to detect them from facial configurations.[17]

3.5. Provided for by law

Observations

Paragraph 43 of the Guidelines: In the context of law enforcement, relevant differences can be found between national legislations. This means that in some situations, also

[15] A controversial Stanford study conducted research on an AI used to determine sexual orientation based on socially constructed interpretations of facial features related to sexuality. Wang, Y., & Kosinski, M. (2017). *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images,*. https://osf.io/zn79k/

[16] Directive (EU) 2016/680 of the European Parliament and of the Council (27/04/2017), *on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

[17] See: Selinger E. (2021)., *A.I. Can't Detect Our Emotion, A conversation with the professor who just turned down a $60,000 grant from Google*, https://onezero.medium.com/a-i-cant-detect-our-emotions-3c1f6fce2539

regional laws and administrative regulations could constitute the legal basis for facial recognition.

Paragraph 44 of the Guidelines: The requirement for the law settled by the Guidelines should be described in a more specific manner. We believe that such laws should identify allowed and forbidden practices.

In specific situations (eg. secret surveillance operations), further safeguards such as a prior judicial authorisation should be necessary[18]. Appears necessary to give more precise criteria in order to distinguish between FRT application that only requires a statutory law to be deployed and FRT applications that need a prior judicial authorisation

Proposal

To ensure compliance with art. 52 (1) of the charter, it appears necessary to specify the notion of "law" that can provide limitations to fundamental rights.

Since uses that differ from the mere authentication or identification can pose higher risks, further processing such as emotion recognition and predictive practices shall be specifically authorised by the law. Moreover, it is our opinion that a general ban on uses different from mere authentication or identification should be called by the EDPD, eventually providing exceptions in specific cases and specific safeguards for data subjects.

3.6. Necessity and proportionality test

As mentioned in paragraph 2.2, at the present stage the use of FRT for law enforcement purposes can pose a serious threat to fundamental rights if used in absence of the appropriate safeguards imposed by law.

In order to avoid undesirable results such as indiscriminate mass surveillance or abuses of power it is vital to conduct a serious evaluation in light of the necessity and proportionality principles, before any application. "*At the core of the notion of proportionality lies the concept of a balancing exercise: the weighing up of the intensity of the interference vs the importance ('legitimacy', using the wording of the case-law) of the objective achieved in the given context*[19]"

On the other hand, testing the necessity of a measure requires "*an explanation of what* ***other measures were considered and whether or not these were found to be more or less privacy intrusive*** *should be presented*[20]*",* taking into account "*the type of information being collected the number of people affected by the measure or the amount of information collected* [...] *the type of information being collected the context*

[18] European Court of Human Rights, Case of Szabò and Vissy v. Hungary, Application n. 373138/14 (12/01/2016), https://hudoc.echr.coe.int/fre?i=001-160020

[19] European Data Protection Supervisor: *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19/12/2019), https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf p. 11

[20] Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (27/02/2014), https://www.pdpjournals.com/docs/88168.pdf

in which the measure is to be carried out or the nature of the activity that is subjected to the measure[21]"

Proposal

As explained in p2.2, the high intrusive and risky nature of the FRT applications per se, impose) to stress the importance of specific and precise consideration on the offence persecuted, the aim of the processing (prevent, punish), the kind of act justifying the deployment (statutory law, judicial authorization, specific internal authorizations), and pre-existing conditions for the deployment (precise evidence, a preexisting warrant, etc.), the level of human intervention. It appears also important to clarify remarks that generic evaluations relating to the aim of pursuing an undefined interest in public order or security would not constitute a necessity or a proportionality test.

Moreover, We suggest that FRT should be limited to the persecution of criminal offences in the context of an investigation already started, not to the mere collection of data meant to be used for future investigations

3.8. Making rights and information known to data subjects in a concise, intelligible and easily accessible form

Observations

Paragraph 84 (and following) **of the Guidelines:** Special attention should be given to how data subjects are informed. In each possible scenario, a serious information asymmetry exists between data subjects (citizens, including children, elders, and other minorities that have no access to information) and the data controller (law enforcement authorities). Also, it should be taken into account that the functioning of new technologies is difficult to understand and privacy notices are generally ignored by people.

Proposal

Therefore, the guidelines should recommend more obligations than required by the LED. In particular, privacy notices must contain:

- the name of the vendors involved and the relevant privacy notices
- justification of automated decision making
- information about human oversight and accountability
- the name of departments in charge of processing

Moreover, data controllers should:

- use multi-layer privacy notices
- use multi-channel privacy notices (i.e., using information video, audio or even comics to explain how the processing takes place)

[21] Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (27/02/2014), https://www.pdpjournals.com/docs/88168.pdf

- publish the DPIA report (at least the parties concerning citizens' rights)
- attach information concerning how facial recognition systems work
- make records of search requests auditable
- publish audit reports
- publish the results of evaluations of the effectiveness of the system conducted both by the vendor of the technology and the law enforcement authority
- publish the outcomes of prior consultation of DPA.

Privacy notices should be available online on the website of the relevant LEAs and easy to reach (for instance, it is possible to open the relevant webpage using a QR code).

Lastly, for anyone identified using an FRT system, that person must be informed that an FRT system was used to identify him/her

3.9. Art 27 – Data protection impact assessment

Observations

Paragraph 96 of the Guidelines. The DPIA is a powerful juridical instrument useful to describe the main characteristics of the data processing and also to demonstrate the data controller's compliance. In addition, data subjects can access the DPIA report[22]; therefore, the document is also to make people aware of how their data are processed and of the warranties adopted.

Proposal

Without prejudice of what is stated by par. 96 of the Guidelines, the DPIA should contain an assessment of the compliance of every third party system used with the principle of privacy by design & by default, the criteria used to create databases, the error percentage estimated by the creator of the facial recognition system, an evaluation of the error percentage carried out by the LEA or by a trusted third party.

3.10. Art. 20 Data protection by design & by default

Observations

To comply with requirements settled by article 20 of LED, LEAs should assess both the compliance of databases used for facial recognition and technologies used to identify people. More information should be provided by the board about the way and the outcomes of such assessments.

Proposal

[22] Even if the data controller has not published the DPIA report (as suggested in this document), data subjects could access the relevant document though a FOIA request

Despite all the entities involved could be considered autonomous data controllers, the LEA carrying out the facial recognition should be encharged to assess the trustworthiness of those instruments. The outcomes should be reported in the DPIA.

4. FURTHER MATTERS OMITTED IN THE CURRENT VERSION OF THE GUIDELINES

4.1. Extra-EEA data transfers and TIA

Observations

Chapter V of LED lays down obligations to ensure that data transfer abroad can take place only where an adequate level of protection is ensured.

Proposal

As a general rule, data transfer abroad of highly sensitive data should be avoided. Whenever data transfers take place, the data controller should carry out a Transfer Impact Assessment that must contain at least the importer country, personal data mapping, a verification of the transfer mechanism, an assessment of laws and practices of the importer country, identification and proof of adoption of supplementary measures, periodic re-evaluation.

4.2. Third-party

Observations

The guidelines do not take into account the hypothesis that the database manager and the LEA carrying out identification are two different legal entities. This could have serious consequences concerning the definition of subjective roles and accountability. For example, different LEAs could operate in one country and one of them could carry out the identification activity on behalf of another. At the same time, databases can be managed by a third legal entity.

Proposal

The guidelines should clarify roles and responsibilities in these different scenarios. For instance, third-party acting as data processors should sign a contract as per article 22 LED. Moreover, the controller must verify the compliance of the processor and carry out an audit at least once a year.

4.3. Accountability

Observations

Article 4(5) of LED settles down the principle of accountability. Accountability is not necessary only to demonstrate compliance in front of the DPA but is also an instrument

to self-assess the lawfulness of data processing and the adequacy of the technical and organisational measures.

Proposal

Considering risks related to processing in scope, greater attention should be given to the way the data controller demonstrates compliance with the law. In particular, a documentation system should be implemented in order to make the relevant documentation easy to find. Moreover, the data controller should have audits performed by a trusted third party at least once a year.

5. ANNEXES

5.1. Annex III - Practical scenarios

We suggest to include among the list of practical examples the following scenarios:

As **emotional facial recognition** or the use of facial recognition and similar technologies to infer emotions of persons has been noted (in paragraphs 104 and 14) as a highly undesirable practice, which should be prohibited, we recommend including a detailed and relevant Example Scenario for it.

Moreover, the following cases require further research and to be specified within the guidelines:

1. **Predictive practices** associated with identification of terrorists in public spaces. Greater clarity is needed in the case of predictive use of facial recognition for 'pre-emptive' interventions.

2. Identification by comparing the facial image of a controlled person by **border officers** to facial images of criminal and missing individuals stored in INTERPOL's Facial Recognition System (IFRS)[23]. Other cases of use in law enforcement: Finding the identity of an ATM fraud criminal, uncovering the identity of a rioter, looking for the identity of a museum thief, and using FRT to find missing persons.

6. CONCLUSION

Privacy Network strongly welcomes the framing of the issue of facial recognition technology applications under the form of threat to human rights violations that go beyond privacy, but also as a threat to human dignity, freedom of movement and freedom of assembly.

[23] World Economic Forum, A Policy Framework for Responsible Limits on Facial Recognition,, https://www3.weforum.org/docs/WEF_A_Policy_Framework_for_Responsible_Limits_on_Facial_Recognition_2021.pdf, p.10

We **strongly support** the generalised ban called upon by the EDPB and EDPS. This is of the utmost importance in a context where the partial prohibition or the limitation of FRT applications may give lee-way for identification of 'loopholes' and 'exemptions' which in reality hides invasive profiling and surveillance practices.

7. ENDNOTES

1. Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (27/02/2014), https://www.pdpjournals.com/docs/88168.pdf

2. Directive (EU) 2016/680 of the European Parliament and of the Council (27/04/2017), *on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

3. European Court of Human Rights, Case of Szabò and Vissy v. Hungary, Application n. 373138/14 (12/01/2016), https://hudoc.echr.coe.int/fre?i=001-160020

4. European Court of Justice, Case of CHEZ Razpredelenie Bulgaria AD vs. Komisia za zashtita ot diskriminatsia, C - 83/14 (16/07/ 2015), https://curia.europa.eu/juris/document/document.jsf?text=&docid=165912&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5608072

5. European Data Protection Board, *EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Councillaying down harmonized rule on artificial intelligence* (Artificial Intelligence Act) (18/06/2021), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

6. European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video (10/07/2019)*, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

7. European Digital Rights, *EDRI Ban Biometric Mass Surveillance*, (13/05/2020) https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf ;

8. European Data Protection Supervisor: *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit* (11/04/2017), https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf

9. European Data Protection Supervisor: *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19/12/2019), https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf, p. 9 - p. 11

10. European Data Protection Supervisor: *EDPS issues opinions on the Police Cooperation Code proposals with a set of recommendations (11/03/2022)*, https://edps.europa.eu/system/files/2022-03/EDPS-2022-07-Opinions-on-Prum-2_EN.pdf

11. European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (21/10/2019), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

12. Selinger E. (2021)., *A.I. Can't Detect Our Emotion, A conversation with the professor who just turned down a $60,000 grant from Google*, https://onezero.medium.com/a-i-cant-detect-our-emotions-3c1f6fce2539

13. Stacchi, L., Huguenin-Elie, E., Caldara, R., & Ramon, M. (2020). *Normative data for two challenging tests of face matching under ecological conditions. Cognitive Research: Principles and Implications,* 5(1). https://doi.org/10.1186/s41235-019-0205-0

14. Wang, Y., & Kosinski, M. (2017). *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images,*.https://osf.io/zn79k/

15. World Economic Forum, A Policy Framework for Responsible Limits on Facial Recognition,, https://www3.weforum.org/docs/WEF_A_Policy_Framework_for_Responsible_Limits_on_Facial_Recognition_2021.pdf, p.10

PRIVACY NETWORK

ABOUT US

Privacy Network is a leading Italian non-profit organisation promoting digital and fundamental rights related to technologies, automation and the internet.

As an organisation we firmly believe that **technology should be at the service of humanity,** and not a tool to exercise power, repress or discriminate against individuals or collectives. Our mission statement is to advocate for a new culture for the defence of privacy and **inviolable rights of people, towards a free and democratic technological society.**

While advocacy is one of our core components, Privacy Network today has expanded to research and legal action, intervening in cases of legislation breaches and joining efforts in European campaigns such as EDRi's **#ReclaimYourFace campaign**.

For any additional insight, do not hesitate to contact us on our email address:

legal@privacy-network.it

Feel free to reach out to us, and follow our webpage for our current initiatives:

https://www.privacy-network.it

PRIVACY NETWORK