USING OPEN-SOURCE IMAGE DATASETS FOR RESEARCH

Jakob Zanol / Jonas Pfister / Jessica Fleisch

Jakob Zanol, Researcher, University of Vienna, Centre for Computers and Law
Schottenbastei 10-16/2/5, 1010 Wien, AT
jakob.zanol@univie.ac.at; http://rechtsinformatik.univie.ac.at

Jonas Pfister, Researcher, University of Vienna, Centre for Computers and Law
Schottenbastei 10-16/2/5, 1010 Wien, AT
jonas.pfister@univie.ac.at; http://rechtsinformatik.univie.ac.at

Jessica Fleisch, Researcher, University of Vienna, Centre for Computers and Law
Schottenbastei 10-16/2/5, 1010 Wien, AT
Jessica.fleisch@univie.ac.at; http://rechtsinformatik.univie.ac.at

Keywords: ***Artificial Intelligence, Image Data Sets, Research, Data, Data Protection***

Abstract: *The application of AI-based Facial Recognition (FRT) raises various legal and ethical questions. A comprehensive analysis must take into consideration not only the creation and future use of facial recognition but has to start even earlier: namely with the selection of the underlying data sets. While it may seem practical to utilize open-source image datasets for the creation, training and testing of models, the compliant use of such data sets still represents a major legal hurdle, especially with regard to international aspects. This is mainly due the fact, that harmonization in the area of research and data protection is very limited and still largely left to national legislators, even within the European Union. In this article, the authors analyse key problems of the use of open-source datasets for research in the area of FRT based on AI.*

1. Introduction

Modern facial recognition technologies are based on machine learning. The basis for the development of all facial recognition technologies are corresponding data sets. The selection of appropriate data sets is a core problem. Although a plethora of datasets are available on the Internet, not every one of them is equally well suited for this purpose. In addition to practical and technical considerations, legal and ethical considerations are required to avoid liability. The recent decisions of various data protection authorities on FRT[1] were a stark reminder, that compliant data use is of utmost importance.[2]

However, especially in the area of research on facial recognition technologies, there are still many legal "grey areas" – issues, that have not yet been resolved and the wording in the law that is open for interpretation. This contribution gives an overview of the legal issues with regard to the interpretation of existing law and mainly on the European General Data Protection Regulation (hereinafter: "GDPR"[3]).[4]

---

1 "FRT" stands for "*Facial Recognition Technology*".

2 See Kanada: Datenschutzbehörde wirft Clearview illegale Massenüberwachung vor, ZD-Aktuell 2021, p. 5045; Strauch, UK: ICO Fines Clearview AI Facial Recognition Company for Breaches of Data Protection Law, ZD-Aktuell 2022, p. 1299; Qasim, Italien: Kein Freifahrtschein für Gesichtserkennungssoftware – Bußgeld iHv 20 Mio. EUR gegen Clearview AI, ZD-Aktuell 2022, p. 1144; Etteldorf, Griechenland: 20 Mio. EUR Bußgeld gegen Clearview AI, ZD-Aktuell 2022, p. 1275.

3 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) OJ L 119, 4.5.2016.

4 For the purposes of this contribution, Facial Image data sets consist of „personal data"; at least the current case law oft he ECJ (starting with ECJ 19 October 2016, C-582/14, *Breyer* but especially ECJ 14 February 2019, C-345/17, *Buivids*) does not leave a lot of room to argue that *face images* are not personal data according to Art 4(1) and Rec 26 GDRP; see for example Helminger, Daten-

2. Applicable Law

The first central legal issue that developers of FRTs are facing when choosing an image data set, is the question of the applicable (data protection) law.

While the GDPR – as an EU "Regulation" that is directly applicable in all Member States[5] – has largely harmonized the rules of data protection law in the EU, there are still many areas of data protection law that remain within the competence of the member states. Even though the GDPR is meant to be a "general" regulation, the legislator intentionally included such "opening clauses" to account for the different (often historically founded) approaches that existed in the national member state law.

Seeing as the GDPR provides such "opening clauses" in the area of research as well, national law must be taken into consideration. If scientific research is conducted in an international consortium, consisting of various legal entities in different member states, the first question that arises is which national law should be applied. It is also conceivable that several national data protection provisions potentially apply.

Complexity increases if research is not just confined to EU member states but also includes institutions from outside the EU, which only partially fall within the territorial scope of the GDPR.[6]

While this might seem a prevalent issue, the literature regarding the question of the **applicable "national" data protection law** – even within the scope of the GDPR – is limited.[7] There are two different approaches in literature to determine which of two (or many) different national data protection rules apply:

According to one approach, the determination is made on the basis of "private international law", while the other approach draws an analogy to the jurisdiction rules of the GDPR.[8] Both approaches can lead to the applicability of several national provisions.

In view of the current case law of the Austrian data protection authority, this ambivalence of applicable laws could lead to territorially applied "*research privileges*"[9] can only be applied territorially.[10]

3. "Role Allocation" under the GDPR

Since the development of FRTs within the context of research is mostly conducted not by a single legal entity, but by various different entities, questions regarding the "role allocation" arise. Whenever processing of personal data is conducted, it is important to qualify each entity's "role" under the data protection regime, and especially determine the controller of a processing activity.

schutzrechtliche Herausforderungen bei der Verwendung von Trainingsdaten, EALR 2022, p. 46 (50) on issues with anonymisation and synthetic data.

5 See Art. 3 GDPR for the territorial scope of the GDPR.

6 Art. 3 GDPR; compare to the examples given in EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) on pp. 16 and 19.

7 See, however, Chakarova, General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues, in: Fina/Vogl, Stanford-Vienna European Union Law Working Papers No. 41 (2019); Leissler/Wolfbauer in: Knyrim, DatKomm Art. 3 DSGVO no. 6 (2021).

8 Zavadil in *Knyrim*, DatKomm Art. 56 DSGVO no. 16.

9 "*Research privilege*" in this context refers to the national law that is give certain privileges with regards to data protection law obligations, if processing activities are conducted for scientific research purposes.

10 Austrian DPA, 21.01.2020, 2020-0.013.649 (DSB-D202.235); while this may seem disadvantageous, it is in line with commentary literature: "The GDPR does not regulate which Member State implementation of an opening clause should apply, so difficult issues are bound to arise in this regard It has been suggested that when private law relationships are involve, then the Member State law of the lex cause should apply.[…] However, complexities will arise and great care must be taken to avoid one Member State imposing its position on others." – Kuner/Bygrave/Docksey, The EU General Data Protection Regulation (GDPR) – A Commentary, p. 84 with reference to Kohler, Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union, 52 Rivista di diritto internazionale private e processuale (2016) p. 653 (657f).

Possible "roles"[11] an entity could take on during the processing of personal data include the controller[12], the processor[13], the data subject[14] and – if none of these apply – the "third party"[15] . The most important part of the role allocation is of course the determination of the controller, since the controller is the main addressee of the obligations in the GDPR.

It should be stressed, that the controller must be determined for each processing activity, which requires that these processing activities be determined beforehand. The collection of data to train a model for facial recognition is part of one processing activity, while the actual training (and testing) of the model are different processing activities. However, this separation is not always carried out strictly. The fact that the assessment of the data protection role is not carried out for every specific processing activity is arguably also due in part to the case law of the European Court of Justice (hereinafter: "*ECJ*").

In particular, the (landmark) decision of the ECJ in the case of "*Wirtschaftsakademie Schleswig Holstein*"[16] has led many scholars to apply the institute of "joint controllership" far more broadly than before that decision, and to include entities as "*joint controllers*" that would simply have been considered "third parties" (in the sense that they are not part of that processing activity, and therefore no obligations under the GDPR apply).

To reiterate: a controller under Art. 4(7) GDPR is the person/entity, "*which, alone or jointly with others,* ***determines the purposes and means*** *of the processing of personal data;* […]"[17]

In short, the ECJ qualified the user of a Facebook fanpage as joint controller with Facebook with regard to certain processing activities (including the placing of "cookies" on visitors of the fanpage). The ECJ had to determine to which extent an administrator of a fan page (hosted on Facebook) determines, jointly with Facebook, the purposes and means of processing the personal data that is conducted. That processing is concerned personal data about the visitors to the fan page.[18]

The ECJ considered that 1) there was a contract between the fanpage administrator and Facebook and 2) that the intention for placing of cookies and the processing of personal data was primarily to enable Facebook to improve its system of advertising transmitted via its network but also to enable the fan page administrator to obtain statistics produced by Facebook from the visits to the page for the purposes of managing the promotion of its activity.

As a result of the decision, the question arose as to whether someone should be qualified as a controller – albeit "jointly" with another entity – based on the fact that that "controller" "*profits*" or "*makes use*" of a processing activity and also at least partially supports that processing activity.[19] In other words: would that be enough to consider this entity as "determining purposes and means" of the processing?

This is an important issue for the development of FRTs as well, seeing as it could be argued that the developer "*makes use*" of already collected and published image data sets and should therefore be considered to be a controller with regard to that reasoning of the ECJ in the *Wirtschaftsakademie Schleswig-Holstein* case.

---

11 See on that role allocation, especially EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, v2.1 (2021).

12 According to Art. 4 (7) GDPR a controller is a person (natural or legal person, public authority, agency, …), who alone or jointly with others determines the purposes and means of the processing of personal data.

13 According to Art. 4 (8) GDPR: a processor is a person, which processes personal data on behalf of the controller

14 According to Art. 4 (1) GDPR: Data subjects are those natural persons, whose data is processed.

15 Art. 4 (10) GDPR.

16 ECJ 5 June 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*; see the reasoning on the joint determination of purpose and means at § 31ff of that decision).

17 Art. 4 (7) GDPR [highlighted by the authors].

18 ECJ 5 June 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, § 44.

19 Compare to Mahieu/Hoboken, van/Asghari, Responsibility for Data Protection in a Networked World: On the Question of the Controller, „Effective and Complete Protection" and its Applicatioon to Data Access Rights in Europe, JIPITEC 10/1 2019, 85.

However, as a keen observer may notice, in contrast to that decision, if the **initial collection** of image data **has been conducted already** (by a different entity), **without encouragement or even any involvement or knowledge** by the developer, then it seems **unfitting to consider the developer a "joint controller".**

This argument is supported by the subsequent decisions of the ECJ in the cases *Fashion ID* (C40/17) and *Jehovan todistajat* (C25/17), where in both cases the ECJ based its qualification of joint controllership on supporting activities with regard to the processing activity.[20] In addition, in the *Fashion ID* case the ECJ pointed out that the qualification as a controller can only be done for a specific processing activity.

So, if the determination of the controller (and the allocation of roles) is conducted not for the overall development process, but separately for each processing activity – and if the reasoning of the ECJ is applied correctly – the collection of an already existing image data set does not make the developer a joint controller with the controller of the initial collection of said data. This might seem an obvious conclusion, but considering the examples given in the more recent guidelines of the European Data Protection Board (hereinafter "*EDPB*"), it has to be pointed out that for a joint controllership to be considered, there has to be at least some link between both entities, with both of them having (at least) supporting roles. The subsequent use of an already collected image data set cannot lead to a person/entity being retroactively qualified as a joint controller.

However, even if the use of a publicly available image data set to develop FRT does – in general – not lead to a joint controllership with regard to the collection of that images, this does not mean, that the manner in which the initial collection took place may not play an important role when determining the lawfulness of use of that personal data.

4. Lawfulness

This section raises certain relevant legal questions with regard to the lawfulness of the processing of training data sets under the GDPR. This means that this section is a "*snap shot*" of two specific legal issues that are associated with the training of FRT.

4.1. Lawfulness of the initial collection of training data (and its impact on subsequent use of the dataset)

The usual approach in developing FRT is to use existing face image data sets to train the AI. This means that the developers of FRT do not collect face image data themselves, but rather use existing training data sets as well as evaluation data sets. These data sets are generally made freely available to the scientific community.[21]

The question arises, whether or not these training data sets can be used in a lawful manner (i.e. in compliance with the GDPR) if these data sets have been collected outside the European Union and perhaps even under legislation that has a lower standard of data protection than EU legislation. This question becomes all the more pressing, if the collection of the data set was apparently unlawful (either in view of the GDPR or in view of the legislative framework that was applicable to the initial collection).

Even though this question appears to be extremely important for assessing the lawfulness of the use of these training data sets, there is little literature on the question **whether or not the initial collection would have to be "lawful" under the GDPR**. If that was the case, the processing of data that have been collected "unlawfully" under the GDPR would be unlawful itself.

---

20 ECJ 10 July 2018, C-25/17, *Jehovan todistajat* and ECJ 29 July 2019, C-40/17, *Fashion ID*.

21 See for example: Moschoglou et al. "AgeDB: The First Manually Collected, In-the-Wild Age Database." 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2017, pp. 1997–2005; Kimmo, Jungseock, "Fairface: Face attribute dataset for balanced race, gender, and age." arXiv preprint arXiv:1908.04913, 2019.

Although this issue has not yet been discussed before the ECJ, two **decisions on a national level** by the respective Supervisory Authority of a member state have come across the question how the lawfulness or **unlawfulness of the initial collection** of data can impact the further processing of that data and came to **very different conclusions**:

The Belgian Data Protection Authority (hereinafter "*DPA*"), for example, has more recently ruled against the use of personal data as evidence in civil law proceedings, **if these data have been obtained without a legal basis** under Art. 6 GDPR.[22] In this case further processing of personal data, even in the context of legal proceedings, was deemed unlawful and was therefore prohibited.

While some practices of obtaining data used as evidence are dubious, in this case it appears to have been a simple mistake. The first defendant sent an e-mail to a third person as a result from his habit of sending e-mails to both the plaintiff and the second defendant, whereas he could have sent an e-mail to both the plaintiff and the second defendant concerning their notary practice and a separate e-mail to the plaintiff only concerning her personal company.[23] The DPA argued that even if unintentional, the transfer of personal data constituted processing of personal data and since the first defendant could have sent a separate e-mail, not including the second defendant, he did not adhere to the data minimisation principle and therefore the processing activity was deemed unlawful.[24]

The second defendant, who was the recipient of these e-mails, then went on to send these to his legal counsel. The DPA neither accepted the argument that the communication was privileged as attorney-client correspondence, nor did it deem the further processing of the data in pending or future legal proceedings possible without violation of the principles of lawfulness, loyalty and transparency.

While this decision of a national DPA cannot represent the EU as a whole, the opinion of a national DPA can still have an EU-wide influence if adopted by the EDPB. Nevertheless, at the current state it is still a singular decision that is contrasted to different national case law of the member states.

Another example would be the decision of the **Maltese court** that, in a similar case, stated that the "fruit of the poisonous tree" doctrine adopted by the US jurisprudence according to which unlawfully obtained evidence was rendered inadmissible in court proceedings, was alien to Maltese law.[25] More importantly the Maltese Court stated, that data protection law, even under the GDPR, does not create or provide for such an "exclusionary rule" in case of illegally obtained evidence.[26] Also, the Maltese Court referenced the European Court of Human Rights' case law according to which the use of illegally obtained evidence is not in breach of the right to a fair trial (Art. 6 ECHR).

The **GDPR does in fact, not explicitly state**, that in order to process data lawfully, the controller must ensure that the **processed data are (initially) obtained lawfully** (e.g., in a manner compliant with the GDPR). This could indicate that this is not a requirement for lawful processing of personal data, i.e. that it could also be lawful, to (further) process data that has initially been obtained unlawfully. This would also fit in with the fact that the legal grounds for processing data in Art. 6 (1) GDPR refer to the current processing activity (and

[22] DPA (BE) Décision quant au fond n° 07/2021 du 29 janvier 2021, available under https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-07-2021.pdf [25.03.2022]; see also Van Beal & Bellis, Data Protection Newsflash, 25th March 2021, available under: https://www.vbb.com/media/Insights_Articles/Data_Protection_Newsflash_-_DPA_prohibits_use_of_personal_data_by_legal_counsel.pdf [25.03.2022].

[23] Ibid.

[24] Ibid.

[25] Bugeja, Can evidence obtained in breach of GDPR be lawfully used as evidence?, Times of Malta 30th June 2009, available under: https://timesofmalta.com/articles/view/can-evidence-obtained-in-breach-of-gdpr-be-lawfully-used-as-evidence.718126 [25.03.2022].

[26] Ibid.

not the previous processing activities) as well as the fact that the existence of Art. 14 GDPR indicates, that personal data must not always be obtained by the data subject itself.[27]

In addition, if we consider the legal bases under Art. 6 (1) GDPR, the further processing of personal data (that initially have been unlawfully obtained) could not be based on consent given by the data subject[28] or the performance of a contract with the data subject[29], seeing as this concerns the initial collection of the data and not the further processing. It could nevertheless be possible, that the national law contains a **legal obligation**[30] **to process personal data even if they have been initially obtained unlawfully**.[31] It could be argued that such a provision (or its interpretation in that manner) would not fulfil the requirement of Art. 6 (3) GDPR, according to which legal obligations in the sense of Art. 6 (1) (c) and (e) GDPR shall meet an objective of public interest and be proportionate to the legitimate aim pursued, but – according to the authors – such a strict interpretation would impose a serious restriction for national legislators and would be in stark contrast to Art. 23 GDPR.

With regard to these considerations, it could be argued that the GDPR requires to determine the lawfulness of the processing for each processing activity separately, without consideration whether these personal data have been collected or in other way processed lawfully before that point.

However, the fact that the GDPR does not explicitly state the requirement of **lawfulness in all stages of processing personal data**, could also be an indication that it is just implicitly **taken for granted** that the initial collection of personal data is required to be lawful under the GDPR. As a matter of fact, the GDPR does require that personal data must be "*processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')*".[32] This seems to indicate a general requirement of lawful processing of personal data throughout their "*life-cycle*" (i.e. from obtaining the data through every processing activity until its deletion).

Also, the fact that personal data have been unlawfully obtained would have to be considered within the balancing of interests under Art. 6 (1) (f) GDPR. In that regard, the fact that personal data have been illegitimately obtained would have to be taken into account and would most likely shift the balance considerably against the further processing of such data by another controller.

It appears that the right answer is somewhere in the middle ground between these doctrinal approaches, one being that processing data that is not collected in accordance with the GDPR to always be unlawful and the other one disregarding the factor altogether. This is elaborated in the conclusions.

4.2. Is using existing training data sets – "further processing" under Art. 6 (4) GDPR?

There are different approaches in the literature regarding the nature of Art. 6 (4) GDPR. While some argue that it is a separate legal basis for processing, others argue that Art. 6 (4) GDPR contains additional requirements for "*further processing*" of personal data, i.e. the processing of personal data that has already been collected for a specific purpose for another ("further") purpose.[33]

---

27 Art. 12–15 GDPR contain specific provisions on the fulfilment of the transparency principle in Art. 5 (1)(a) GDPR; there are different provisions regarding information that is to be provided to the data subject by the controller, depending on whether the data have been collected by the data subject or obtained from sources other than the data subject (e.g. third parties, "the internet", etc.).

28 Art. 6 (1)(a) GDPR.

29 Art. 6 (1)(b) GDPR.

30 Art. 6 (1)(c) GDPR.

31 Consider, for example, national criminal law and the obligation to initiate criminal proceedings if evidence suggests that there have been a crime; the Code of Criminal Procedure in Austria contains such an obligation (§ 2(1) Strafprozeßordnung 1975 (StPO; *Austrian Code of Criminal Procedure*); „Amtswegigkeit" [*prosecution ex officio*]).

32 Art. 5 (1)(a) GDPR.

33 Against an interpretation as additional legal basis of processing e.g. *Bergauer*, Zur Rechtmäßigkeit der (Weiter)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018, (pp 235ff) with additional references; Feiler/Forgó, EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkommentar (2017) Art. 6 Rec 15; see also Leffer/Leicht, Datenschutzrechtliche Heraus-

While an elaboration on the discussion in the literature would go too far, we can safely assume that also in this case, the right answer is somewhere in the middle ground between these doctrinal approaches:

While it would seem unconvincing to consider processing of personal data "lawful", based on the single fact that it is "compatible" with the (perhaps unlawful) purpose of its collection, it also would be strange to have an additional condition on further processing of already collected data that goes beyond the requirements of a new collection of the very same data.

5. Conclusion

As has been discussed, the use of already existing image datasets to develop facial recognition technologies (FRTs) based on machine learning can entail various rather complex legal questions with regard to data protection, that are discussed in literature still only to a very limited degree.

Complex issues arise with regard to the applicable national data protection law, which is of importance where different entities work together in the development stage (e.g. in an international context, but also within the scope of the GDPR, if the processing falls under one of the "opening clauses").

A key issue for any compliance evaluation under the GDPR is the "role allocation". This contribution has elaborated why the use of an already existing image data set by a developer does – in general[34] and by itself – not lead to a "joint controllership", since even under the current case law of the ECJ, a retroactive controllership cannot be constructed, if there is no indication of an entity to support the (initial) processing activity in any way.

However, a developer should take **reasonable steps** to ensure that the personal data of an image data set is not collected in an unlawful manner. According to the authors, the developer should use an image data set only if that image data set has not been obviously collected in contradiction to the rules of the GDPR. This requires a consideration of relevant factors of the initial collection and the publication (e.g. the initial collector as an entity, the purposes of the initial collection, the manner in which it was collected, the restriction of access to the data set, etc.).

While the fact that personal data has been collected unlawfully does not prohibit its use *per se,* the fact that personal data that is part of an image data set that contains images which were not collected in accordance with the GDPR should be considered when balancing either public interests (e.g Art. 6 (1) (e) GDPR) or (private) legitimate interests (Art. 6 (1) (f) GDPR) with the rights of the data subject. The aforementioned reasonable steps for the developer to take are to ensure they– to the best of their knowledge – choose an image data set that has been collected in accordance with the GDPR.

6. Acknowledgement

This work has been partially supported by the European CHIST-ERA program via the Austrian Research Promotion Agency (FFG) within the XAIface project (grant agreement CHIST-ERA-19-XAI-011).[35]

forderungen beim Einsatz von Trainingsdaten für KI-Systeme, in: Schweighofer/Saarenpää/Eder/Zanol/Schmautzer/Kummer/Hanke (Hrsg.) Recht DIGITAl – 25 Jahre IRIS, Proceedings of the 25th International Legal Informatics Symposium IRIS 2022, p 89.

34 I.e. excluding exceptional or very specific cases where it might be different.

35 Finally, the authors would also like to express their gratitude to Prof. Erich Schweighofer, who is the head of the university's legal informatics working group, for his support and constructive comments.