

On Responsible Machine Learning Datasets with Fairness, Privacy, and Regulatory Norms

Surbhi Mittal¹, Kartik Thakral¹, Richa Singh¹, Mayank Vatsa^{1*},
Tamar Glaser², Cristian Canton Ferrer², Tal Hassner²
¹IIT Jodhpur, India, ²Meta, USA

Abstract

Artificial Intelligence (AI) has made its way into various scientific fields, providing astonishing improvements over existing algorithms for a wide variety of tasks. In recent years, there have been severe concerns over the trustworthiness of AI technologies. The scientific community has focused on the development of trustworthy AI algorithms. However, machine and deep learning algorithms, popular in the AI community today, depend heavily on the data used during their development. These learning algorithms identify patterns in the data, learning the behavioral objective. Any flaws in the data have the potential to translate directly into algorithms. In this study, we discuss the importance of *Responsible Machine Learning Datasets* and propose a framework to evaluate the datasets through a *responsible rubric*. While existing work focuses on the post-hoc evaluation of algorithms for their trustworthiness, we provide a framework that considers the data component separately to understand its role in the algorithm. We discuss responsible datasets through the lens of fairness, privacy, and regulatory compliance and provide recommendations for constructing future datasets. After surveying over 100 datasets, we use 60 datasets for analysis and demonstrate that none of these datasets is immune to issues of *fairness*, *privacy preservation*, and *regulatory compliance*. We provide modifications to the “datasheets for datasets” with important additions for improved dataset documentation. With governments around the world regularizing data protection laws, the method for the creation of datasets in the scientific community requires revision. We believe this study is timely and relevant in today’s era of AI.

I. INTRODUCTION

With the proliferation of artificial intelligence (AI) and machine learning (ML) techniques, different nation-level projects and *technology for good* programs are touching the lives of billions. These systems have provided incredibly accurate results ranging from face recognition of a million faces [1] to beating eight world champions at Bridge [2]. It has achieved superlative performance in comparison with experienced medical practitioners in identifying pneumonia and analyzing heart scans, among other medical problem domains [3], [4]. Recently, art generated by an AI algorithm won a fine arts competition [5]. While the systems are broadly accelerating the frontiers of smart living and smart governance, they have also shown to be riddled with problems such as bias in vision and language models, leakage of private information in social media channels, and adversarial attacks, including deepfakes. This problematic behavior has been affecting the trustworthiness of AI/ML systems. This has led to the design of the *Principles of Responsible AI* which focus on designing systems that are safe, trustworthy, reliable, reasonable, privacy-preserving, and fair [6].

Among the different stages of an AI system development pipeline, data collection and annotation is one of the most important ingredients which can have a significant impact on the system. Current AI algorithms are deemed *data-hungry* and tend to be extremely data-driven, and any irregularities in the datasets utilized during the development of these algorithms can directly impact the learning process. Several researchers have demonstrated that non-responsible use of datasets can lead to challenges such as fairness of the model and leakage of private information such as identity information or other sensitive attributes. Certain gender and race subgroups are shown to be under-represented in face-based image datasets [7], [8] while some datasets contain objects specific to certain geographies or specific contexts [9], [10]. Many algorithms have also been shown to suffer from spurious correlations in the dataset [11], [12], [13]. Similarly, concerns regarding the leakage of private information from popular datasets such as ImageNet have surfaced over recent years. In order to build responsible AI systems, it is therefore important to use datasets that are responsibly curated. We assert that *Responsible Datasets leads to building Responsible AI Systems*.

Current research for understanding and evaluating trustworthiness focuses primarily on the performance of the models. However, by identifying these issues at the dataset level, we can lay the ground for creating better and *responsible* datasets, and better AI. With the motivation to evaluate the reliability or trustworthiness of data, in this research, we present a framework to evaluate datasets via the proposed *responsible rubric* across the axes of fairness, privacy, and regulatory compliance (refer to Figure 1). To the best of our knowledge, this is the first framework that quantitatively evaluates the trustability of the data used for training ML models. For defining dataset fairness, we consider the impact of three factors: diversity, inclusivity, and

Email: {mittal.5, thakral.1, richa, mvatsa}@iitj.ac.in, {tamarglaser, ccanton, thassner}@meta.com.

* corresponding author

† All data was stored and experiments performed on IITJ servers by IITJ faculty and students.

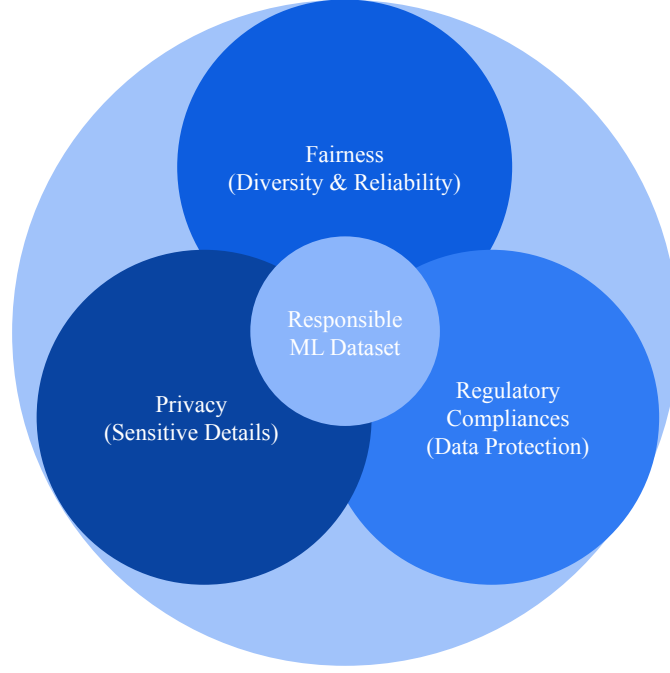


Fig. 1. We introduce the concept of Responsible Machine Learning Datasets and propose a quantitative rubric along with recommendations for future datasets.

reliability of annotations. *Inclusivity* considers whether different groups of people are present in the dataset across parameters of sex, skin tone, ethnic group, and age, and *diversity* quantifies the distribution of these groups in the dataset.

For evaluating privacy preservation in datasets, we identify vulnerable annotations that can lead to the leakage of private information. Finally, we assess datasets for their degree of compliance with contemporary regulatory norms. Different governments around the world have approved various data privacy laws in the past few years. The popular General Data Protection Regulation (GDPR) [14] requires the right to erasure based on its Article 17 (denoted as [Art. 17, GDPR]) and may require the consent of data subjects [Art. 12, GDPR] among other laws for data protection. Subjects providing data should have complete knowledge as to how their data will be used, and they should have the ability to revoke their consent. Further, if a dataset contains information such as images or potentially unethical data, there should be a mechanism to report such incidents. Through the axes of fairness, privacy and regulations, we demonstrate the applicability of the proposed framework by analyzing datasets from biometrics and healthcare domains, particularly face recognition and chest XRay datasets. After surveying over 100 datasets and discarding datasets unusable for this study because of their small size or unavailability, we utilized a total of 60 datasets. Some of our key observations are as follows:

- Most of the existing datasets suffer on all three axes of *fairness*, *privacy* and *regulatory compliance*, as per the proposed rubric.
- Fairness is a major concern for most of the datasets we surveyed.
- Most existing datasets do not focus on regulatory compliances.
- Our analysis highlights that curating datasets from the web poses major risks to privacy preservation.
- We also observe the *fairness-privacy paradox* that exists in the development of datasets where the presence of sensitive attributes aids fairness evaluation but potentially leaks a subject's private information.

Finally, we provide recommendations for constructing datasets. These recommendations can serve as an ethical sounding board for development of responsible datasets in the future.

II. RELATED WORK

In recent years, there has been an increasing focus on datasets being used in ML and deep learning. Specifically, such concerns are heightened when datasets pertain to the collection of sensitive data such as biometrics and medical data. According to a recent study, the importance of dataset quality being used in AI/ML is constantly undermined, and the data collection work is often undervalued in the community [32].

Researchers have addressed the need for data-centric AI as well as the impact of regulations and policies on trustworthy AI [33]. Heger et al. [34] conducted interviews with ML practitioners and discovered the need to emphasize the relationship between data documentation and responsible AI. Scheuerman et al. identified the patterns followed in the collection process of computer vision datasets based on 1000+ publications and also emphasized the importance of proper dataset documentation [35].

TABLE I
SOME OF THE LAWS SURROUNDING DATA PRIVACY AROUND THE WORLD OTHER THAN THE GDPR [14].

Country(s)	Title of Law	From	Amended	Relevant Authority	Region
Brazil	General Data Privacy Law (LGPD) [15]	2018	2019	Autoridade Nacional de Proteção de Dados (ANPD)	Latin America
India	Information Technology Act 2000 [16] India's Personal Data Protection Bill (PDPB) 2019 [17]	2000 2019	2008 2019	Ministry of Law and Justice Data Protection Authority of India	Asia
Israel	Protection of Privacy Law of 1981 [18]	1981	2020	Privacy Protection Authority (PPA)	Middle East
Japan	Act on Protection of Personal Information [19]	2003	2020	Personal Information Protection Commission	Asia
Lithuania	Law on Legal Protection of Personal Data [20]	1996	2018	State Data Inspectorate	Europe
New Zealand	New Zealand's 1993 Privacy Act [21]	1993	2020	Privacy Commissioner	Australasia
Nigeria	Nigeria Data Protection Regulation 2019 (NDPR) [22]	2019	2019	Nigerian Information Technology Development Agency	Africa
South Africa	Protection of Personal Information Act (POPIA) [23]	2013	2013	Information Regulator	Africa
Switzerland	Data Protection Act [24]	1992	2020	Federal Data Protection and Information Commissioner	Europe
Thailand	Personal Data Protection Act (PDPA) 2019 [25]	1997	2019	Personal Data Protection Committee	Asia
Turkey	Law 6698 on Personal Data Protection (LPDP) [26]	2016	2016	Data Protection Authority	Europe
USA: California	California Privacy Rights Act of 2020, amending California Consumer Privacy Act [27]	2020	2020	California Privacy Protection Agency (CPPA)	North America
USA: Illinois	Biometric Information Privacy Act (BIPA) [28]	2008	-	U.S. Court of Appeals for the Ninth Circuit	North America
USA: Texas	Texas Consumer Privacy Act (TXCPA) [29] Texas Capture or Use of Biometric Identifier Act (CUBI) [30]	2019 2009	- 2017	Texas House of Representatives Texas Attorney General	North America
USA: Washington	Washington Biometric Privacy Protection Act (House Bill 1493) [31]	2017	-	Washington State Attorney General	North America

There has been discussion around the collection of socio-cultural data where researchers have highlighted the need to design institutional frameworks and procedures inspired by archival data [36]. Some of the essential considerations are consent, inclusivity, power, transparency, ethics, and privacy. Similarly, focusing on the entire dataset development pipeline, Peng et al. [37] studied nearly 1000 papers citing problematic datasets such as Labeled Faces in the Wild (LFW), MS-Celeb-1M (*decommissioned*), and DukeMTMC (*decommissioned*). The authors provide recommendations for dataset creators as well as conference program committees to encourage more ethical creation of datasets.

In 2021, Gebru et al. [38] proposed a comprehensive 'datasheet' detailing information about the dataset accompanying its release. The datasheets are designed to raise transparency and accountability in the datasets. On similar lines, Hutchinson et al. introduced a framework that helps build accountability and transparency in the data development process [39]. By segregating data development process into various stages, the authors described the roles played by individuals such as requirements owner, stakeholder, and reviewer at each stage. Palluda et al. [40] promoted the usage of quantitative as well as qualitative measures for the effective development of datasets. They showcase how representational harms and spurious correlations present in the datasets can lead to unfair decisions.

Fairness in Datasets: In order to build fairer AI, researchers have studied bias in various settings [41], [42], [43], [44]. A recent report by NIST for identifying and managing bias in AI has cited the reliance on large-scale datasets as the leading cause of using unsuitable datasets for training and evaluation [45]. The report discusses various challenges and factors associated with datasets in modern AI such as lack of representation, and statistical and socio-technical factors. Towards better representation in AI, Kamikubo et al. analyzed 190 accessibility datasets. Their analysis revealed harmful trends such as lack of older adults for autism, developmental and learning communities. To this end, they suggested more meaningful interactions with data contributors [46]. Similarly, in the domain of NLP, some researchers have proposed the use of data statements that can help understand the intent and, specifically, the biases of the data [47]. The data statement emphasizes the inclusion of information such as the curation rationale and annotator demographic. Some researchers have proposed toolkits for evaluation of bias in the dataset which include object-based, person-based, and geography-based analyses through annotations [48].

Privacy Leakage in Datasets: In this work, we refer to the term *privacy leakage* as "the unintended or unauthorized/accidental exposure of sensitive or protected personal data/information, which may compromise an individual's identity." The concerns of privacy leakage surrounding datasets in deep learning have grown over the past few years. In Birhane et al. [49], the authors discuss the issues of consent and privacy breaches in the context of large-scale vision datasets such as ImageNet. They highlight the harms associated with poor dataset curation practices and propose mandatory institutional reviews.

In the field of security and privacy, researchers have attempted to preserve privacy by adopting different concepts, such as k -anonymity [50] and differential privacy [51]. To quantify privacy leakage, researchers have proposed various metrics, such as l -diversity [52], k -anonymity [50], t -closeness [53], and m -invariance [54], among others. A detailed list of these metrics has been provided by Wagner et al. [55]. These metrics are designed to capture the extent of privacy leakage from the perspective of

TABLE II
THE DIFFERENT DEMOGRAPHIC SUBGROUPS CONSIDERED FOR FAIRNESS QUANTIFICATION.

Demography	Subgroups
Sex	Male, Female, Other
Ethnicity	White/Caucasian, Black/African, Southeast Asian, East Asian, Indian, Hispanic/Latino, Middle Eastern, Mixed-race, Other
Skin tone	Type I-VI using Fitzpatrick scale
Age	0-3, 4-7, 8-15, 16-20, 21-30, 31-40, 41-50, 51-60, 61-70, 71-100

an adversary with knowledge [53], equivalent representation of sensitive attributes [52], protection from homogeneity attacks [50], and other reasons.

After the introduction of k -anonymity [56], several researchers have developed techniques for facial privacy preservation. Zang et al. [57] devised a function to add random noise to existing data samples to synthesize new samples. This was aimed at masking sensitive information in the dataset while preserving the performance of the model. Chhabra et al. [58] proposed an algorithm that provides the control to the user to anonymize k -facial attributes while preserving other attributes and identity information. Li et al. [59] proposed a technique to anonymize identity and attribute while maintaining the data utility. The authors also performed quantification of privacy preservation through k -anonymity.

In other works, researchers have used Mechanical Turk participants to identify privacy-sensitive information in images to automate the privacy attribute selection/identification task for obfuscation [60]. Gervais et al. [61] propose a framework to infer the location by analysing the consumer purchase histories. Further, experiments have demonstrated the benefit of teaching algorithms to predict the presence and purpose of private information. Orekondy et al. [62] propose an algorithm to predict a leakage risk score for the input image using their proposed VISPR dataset. Orekondy et al. [63] have also proposed a redaction by segmentation approach to aid users in selectively sanitizing images of private content. The proposed approach segments out the privacy attributes in images and provides privacy vs data-utility evaluation analysis. Gurari et al. [64] propose a dataset and study visual privacy issues faced by people who are blind and are trying to learn about their physical surroundings.

Regulatory Compliance in Datasets: With the increasingly high emphasis on data protection, various countries around the world have put legislation in place for data security and privacy. According to a report, 157 countries in the world had instated data privacy laws by mid-March 2022 [65], [66], [67]. Most of these laws are influenced by GDPR [14] but contain certain variations. The GDPR may prohibit the processing of biometric data unless explicit consent from the subjects is not provided. By providing the *right to be forgotten*, the GDPR puts the subject in charge of their data. Different studies have been conducted to understand the impact of GDPR on artificial intelligence [68], [69].

In Table I, we summarize data privacy laws for some of the countries around the world. There are other laws specific to certain kinds of data, such as the Health Insurance Portability and Accountability Act (HIPAA) [70] for medical health in the US and the Biometric Information Privacy Act (BIPA) [28] protecting biometric information in the state of Illinois, US. Other US states are actively working towards enforcing their data privacy laws [71]. The privacy implications of some of these acts have also received significant attention in the research community [72]. Notably, the European Commission released *Ethics Guidelines for Trustworthy AI*, which discusses the framework, foundations, and possible assessments for trustworthy AI [73], as well as is in the process of amending and debating the Artificial Intelligence Act [74] to address risks associated with AI applications. Recent work discusses the impact of the Artificial Intelligence Act on facial processing applications [75].

While different works identify different problematic aspects of dataset collection, very few works have looked at the factors of fairness, privacy, and regulatory compliance in datasets holistically. In this work, we provide quantitative as well as qualitative insight across the three factors and how data collection in AI needs to turn towards better and more responsible datasets.

III. METHODS

In this section, we describe the methodology adopted for designing the framework for *Responsible Datasets*. We quantify datasets across the axes of fairness, privacy, and regulatory compliance. The concerns regarding these factors may vary from domain to domain. For example, fairness in a face image dataset may differ from those in an object or egocentric dataset. The quantification in this section is based on datasets centered around individuals and specifically, face-based datasets.

A. Quantifying Dataset Fairness

In deep learning, fairness concerns have been raised for datasets in multiple domains in different contexts [7], [10]. In face-based image datasets, some sex and race subgroups may be under-represented [7], [8]. In object-based datasets, datasets may contain objects specific to certain geographies or in specific contexts [10], [9]. Similarly, text-based and multi-modal datasets may suffer from spurious correlations in datasets leading to bias in the performance of trained models [11].

In this work, we consider the impact of three factors for quantification of dataset fairness- diversity, inclusivity, and labels (See Fig. 2). In the context of face-based datasets, *inclusivity* quantifies whether different groups of people are present in the dataset across parameters of sex, skin tone, ethnic group, and age. *Diversity* quantifies the distribution of these groups in the dataset, with an assumption that a balanced dataset is the most fair. While a balanced dataset does not guarantee equal performance, existing work has shown improved fairness with the use of balanced datasets [76], [77]. We note that such a dataset may not be ideal in many cases, but it acts as a simplifying assumption for the proposed formulation. Finally, we consider the reliability of the *labels* depending on whether they have been self-reported by the subjects in the dataset or are annotated based on apparent characteristics.

We consider four demographic groups- *sex*, *skin tone*, *ethnicity*, and *age*. The different subgroups considered for these demographics are specified in Table II. We utilize the information regarding the biological sex of an individual while leaving room for error in the class *Other*. For ethnic subgroups, we take inspiration from the FairFace dataset [78] with the addition of the mixed-race as a separate category. Ethnicity subgroups around the world tend to be extremely variable. We have adopted the maximum ethnic subgroups as represented in the literature by the FairFace dataset. The age subgroup classification is based on the categories in the AgeDB dataset [79]. The age annotations were binned as per AgeDB categorization for datasets that provided continuous age values.

The proposed formulation for quantification of fairness in a dataset is dependent on the annotations available in a dataset (See Fig. 2). Let $\mathbf{D} = \{\text{sex, skintone, ethnicity, age}\}$ denote the complete set of demographics considered for evaluation of any dataset, and \mathbf{S} denote the corresponding subgroups in each demographic (Refer Table II for subgroups considered for each demographic). Then, $\mathbf{D}_1 = \text{sex}$, and $\mathbf{S}_1 = \{\text{male, female, other}\}$. For a given dataset, \mathbf{d} denotes the set of demographics annotated in the dataset, and \mathbf{s} denotes the subgroups corresponding to those demographics. For example, for the AgeDB dataset [79], $\mathbf{d} = \{\text{sex, age}\}$, and $\mathbf{s}_i = \{\text{male, female}\}$ for i th demographic in \mathbf{d} , and $\mathbf{s}_{ij} = \text{male}$ for j th subgroup of i th demographic ($i = 1, j = 1$). Then, the **inclusivity** r_i for each demography is defined as the ratio of demographic subgroups present in the dataset and the pre-defined demographic subgroups in \mathbf{S}_i . This is quantified as-

$$r_i = |\mathbf{s}_i|/|\mathbf{S}_i| \quad (1)$$

The **diversity** v_i is calculated using Shannon's diversity index [80] to capture the distribution of different subgroups for a given demography.

$$p_{ij} = \text{num}(\mathbf{s}_{ij}) / \sum_j \text{num}(\mathbf{s}_{ij}) \quad (2)$$

$$v_i = - \sum_j p_{ij} * \ln(p_{ij}), \quad (3)$$

where $\text{num}(\mathbf{s}_{ij})$ denotes the number of samples for the j th subgroup of the i th demographic in the dataset. In certain cases where the number of samples is not available, we consider num to denote the number of subjects in the dataset. Fairness across each of the demographics is measured between 0 to 1. For example, if a dataset contains images corresponding to each of the six skin tones, it will have an inclusivity score of $6/6 = 1$, and if the number of samples is balanced across each of the subgroups of skin tone, the diversity score will also be 1. When combined, that will provide an overall score of $1*1 = 1$. By multiplying the inclusivity and diversity scores, we are providing information about the presence as well as distribution of samples corresponding to a given demographic. These scores are added for the four demographic attributes.

The **label score** l , is then calculated based on whether the labels or annotations for the dataset are self-reported, classifier-generated, or apparent. *Self-reported labels* indicate that the subjects provided their demographic information as a part of the data collection process. *Classifier-generated labels* imply that the demographic labels were obtained through an automated process of classification. Finally, *apparent labels* indicate that the annotations were done by an external annotator after observing the images (for example, through Amazon Mechanical Turk). Based on the type of annotations, a *label score* is assigned for the dataset between 0 to 1, with self-reported labels assigned a value of 1, classifier-generated labels assigned 0.67, and apparent labels assigned a value of 0.33. machine-generated labels, sometimes referred to as *pseudo labels*, are assigned a higher score since they have been shown to be more reliable than human-annotated labels for use in deep learning-based applications [81], [82], [83]. We acknowledge that there may be different perceptions of reliability in annotation based on the task and nature of the data. However, the labels generated by a trained classifier are consistent while that may not be true for human annotators. Based on this rationale, we assign a higher score to classifier-generated labels.

In cases where the labels are collected using more than one of the three categories, an average of the corresponding categories' scores is taken. For medical datasets, a score of 1 is provided if a medical professional provides/validates the annotations, else a score of 0 is provided. The label score is provided for the entire dataset as per the current formulation. To calculate the **fairness score**, F , for the dataset, the factors of inclusivity, diversity, and labels are combined as follows,

$$F = \sum_i (r_i * (1 - v_i)) + l \quad (4)$$

The fairness score is designed such that a higher value indicates a fairer dataset while a lower value indicates a less fair dataset.

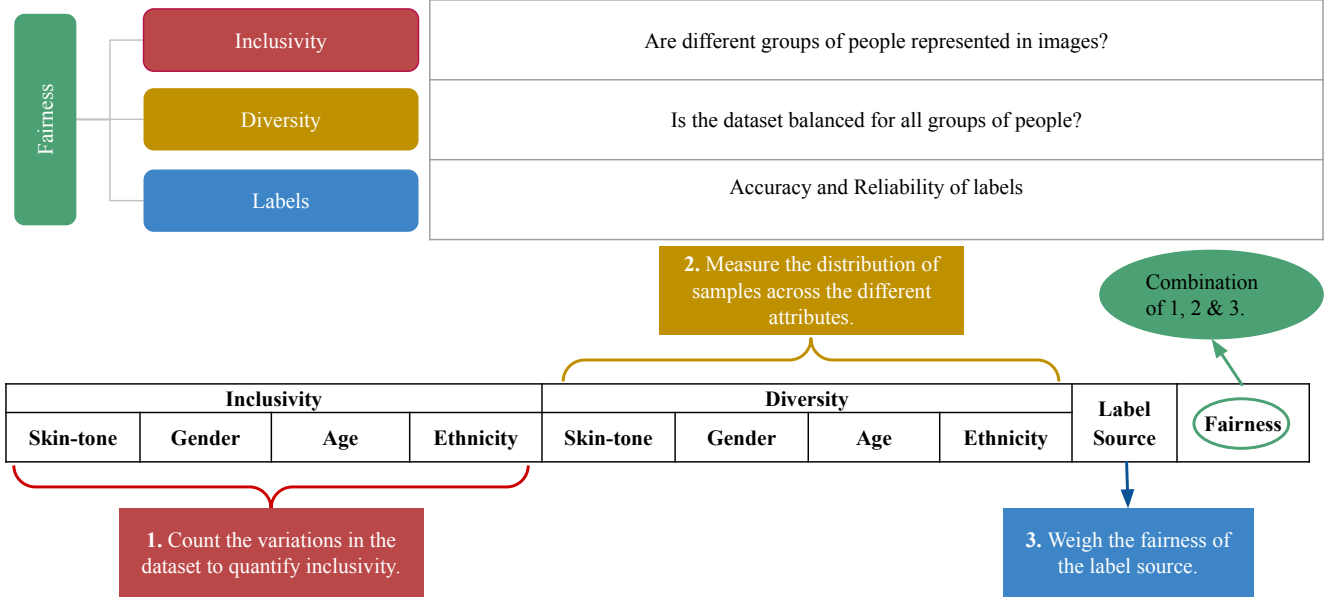


Fig. 2. (Top) The three aspects involved in fairness quantification- Inclusivity, Diversity, and Labels, and the questions they answer. (Bottom) The formulation employed for the calculation of the fairness score.

B. Quantifying Dataset Privacy

Deductions and attacks can be carried out using the annotated labels in publicly available supervised datasets (See Figure 3). Annotated attributes in a face dataset, for example, can be used for face profiling [84], [85], [86], [87]. In contrast, vehicle registration numbers from location datasets can be used to make malicious deductions and track someone down [62], [88]. As a result, the more annotations there are in the dataset, the more privacy is potentially leaked. The extent of privacy leakage can be summarized in terms of the quantity of information leaked and the extent to which private information is exposed in the annotated labels.

In this work, for quantification of privacy leakage in the publicly available datasets, we identify vulnerable label annotations that can lead to the potential leakage of private information and devise a mathematical formulation. This formulation employs the dataset's annotated labels to quantify the potential privacy leakage. We identify six label annotations that are widely available in the datasets and lead to leakage of privacy in datasets: *name identification*, *sensitive and protected attributes*, *accessories*, *critical objects*, *location inference*, and *medical condition*. Let the set A constitute these identified attributes, i.e.:

$$A = \{A_N, A_{SP}, A_{AC}, A_C, A_L, A_M\} \quad (5)$$

The attributes used in defining A are as follows:

- *Name Identification Information* A_N : This attribute refers to the name of each individual annotated in the dataset. This annotation potentially leads to the highest level of privacy leakage.
- *Sensitive and Protected Attribute Information* A_{SP} : These attributes refer to information regarding gender, sexual orientation, race, past records, etc., corresponding to an individual.
- *Accessory Information* A_{AC} : This attribute denotes the presence of accessories such as hats and sunglasses in a face image as well as other attributes such as five 'o'clock shadow.
- *Critical Objects* A_C : This attribute denotes the presence of objects revealing the identity of a person, such as credit cards or signatures.
- *Location Information* A_L : This attribute denotes the presence of information in the image that can potentially disclose a person's location, such as geographical coordinates or popular landmarks in the image background.
- *Medical Condition Information* A_M : This attribute denotes the presence of any information regarding the medical condition of an individual in the dataset.

For a dataset, we manually check for the presence of the annotations from the aforementioned list to estimate its privacy leakage, and a point is awarded for each attribute annotation. The privacy leakage score (PL) is then calculated as the sum of all the present attributes as described below:

$$PL = \sum_{i=1}^6 A_i. \quad (6)$$

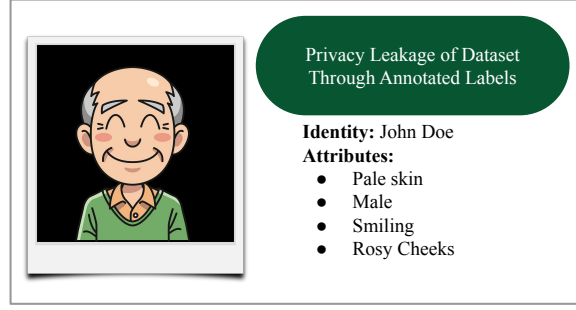


Fig. 3. Privacy leakage through the information available in datasets. The sample is representative of information present in datasets such as the LFW dataset [89], [90].

Finally, the **privacy preservation score**, P , for a given dataset is estimated as,

$$P = (|A| - PL). \quad (7)$$

P indicates the amount of information being preserved in a dataset and represents its dependability for public use. We note that while the presence of these annotations constitutes privacy leakage in our formulation, it aids the computation of the fairness score described in the previous section. We discuss this fairness-privacy paradox in detail later in the text.

C. Quantifying Regulatory Compliance

Different countries around the world have approved various data privacy laws in the past few years. One of the most widely accepted documents covering data privacy laws is the one applicable in European countries known as the GDPR [14]. The following laws can be applied to deep learning methodologies and/or datasets,

- Right to be forgotten (right to erasure) [Art. 17]
- Consent of data subjects [Art. 12]
- Right to object/restriction to the processing of their data [Art. 5, 6, 9, 18, 19]
- Right to rectification [Art. 16]
- Right of access by the data subject [Art. 15]
- Right to object and automated individual decision-making [Art. 21 and 22] [Recital 71]
- Right to lodge complaint [Art. 77]
- Right to effective judicial remedy [Art. 78,79]

Some of these laws restrict the use of users' personal data unless their consent is available for that particular application [Art. 5, 6, 9, 18, 19]. Other laws and conditions specified in the GDPR include,

- Right to data portability [Art. 20]
- Security of personal data [Art. 32, 33, 34]
- Conditions for consent [Art. 7]
- Conditions for protection of children's personal data [Art. 8]
- Requirements for regular data protection impact assessments (DPIA) [Art. 35]
- Cryptographic protection of sensitive data
- Breach notification requirements. [Art. 33]

Apart from the laws specified above, datasets in deep learning can benefit from existing mechanisms for institutional approval (such as IRB) and newer requirements set by popular conferences such as ethics and impact statement for datasets [91]. In this paper, the **regulatory compliance score**, R , in the dataset is quantified based on three factors- institutional approval (yes/no: the numerical value of 1/0), the subject's consent to the data collection (yes/no: the numerical value of 1/0), and the facility for expungement/correction of the subject's data from the dataset (yes/no: the numerical value of 1/0). If a dataset satisfies all three criteria, a compliance score of 3 is provided. While the absence of a data subject's consent may not necessarily breach regulatory norms, for lack of a more subtle evaluation, we utilize *subject consent* in the dataset as one of the factors for compliance. For example, the privacy rule in HIPAA compliance does not restrict the distribution of de-identified health data. The different factors for compliance are manually validated via information present in the published paper, webpage, and/or GitHub page for the dataset. Unless the information is explicitly specified in the aforementioned resources, it is assumed to be absent in which case we assign a value of zero.

IV. RESULTS

For this work, we surveyed a large number of datasets. Datasets containing human subjects were selected for the study. While fairness and privacy issues persist across different data domains such as objects and scenes [10], [9], current regulatory

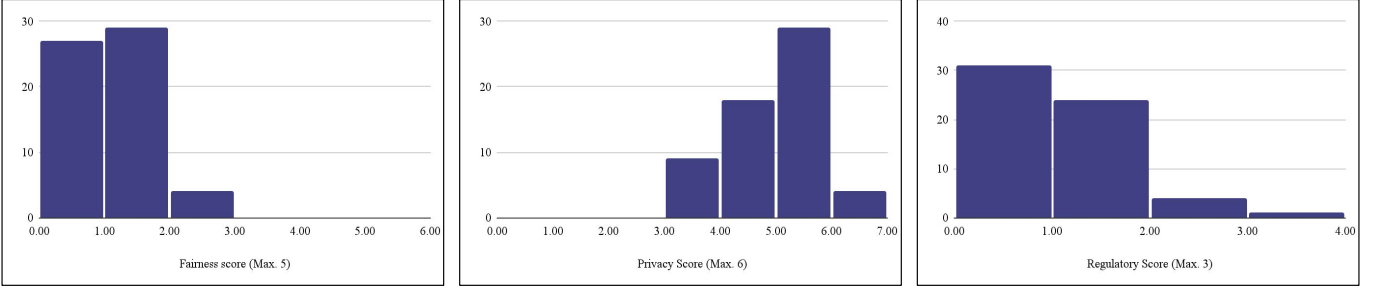


Fig. 4. The summary of fairness, privacy, and regulatory compliance scores through histogram visualization for the datasets we surveyed. (Left) The maximum value of the fairness score that can be obtained is 5, but it is observed that the fairness scores do not exceed a value of 3. (Middle) While most datasets in our study preserve privacy in terms of not leaking location or medical information, very few provide perfect privacy preservation. (Right) Most datasets comply with no regulatory norm or only one. We can observe from this plot that most datasets provide a low fairness score and perform poorly on the regulatory compliance metric.

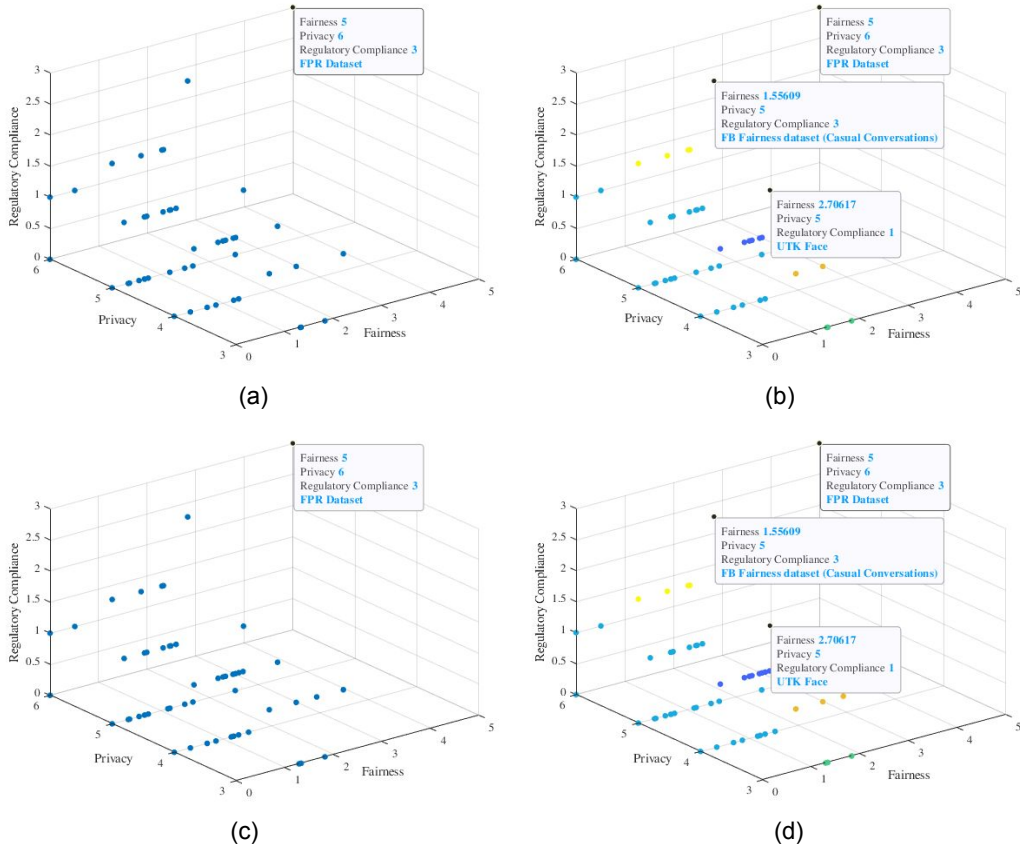


Fig. 5. Cluster analysis based on the 3-tuple quantification of fairness, privacy, and regulatory compliance for (a-b) only face-based datasets and (c-d) jointly with medical datasets. (a, c) The 3-D scatter plot of the different datasets across the three axes with the *FPR* dataset plotted with perfect fairness, privacy preservation, and regulatory compliance. (b, d) The scatter plot after performing DBSCAN clustering with $\epsilon = 1$. We observe that the FB Fairness Dataset and the UTKFace dataset lie the closest to the *FPR* dataset.

norms are designed for people. While it is possible to extend the concepts presented in this study to other domains, we limit our discussion to face-based and medical imaging datasets. After filtering through a total of 100 datasets and discarding datasets that are decommissioned, small in size (less than 100 images), and whose data could not be downloaded/accessed/requested, we were left with 60 datasets. These 60 datasets are used for the analysis and quantification of the responsible rubric. We use 52 face-based biometric datasets (Table VII), and eight chest Xray based medical datasets (Table VIII). For face-based datasets, we filtered through over 120 datasets removing datasets that had been decommissioned, older than 2010, and whose data was inaccessible. For chest Xray datasets, we similarly surveyed through about 20 datasets before obtaining the eight analyzed in this work. We quantify the datasets across the dimensions of fairness, privacy, and regulatory compliance. Using the specified quantification methodology, we obtain a 3-tuple containing scores across the three dimensions.

TABLE III

SUMMARY OF THE DIFFERENT SCORES OBTAINED FOR FAIRNESS, PRIVACY, AND REGULATORY COMPLIANCE QUANTIFICATION OBTAINED FOR THE BIOMETRIC DATASETS IN THE STUDY. AS CAN BE CLEARLY SEEN, THE HIGHEST WEIGHTED AVERAGE FOR FAIRNESS, PRIVACY, AND REGULATORY COMPLIANCE IS OBTAINED ON THE FB FAIRNESS DATASET (CASUAL CONVERSATIONS).

Dataset Name	Fairness score (Max. 5)	Privacy Score (Max. 6)	Regulatory Score (Max. 3)	Weighted Average
MORPH [92]	2.2045	3	1	0.4247
Caltech 10K Web Faces [93]	0.0000	6	0	0.3333
FaceTracer [94]	0.6791	4	0	0.2675
CMU Multi-PIE [95]	0.2463	5	1	0.4053
PubFig [96]	1.3349	3	0	0.2557
Plastic surgery database [97]	0.0000	5	0	0.2778
Texas 3D Face recognition database [98]	1.1835	5	1	0.4678
ChokePoint [99]	0.5097	6	1	0.4784
SCFace [100]	1.8257	3	0	0.2884
YouTube Faces [101]	0.0000	5	0	0.2778
EGA [102]	0.7141	5	1	0.4365
10k US Adult Faces Database [103]	0.5966	5	2	0.5398
Denver Intensity of Spontaneous Facial Action (DISFA) Database [104]	1.2085	5	1	0.4695
IMFDB-CVIT [105]	1.3205	3	0	0.2547
SiblingsDB Database HQ Faces [106]	1.2643	4	1	0.4176
SiblingsDB Database LQ Faces [106]	0.6706	5	0	0.3225
Stirling 3D Face Dataset [107]	1.0040	4	1	0.4003
Adience [108]	0.5543	5	0	0.3147
CACD [109]	1.2337	3	1	0.3600
CelebA [90]	1.2262	4	0	0.3040
FaceScrub [110]	0.6670	5	0	0.3222
LFWA [90]	1.3276	3	0	0.2552
MOBIO - Mobile Biometry Face and Speech Database [111]	1.0501	5	1	0.4589
CAFE - The Child Affective Face Set [112]	1.0261	5	2	0.5684
UFI - Unconstrained Facial Images [113]	0.0000	5	0	0.2778
AFAD [114]	1.1887	5	0	0.3570
IMDB-Wiki [115]	0.6797	3	1	0.3231
AgeDB [79]	0.8603	4	0	0.2796
Large Age-Gap Database (LAG) [116]	0.3333	4	0	0.2444
PPB [117]	1.3274	4	0	0.3107
The IST-EURECOM Light Field Face Database [118]	1.2160	4	1	0.4144
UTK Face [119]	2.7062	5	1	0.5693
VGGFace2 [7]	0.0000	4	0	0.2222
Disguised Faces in the Wild (DFW) [120]	0.0000	6	0	0.3333
IJB-C [121]	2.1279	4	1	0.4752
IMDB-Face [122]	0.4067	4	1	0.3604
LAOFIW [123]	0.0000	5	2	0.5000
RFW [124]	1.4959	5	0	0.3775
VIP_attribute Dataset [125]	0.6667	5	0	0.3222
AAF [126]	0.7449	5	0	0.3274
BUPT-Balancedface [127]	0.3333	5	0	0.3000
BUPT-GlobalFace [127]	0.3595	5	0	0.3017
DroneSURF [128]	0.0000	6	1	0.4444
FairFace [78]	2.5357	5	0	0.4468
Indian Institute of Science Indian Face Dataset (IISCIID) [129]	1.0570	5	2	0.5705
Injured Face v2 (IF-V2) database [130]	0.0000	5	0	0.2778
SOF dataset [131]	1.3183	5	1	0.4768
BFW [132]	0.6667	5	1	0.4333
DiveFace [133]	1.6636	5	0	0.3887
FB Fairness dataset (Casual Conversations) [134]	1.5561	5	3	0.7149
MAAD-Face [135]	0.9022	4	1	0.3935
Sejong Face Database (SFD) [136]	1.0566	4	1	0.4038

Analysis across the three different dimensions has been obtained through Fig. 4 where the distribution of scores has been plotted.

Fairness in Datasets: The fairness of datasets is calculated based on Eqn. 4. Representative and balanced datasets have been shown to provide fairer performance across different demographic subgroups [76]. The fairness metric described in this work provides a maximum value of 5, with five being the fairest. The average value for the fairness score obtained for the datasets comes out to be 0.96 ± 0.64 , signifying that, on average, the fairness score of a dataset ranges from 0.32 to 1.6. The detailed results are provided in Tables III and IV for biometric and medical datasets, respectively. The UTKFace dataset is observed to be the fairest, with a score of 2.71 among the datasets listed here, providing maximum representation. It should be noted that with a maximum score of 5, the UTKFace dataset achieves slightly more than half that score. Interestingly, the average fairness score for the eight medical datasets was 1.34 ± 0.17 while the same score for biometric datasets came out to be 0.90

TABLE IV

SUMMARY OF THE DIFFERENT SCORES OBTAINED FOR FAIRNESS, PRIVACY, AND REGULATORY COMPLIANCE QUANTIFICATION OBTAINED FOR THE MEDICAL DATASETS IN THE STUDY. THE CHEST XRAY DATASETS IN THIS STUDY PROVIDE A POOR REGULATORY COMPLIANCE SCORE. THE HIGHEST WEIGHTED AVERAGE FOR FAIRNESS, PRIVACY AND REGULATORY COMPLIANCE IS OBTAINED ON THE MONTGOMERY COUNTY CHEST X-RAY SET (MC).

Dataset Name	Fairness score (Max. 5)	Privacy Score (Max. 6)	Regulatory Score (Max. 3)	Weighted Average
Montgomery County chest X-ray set (MC) [137]	1.4164	4.00	1.00	0.4278
Shenzhen chest X-ray set [137]	1.3300	4.00	1.00	0.4220
ChestX-ray8 (NIH) [138]	1.1740	4.00	0.00	0.3005
RSNA Pneumonia Challenge [139]	1.1478	5.00	0.00	0.3543
CheXpert (Stanford University) [140]	1.5318	4.00	0.00	0.3243
PadChest (University of Alicante) [141]	1.2094	4.00	1.00	0.4140
BIMCV+ dataset [142]	1.6556	3.00	1.00	0.3882
COVID-19 Image Data Collection (CIDC) [143]	1.2922	3.00	0.00	0.2528

± 0.67 .

Privacy Preservation in Datasets: The privacy preserved in datasets is computed based on the presence of privacy-compromising information in the annotations, such as names of subjects and the presence of critical objects such as credit cards. A P indicating the privacy preservation capacity and PL indicating privacy leakage of the dataset are calculated. The distribution of P for privacy quantification is presented in Fig. 4. The best value of P is 6. We observe that the DroneSURF dataset does not contain any private information, which makes it perfectly privacy-preserving. The medical datasets in the study de-identify their subjects but naturally leak information about medical conditions, while some further provide sensitive information such as location.

Regulatory Compliance in Datasets: With modern IT laws in place, the regulatory compliance of datasets is quantified based on institutional approval of the dataset, subject's consent to the data collection, facility for expungement/correction of the subject's data from the dataset. Based on these criteria, the compliance scores are calculated with a maximum value of three. The distribution of scores is provided in Fig. 4. On average, a regulatory score value of 0.58 is obtained. We observe that the FB Fairness Dataset (Casual Conversations) satisfies all regulatory compliances, thereby obtaining the maximum regulatory score, whereas most datasets provide a score of 0 or 1.

Fairness-Privacy Paradox in Datasets: Many face-based biometric datasets provide sensitive attribute information. This leads to a *fairness-privacy paradox* where the presence of these annotations enables fairness quantification but leads to privacy leakage. One way to remedy the situation is by providing population statistics in the published dataset papers instead of sensitive attribute labels for each sample. However, current fairness algorithms are evaluated through sensitive attribute annotations in the dataset, and their absence can hinder the fairness evaluation process. In differential privacy-based solutions, it has been observed that the performance degradation is unequal across different subgroups [144], highlighting the need for labels for fairness analysis. The *fairness-privacy paradox* remains an open problem for datasets containing sensitive attribute information such as biometrics and medical imaging. With ongoing discussion regarding concerns for privacy and fairness, regulations can sometimes provide conflicting guidance on privacy laws and proposed AI laws, giving researchers and industry a reason to approach this paradox with caution in dataset development. Recent work in face recognition is exploring models trained using synthetically generated datasets [145], [146], [147]. However, the training of powerful generative models utilizes large face datasets. Some diffusion-based models have also been shown to replicate the training data during generation.

Holistic View of Responsibility in Datasets: When the aforementioned factors are studied in conjunction, we obtain a three-dimensional representation of the datasets. The 3-tuple provides insight into how responsible a dataset may be considered for downstream training. To observe the behavior of the 3-tuple visually, we plotted a 3-D scatter plot for the face datasets along with a hypothetical *FPR dataset* (Fig. 5(a)). The hypothetical FPR dataset has a perfect fairness, privacy, and regulatory score. After applying the DBSCAN algorithm with $eps = 1$ (the maximum distance between two points to be considered as a part of one cluster), we observe five clusters with two outliers. The FB Fairness Dataset and the UTKFace dataset come out to be outliers with a Euclidean distance of 3.59 and 3.20 units from the *FPR dataset*. When compared to the other clusters, we observe that FB Fairness Dataset and the UTKFace dataset lie the closest to the *FPR dataset*.

Other cluster centers lie at a distance of 4.56, 4.79, 5.11, 5.20, and 5.33 units from the *FPR dataset*, with the clusters containing 4, 7, 3, 32, and 4 points, respectively. The next closest cluster is formed by the LAOFIW, 10k US Adult Faces Database, CAFE Database, and IISCFD datasets with average scores of 0.67, 5, and 2 for fairness, privacy, and regulatory compliance, respectively. Similar observations can be made when the scatter plot includes medical datasets along with the face datasets (Fig. 5(c-d)). The numerical results are tabulated in Tables III and IV. A weighted average of the three scores is calculated by dividing each score by its maximum value and then taking an average that provides a value in the range of 0 to 1 (Table III). By utilizing this average, we observe that the top three responsible datasets come out to be the FB Fairness

dataset (Casual Conversations), the Indian Institute of Science Indian Face Dataset (IISCFD), and the UTKFace dataset. A high regulatory compliance score plays an important role in the overall responsibility score of FB Fairness and IISCFD datasets. In contrast, a high fairness score imparts UTKFace a high responsible rubric value. To summarize the observations made over the existing face datasets, we find that-

- Most of the existing datasets suffer on all the three axes of *fairness*, *privacy* and *regulatory compliance* as per the proposed metric. For example, the UTKFace dataset is among the fairest datasets but performs poorly on regulatory compliance. On the other hand, the LFWA dataset lacks on all three fronts- fairness, privacy preservation, and regulatory compliance.
- While many works claim fairness as the primary focus in their datasets, these datasets provide poor fairness scores on evaluation. One such example is the DiveFace dataset. The fairness quantification of datasets using our framework shows that being fair is a major concern with 91% of the existing datasets obtaining a fairness score of two or less out of five.
- A vast number of large-scale datasets in Computer Vision are web-curated without any institutional approval. These datasets are often released under various CC-BY licenses even when these datasets do not have subject consent. We found that these datasets also fares low on the fairness front since the annotations are not always reliable, posing major risks to overall data responsibility.
- Following regulatory norms effectively improves the responsibility rubric for a given dataset; however, most datasets are not compliant based on the available information with 89% datasets having a compliance score of 0 or 1.
- When comparing fairness, privacy, and regulatory scores, it is clear that the privacy scores are higher in general. It is worth noting that privacy standards and constraints are already defined and have existed for a few years now [14], and datasets are possibly collected with these regulations in mind. This further indicates a need for fairness and regulatory constraints that promote data collection with higher fairness and regulatory standards.

Recommendations: Based on the observations of our framework on a large number of datasets, we provide certain recommendations to aid better dataset collection in the future.

- *Institutional Approval, Ethics Statement, and Subject Consent:* Datasets involving human subjects should receive approval from the institutional review board (such as IRB in the United States). Future regulations may require consent from subjects to be obtained explicitly for the dataset and its intended use.
- *Facility for Expungement/Correction of Subject's Data:* Datasets should provide a facility to contact the dataset owners to remove and/or correct information concerning the subject. This is necessary to be compliant with data privacy laws such as GDPR. Some existing datasets already provide the facility for expungement in their datasets such as the FB Fairness Dataset, IJB-C and the UTKFace datasets.
- *Fairness and Privacy:* Datasets should be collected from a diverse population, and distribution across sensitive attributes should be provided while being privacy-preserving. The proposed fairness and privacy scores can aid in quantifying a dataset's diversity and privacy preservation.
- *Datasheet:* Datasets should curate and provide a datasheet containing information regarding the objectives, intended use, funding agency, the demographic distribution of subjects/images, licensing information, and limitations of the dataset. By specifying intended use, the data can be restricted for processing outside of intended use under the GDPR. An excellent resource for the construction of datasheets is provided by Gebru et al. [38]. We propose modifications in the datasheet by Gebru et al. by adding questions concerning fairness, privacy, and regulatory compliance in datasets (Refer Tables V and VI).

Limitations: The formulation for quantification in this work considers a dataset fair based on the distribution of its labels. However, we do not account for the diversity of the data such as the presence of duplicate images for particular subgroups. Further, we do not comment on equity vs equality in the distribution of images. We note that it may be desirable to have unequal distribution between groups (e.g., when one group is harder to process than others and requires more data for the model to reach equal performance across groups) for some applications. Further, the current formulation for fairness, privacy, and regulatory scores is provided for datasets constituting individuals. While object-based datasets may also suffer from fairness issues, current data regulations are designed in accordance with the impact on human individuals. We leave analysis on object-based datasets for future work. Finally, we would like to note that the recommendations and datasheets introduced in this work are intended to establish the highest standards which can be challenging to achieve given the capabilities of current technologies. These recommendations are meant to serve as a “north star” and reaching them requires deliberate research effort. The fairness-privacy paradox remains an open problem in the community. Similarly, removing instances of data from already trained models requires *unlearning* techniques, which while being actively explored, are far from being perfect.

V. CONCLUSION

While the vast majority of the existing literature focuses on the design of trustworthy machine learning algorithms, in this work, we offer a fresh perspective for evaluating reliability through a discussion of responsible datasets with respect to fairness, privacy, and regulatory compliance. A detailed analysis is performed for face-based and chest Xray image datasets. We further provide recommendations for the design of ‘responsible ML datasets.’ With governments around the world regularizing data

TABLE V
RESEARCH QUESTIONS TO ACCOUNT FOR THE PREPARATION OF DATASETS. PARTS OF THIS TABLE ARE TAKEN FROM GEBRU ET AL.[38]. THE PROPOSED QUESTIONS ARE HIGHLIGHTED IN **BOLD**.

Category	Research Questions
Motivation	For what purpose was the dataset created? Who created the dataset (e.g., which team, research group) and on behalf of which entity (e.g., company, institution, organization)? Who funded the creation of the dataset?
Composition	What do the instances that comprise the dataset represent (e.g., documents, photos, people, countries)? How many instances are there in total (of each type, if appropriate)? What is the distribution of the instances with respect to the target or label? Is the distribution of instances in the dataset long-tailed with respect to the target or label? Does the dataset contain all possible instances or is it a sample (not necessarily random) of instances from a larger set? What data does each instance consist of? Is there a label or target associated with each instance? Is any information missing from individual instances? Are relationships between individual instances made explicit (e.g., users' movie ratings, social network links)? Are there recommended data splits (e.g., training, development/validation, testing)? Is the dataset self-contained, or does it link to or otherwise rely on external resources (e.g., websites, tweets, other datasets)? If biometric (or sensitive) information is present in the instances of the dataset such as fingerprint or faces, are these annotated? If the biometric (or sensitive) information is not annotated, is it discussed in detail in the accompanying research paper or elsewhere?
Collection Process	If the dataset is a sample from a larger set, what was the sampling strategy (e.g., deterministic, probabilistic with specific sampling probabilities)? How was the data associated with each instance acquired? Who was involved in the data collection process (e.g., students, crowdworkers, contractors) and how were they compensated (e.g., how much were crowdworkers paid)? What is the demographic of the people involved in the collection and annotation process? Over what timeframe was the data collected?
Preprocessing/ cleaning/ labeling	Was any preprocessing/cleaning/labeling of the data done (e.g., discretization or bucketing, tokenization, part-of-speech tagging, SIFT feature extraction, removal of instances, processing of missing values)? Was the "raw" data saved in addition to the preprocessed/cleaned/labeled data (e.g., to support unanticipated future uses)? Is the software that was used to preprocess/clean/label the data available?
Distribution	Will the dataset be distributed to third parties outside of the entity (e.g., company, institution, organization) on behalf of which the dataset was created? How will the dataset will be distributed (e.g., tarball on website, API, GitHub)? When will the dataset be distributed? Will the dataset be distributed under a copyright or other intellectual property (IP) license, and/or under applicable terms of use (ToU)? Have any third parties imposed IP-based or other restrictions on the data associated with the instances? Is there a repository that links to any or all papers or systems that use the dataset?
Maintenance	Who will be supporting/hosting/maintaining the dataset? How can the owner/curator/manager of the dataset be contacted (e.g., email address)? Who bears responsibility in case of a violation of rights? Is there an erratum? Will the dataset be updated (e.g., to correct labeling errors, add new instances, delete instances)? Will older versions of the dataset continue to be supported/hosted/maintained? If others want to extend/augment/build on/contribute to the dataset, is there a mechanism for them to do so? Are there specific guidelines for derivative work such as allowed/disallowed derivatives, distribution and licensing requirements?

protection laws, the method for the creation of datasets in the scientific community requires revision, and it is our assertion that the proposed quantitative measures, qualitative datasheets, and recommendations can stimulate the creation of responsible datasets which can lead to building responsible AI systems.

REFERENCES

- [1] "Face recognition on 330 million faces at 400 images per second," <https://towardsdatascience.com/face-recognition-on-330-million-images-at-400-images-per-second-b85e594eab66>, 2020.
- [2] "Hybrid AI beats eight world champions at bridge," <https://indiaai.gov.in/article/hybrid-ai-beats-eight-world-champions-at-bridge>, 2022.
- [3] "An AI used medical notes to teach itself to spot disease on chest x-rays," <https://www.technologyreview.com/2022/09/15/1059541/ai-medical-notes-teach-itself-spot-disease-chest-x-rays/>, 2022.
- [4] "First-of-its-kind trial shows AI beat humans at analyzing heart scans," <https://www.freethink.com/health/lvef-echonet>, 2022.
- [5] "AI-generated art won a fine arts competition – and artists are up in arms," <https://www.creativebloq.com/news/ai-art-wins-competition>, 2022.
- [6] NITI Aayog, "Responsible AI for all: Adopting the framework – a use case approach on facial recognition technology," https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf.
- [7] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "Vggface2: A dataset for recognising faces across pose and age," in *2018 13th IEEE International Conference on Automatic Face & Gesture recognition (FG)*, 2018, pp. 67–74.
- [8] D. Yi, Z. Lei, S. Liao, and S. Z. Li, "Learning face representation from scratch," *arXiv preprint arXiv:1411.7923*, 2014.
- [9] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, "Imagenet: A large-scale hierarchical image database," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2009, pp. 248–255.
- [10] W. A. G. Rojas, S. Diamos, K. R. Kini, D. Kanter, V. J. Reddi, and C. Coleman, "The dollar street dataset: Images representing the geographic and socioeconomic diversity of the world," in *Conference on Neural Information Processing Systems Datasets and Benchmarks Track*, 2022.

TABLE VI

RESEARCH QUESTIONS SURROUNDING THE FAIRNESS, PRIVACY AND REGULATORY COMPLIANCE OF DATASETS. PARTS OF THIS TABLE ARE TAKEN FROM GEBRU ET AL.[38]. THE PROPOSED QUESTIONS ARE HIGHLIGHTED IN **BOLD**.

	Research Questions
Fairness	<p>Does the dataset identify any subpopulations (e.g., by age, gender)?</p> <p>Which subpopulations are identified in the dataset and how many subgroups of each subpopulation are represented? (inclusivity score)</p> <p>What is the distribution of the subgroups for each of the subpopulations? (diversity score)</p> <p>What mechanisms or procedures were used to collect the data (e.g., hardware apparatuses or sensors, manual human curation, software programs, software APIs)?</p> <p>How reliable is the source of annotation for subpoulations and were the labels self-reported, apparent or classifier-generated? (label score)</p> <p>Based on the annotation in the dataset for the sensitive attributes, what is the inclusivity score, diversity score, label score and the overall fairness score?</p> <p>Are there any correlations between the sensitive attributes or with other attributes? (shortcuts/spurious correlations)</p>
Privacy	<p>Does the dataset contain data that might be considered confidential (e.g., data that is protected by legal privilege or by doctor-patient confidentiality, data that includes the content of individuals' non-public communications)?</p> <p>Does the dataset contain data that, if viewed directly, might be offensive, insulting, threatening, or might otherwise cause anxiety?</p> <p>Is it possible to identify individuals (i.e., one or more natural persons), either directly or indirectly (i.e., in combination with other data) from the dataset?</p> <p>If the data has been de-identified, what mechanism has been used for de-identification?</p> <p>Does the dataset contain data that might be considered sensitive in any way (e.g., data that reveals race or ethnic origins, sexual orientations, religious beliefs, political opinions or union memberships, or locations; financial or health data; biometric or genetic data; forms of government identification, such as social security numbers; criminal history)?</p>
Regulatory	<p>Were any ethical review processes conducted (e.g., by an institutional review board)?</p> <p>Did you collect the data from the individuals in question directly, or obtain it via third parties or other sources (e.g., websites)?</p> <p>Were the individuals in question notified about the data collection?</p> <p>Did the individuals in question consent to the collection and use of their data?</p> <p>If consent was obtained, were the consenting individuals provided with a mechanism to revoke their consent in the future or for certain uses?</p> <p>Irrespective of consent, is there a mechanism to expunge the data of individuals on request?</p> <p>What tasks has the dataset been used for (if any) and what other tasks can the dataset be used for?</p> <p>Are there tasks for which the dataset should not be used?</p> <p>If the dataset relates to people, are there applicable limits on the retention of the data associated with the instances (e.g., were the individuals in question told that their data would be retained for a fixed period of time and then deleted)?</p> <p>In case of an expungement request of data, what happens to the model trained using the previous data (if any)?</p> <p>Is there a mechanism to extract the data from the trained models?</p> <p>Do any export controls or other regulatory restrictions apply to the dataset or to individual instances?</p> <p>Does the dataset follow the applicable data privacy laws in your region such as GDPR in EU (if any)?</p>
Future Impact	<p>Has an analysis of the potential impact of the dataset and its use on data subjects (e.g., a data protection impact analysis) been conducted?</p> <p>Is there anything about the composition of the dataset or the way it was collected and preprocessed/cleaned/labeled that might impact future uses?</p> <p>Could there be any ethical concerns raised for the data?</p>

- [11] R. Geirhos, J.-H. Jacobsen, C. Michaelis, R. Zemel, W. Brendel, M. Bethge, and F. A. Wichmann, "Shortcut learning in deep neural networks," *Nature Machine Intelligence*, vol. 2, no. 11, pp. 665–673, 2020.
- [12] Z. Li, I. Evtimov, A. Gordo, C. Hazirbas, T. Hassner, C. C. Ferrer, C. Xu, and M. Ibrahim, "A whac-a-mole dilemma: Shortcuts come in multiples where mitigating one amplifies others," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2023.
- [13] R. Mehta, V. Albiero, L. Chen, I. Evtimov, T. Glaser, Z. Li, and T. Hassner, "You only need a good embeddings extractor to fix spurious correlations," in *European Conference on Computer Vision Workshops*, 2022.
- [14] General Data Protection Regulation, "Regulation eu 2016/679 of the European Parliament and of the council of 27 April 2016," *Official Journal of the European Union*. Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 20 September 2017), 2016.
- [15] Presidency of the Republic, "Law no. 13,709, of August 14, 2018," http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
- [16] Ministry of Law and Justice, "The information technology (amendment) act, 2008," https://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf.
- [17] Lok Sabha, "The personal data protection bill, 2019," http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
- [18] Minister of Justice, "Privacy protection (transfer of data to databases abroad) regulations, 5761-2001," <https://www.dataguidance.com/notes/israel-data-protection-overview>.
- [19] "Act on the protection of Personal Information Act no. 57 of (2003) (in English, unofficial translation)," <https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.
- [20] Teises Akto Registras, "The law on the legal protection of personal data of the Republic of Lithuania," <https://www.e-tar.lt/portal/lt/legalActEditions/TAR.5368B592234C?faces-redirect=true>.
- [21] New Zealand Legislation, "Privacy act 1993," <https://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html>.
- [22] National Information Technology Development Agency, "Nigeria data protection regulation 2019," <https://olumidebabalolalp.com/wp-content/uploads/2021/01/NDPR-NDPR-NDPR-Nigeria-Data-Protection-Regulation.pdf>.
- [23] Government Gazette, "Protection of Personal Information Act, 2013," https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf.
- [24] F. The Federal Council, "Federal Act on Data Protection," https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en.
- [25] Government Gazette, "Personal Data Protection Act (unofficial translation)," <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf>.
- [26] —, "Law on the Protection of Personal Data no. 6698, 2016 (in Turkish)," <https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf>.
- [27] Attorney General'S Office, "The California Privacy Rights and Enforcement Act of 2020," <https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf>.

TABLE VII

DETAILS OF THE BIOMETRIC DATASETS EMPLOYED FOR THE STUDY. THE *Demographic Attributes* SPECIFY THE ANNOTATIONS FOR ATTRIBUTES SUCH AS ETHNICITY, SKIN TONE, AGE, AND GENDER.

Dataset Name	Year	Images	Facial Tasks	Demographic Attributes	Web Collected
MORPH [92]	2006	400K	Recognition	Ethnicity, Gender, Age	No
Caltech 10K Web Faces [93]	2007	10.5K	Detection	-	Yes
FaceTracer [94]	2008	3.1M	Attribute Classification	Ethnicity, Gender, Age	Yes
CMU Multi-PIE [95]	2009	755K	Recognition	Ethnicity, Gender	No
PubFig [96]	2009	58.7K	Verification	Ethnicity, Gender, Age	Yes
Plastic surgery database [97]	2010	900 image pairs	Verification	-	Yes
Texas 3D Face recognition database [98]	2010	1.1K	Recognition	Ethnicity, Gender, Age	No
ChokePoint [99]	2011	64.2 K images, 48 videos	Person Recognition	Gender	No
SCFace [100]	2011	4.1K	Recognition	Ethnicity (Caucasian), Gender, Age	No
YouTube Faces [101]	2011	3.4K videos	Recognition	-	Yes
EGA [102]	2012	2.3K	Recognition	Ethnicity, Gender, Age	No
MOBIO - Mobile Biometry Face and Speech Database [111]	2012	75 videos	Recognition	Gender	No
10k US Adult Faces Database [103]	2013	2.2K	Recognition	Ethnicity, Gender	Yes
Denver Intensity of Spontaneous Facial Action (DISFA) Database [104]	2013	130K	Expression Recognition	Ethnicity, Gender	No
IMFDB-CVIT [105]	2013	34.5K	Recognition	Ethnicity (Indian), Gender, Age	Yes
Stirling 3D Face Dataset [107]	2013	2K (subset)	3D Reconstruction	Gender	No
Adience [108]	2014	26.5K	Age and Gender Classification	Gender, Age	Yes
CACD [109]	2014	160K	Recognition	Age	Yes
FaceScrub [110]	2014	106.8K	Recognition	Gender	Yes
SiblingsDB Database HQ Faces [106]	2014	0.4K	Verification	Ethnicity (Caucasian), Gender, Age	No
SiblingsDB Database LQ Faces [106]	2014	0.2K	Verification	Ethnicity (Caucasian), Gender	Yes
CAFE - The Child Affective Face Set [112]	2015	1.2K	Expression Recognition	Ethnicity, Gender, Age (Children)	No
CelebA [90]	2015	200K	Detection, Landmark Detection, Editing and Synthesis	Skin-tone, Gender, Age	Yes
LFWA [90] (40 attributes)	2015	200K	Detection, Attribute Classification, Landmark Detection, Editing and Synthesis	Skin-tone, Gender, Age	Yes
UFI - Unconstrained Facial Images [113]	2015	4.3K	Identification	-	Yes
AFAD [114]	2016	160K	Age Estimation	Ethnicity (East Asian), Gender, Age	Yes
AgeDB [79]	2017	16.4K	Recognition, Age Estimation	Gender, Age	Yes
Large Age-Gap Database (LAG) [116]	2017	3.8K	Verification	Age	Yes
The IST-EURECOM Light Field Face Database [118]	2017	4K	Recognition	Gender, Age	No
UTK Face [119]	2017	20K	Detection, Age Estimation and Progression, Landmark Detection	Ethnicity, Gender, Age	Yes
Disguised Faces in the Wild (DFW) [120]	2018	11.1K	Recognition	Ethnicity (Indian, Caucasian)	Yes
IJB-C [121]	2018	31.3 k images, 11.7K videos	Detection, Recognition, Verification, Clustering	Skin-tone, Gender, Age	Yes
IMDB-Face [122]	2018	1.7M	Recognition	Gender, Age	Yes
IMDB-Wiki [115]	2018	523K	Age Estimation	Gender, Age	Yes
LAOFIW [123]	2018	14K	Attribute Classification	Ethnicity	Yes
PPB [117]	2018	1.3K	Attribute Classification	Skin-tone, Gender	Yes
VGGFace2 [7]	2018	3.3M	Recognition	-	Yes
VIP_attribute Dataset [125]	2018	1K	Attribute Classification	Gender	Yes
AAF [126]	2019	13.2K	Age Estimation, Gender Classification	Ethnicity (Asian), Gender, Age	Yes
DroneSURF [128]	2019	411K images, 200 videos	Detection, Recognition	Age	No
Indian Institute of Science Indian Face Dataset (IIS-CIFD) [129]	2019	1.6K	Attribute Classification	Ethnicity (North Indian, South Indian), Gender, Age	Yes
Injured Face v2 (IF-V2) database [130]	2019	0.9K	Identification	-	Yes
RFW [124]	2019	40K	Recognition, Landmark Detection	Ethnicity, Gender	Yes
SOF dataset [131]	2019	42.5K	Attribute Classification, Detection, Recognition	Gender, Age	No
BFW [132]	2020	20K	Recognition	Ethnicity, Gender	Yes
BUPT-Balancedface [127]	2020	1.3M	Recognition	Ethnicity	Yes
BUPT-GlobalFace [127]	2020	2M	Recognition	Ethnicity	Yes
DiveFace [133]	2020	120K	Recognition	Ethnicity, Gender	Yes
FairFace [78]	2021	108.5K	Attribute Classification	Ethnicity, Gender, Age	Yes
FB Fairness dataset (Casual Conversations) [134]	2021	45.1K videos	Attribute Classification, Face Manipulation	Skin-tone, Gender, Age	No
MAAD-Face [135]	2021	3.3M	Attribute Classification	Ethnicity, Gender, Age	Yes
Sejong Face Database (SFD) [136]	2021	24.5K	Recognition	Ethnicity, Gender	No

[28] Illinois General Assembly, “Biometric Information Privacy Act,” <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004>.

[29] M. Fischer, “Texas Consumer Privacy Act,” <https://capitol.texas.gov/tlodocs/86R/billtext/pdf/HB045181.pdf>.

[30] Business and C. Code, “Texas capture or use of biometric identifier,” <https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm>.

[31] House Technology & Economic Development, “Substitute house bill 1493,” <https://lawfilesexst.leg.wa.gov/biennium/2017-18/Pdf/Bills/House%20Bills/1493-S.pdf?q=20230308063651>.

[32] N. Sambasivan, S. Kapania, H. Highfill, D. Akrong, P. Paritosh, and L. M. Aroyo, ““Everyone wants to do the model work, not the data work”: Data cascades in high-stakes AI,” in *proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–15.

[33] W. Liang, G. A. Tadesse, D. Ho, L. Fei-Fei, M. Zaharia, C. Zhang, and J. Zou, “Advances, challenges and opportunities in creating data for trustworthy AI,” *Nature Machine Intelligence*, vol. 4, no. 8, pp. 669–677, 2022.

TABLE VIII

TABLE CONTAINING DETAILS OF THE MEDICAL DATASETS EMPLOYED FOR THE STUDY. THE *Demographic Attributes* SPECIFY THE ANNOTATIONS FOR ATTRIBUTES SUCH AS ETHNICITY, SKIN TONE, AGE, AND GENDER.

Dataset Name	Year	Images	Tasks	Demographic Attributes	Web Collected
Montgomery County chest X-ray set (MC) [137]	2014	0.01K	Tuberculosis Detection	Gender, Age	No
Shenzhen chest X-ray set [137]	2014	0.7K	Tuberculosis Detection	Gender, Age	No
ChestX-ray8 (NIH) [138]	2017	108K	Thoracic Disease Classification	Gender, Age	No
RSNA Pneumonia Challenge [139]	2018	30K	Pneumonia Detection	Gender, Age	No
CheXpert (Stanford University) [140]	2019	224K	Disease Classification	Gender, Age	No
PadChest (University of Alicante) [141]	2019	160K	Disease Classification	Gender, Age	No
BIMCV+ dataset [142]	2020	2.4K	Covid-19 Detection	Gender, Age	No
COVID-19 Image Data Collection (CIDC) [143]	2020	0.95K	Covid-19 Detection	Gender, Age	Yes

- [34] A. K. Heger, L. B. Marquis, M. Vorvoreanu, H. Wallach, and J. Wortman Vaughan, "Understanding machine learning practitioners' data documentation perceptions, needs, challenges, and desiderata," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, pp. 1–29, 2022.
- [35] M. K. Scheuerman, A. Hanna, and E. Denton, "Do datasets have politics? disciplinary values in computer vision dataset development," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, pp. 1–37, 2021.
- [36] E. S. Jo and T. Gebru, "Lessons from archives: Strategies for collecting sociocultural data in machine learning," in *Proceedings of the Conference on Fairness, Accountability, and Transparency (FACt)*, 2020, pp. 306–316.
- [37] K. L. Peng, A. Mathur, and A. Narayanan, "Mitigating dataset harms requires stewardship: Lessons from 1000 papers," in *Thirty-fifth Conference on Neural Information Processing Systems (NeurIPS) Datasets and Benchmarks Track*, 2021.
- [38] T. Gebru, J. Morgenstern, B. Vecchione, J. W. Vaughan, H. Wallach, H. D. Iii, and K. Crawford, "Datasheets for datasets," *Communications of the ACM*, vol. 64, no. 12, pp. 86–92, 2021.
- [39] B. Hutchinson, A. Smart, A. Hanna, E. Denton, C. Greer, O. Kjartansson, P. Barnes, and M. Mitchell, "Towards accountability for machine learning datasets: Practices from software engineering and infrastructure," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FACt)*, 2021, pp. 560–575.
- [40] A. Paullada, I. D. Raji, E. M. Bender, E. Denton, and A. Hanna, "Data and its (dis) contents: A survey of dataset development and use in machine learning research," *Patterns*, vol. 2, no. 11, p. 100336, 2021.
- [41] T. Tommasi, N. Patricia, B. Caputo, and T. Tuytelaars, "A deeper look at dataset bias," *Domain Adaptation in Computer Vision Applications*, pp. 37–55, 2017.
- [42] K. Yang, K. Qinami, L. Fei-Fei, J. Deng, and O. Russakovsky, "Towards fairer datasets: Filtering and balancing the distribution of the people subtree in the ImageNet hierarchy," in *Proceedings of the Conference on Fairness, Accountability, and Transparency (FACt)*, 2020, pp. 547–558.
- [43] T. De Vries, I. Misra, C. Wang, and L. Van der Maaten, "Does object recognition work for everyone?" in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2019, pp. 52–59.
- [44] R. Singh, P. Majumdar, S. Mittal, and M. Vatsa, "Anatomizing bias in facial analysis," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, no. 11, 2022, pp. 12 351–12 358.
- [45] R. Schwartz, A. Vassilev, K. Greene, L. Perine, A. Burt, P. Hall, "Towards a standard for identifying and managing bias in artificial intelligence," *Technical Report, NIST*, 2022.
- [46] R. Kamikubo, L. Wang, C. Marte, A. Mahmood, and H. Kacorri, "Data representativeness in accessibility datasets: A meta-analysis," in *Proceedings of the International ACM SIGACCESS Conference on Computers and Accessibility*, 2022, pp. 1–15.
- [47] E. M. Bender and B. Friedman, "Data statements for natural language processing: Toward mitigating system bias and enabling better science," *Transactions of the Association for Computational Linguistics*, vol. 6, pp. 587–604, 2018.
- [48] A. Wang, A. Liu, R. Zhang, A. Kleiman, L. Kim, D. Zhao, I. Shirai, A. Narayanan, and O. Russakovsky, "Revise: A tool for measuring and mitigating bias in visual datasets," *International Journal of Computer Vision (IJCV)*, pp. 1–21, 2022.
- [49] A. Birhane and V. U. Prabhu, "Large image datasets: A pyrrhic win for computer vision?" in *IEEE Winter Conference on Applications of Computer Vision (WACV)*, 2021, pp. 1536–1546.
- [50] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," *Technical Report SRI-CSL-98-04, Computer Science Laboratory, SRI International*, 1998.
- [51] C. Dwork, "Differential privacy: A survey of results," in *Proceedings of the International Conference on Theory and Applications of Models of Computation (TAMC)*, 2008, pp. 1–19.
- [52] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkatasubramanian, "l-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 2007.
- [53] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *IEEE International Conference on Data Engineering*, 2006, pp. 106–115.
- [54] X. Xiao and Y. Tao, "M-invariance: towards privacy preserving re-publication of dynamic datasets," in *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, 2007, pp. 689–700.
- [55] I. Wagner and D. Eckhoff, "Technical privacy metrics: a systematic survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 3, pp. 1–38, 2018.
- [56] L. Sweeney, "k-anonymity: A model for protecting privacy," *International journal of uncertainty, fuzziness and knowledge-based systems*, 2002, vol. 10, no. 05, pp. 557–570.
- [57] T. Zhang, Z. He, and R. B. Lee, "Privacy-preserving machine learning through data obfuscation," *arXiv preprint arXiv:1807.01860*, 2018.
- [58] S. Chhabra, R. Singh, M. Vatsa, and G. Gupta, "Anonymizing k-facial attributes via adversarial perturbations," in *International Joint Conference on Artificial Intelligence (IJCAI)*, 2018, p. 656–662.
- [59] T. Li and L. Lin, "Anonymousnet: Natural face de-identification with measurable privacy," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2019, pp. 0–0.
- [60] Y. Li, W. Troutman, B. P. Knijnenburg, and K. Caine, "Human perceptions of sensitive content in photos," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2018, pp. 1590–1596.
- [61] A. Gervais, H. Ritzdorf, M. Lucic, V. Lenders, and S. Capkun, "Quantifying location privacy leakage from transaction prices," in *European Symposium on Research in Computer Security (ESORICS)*, Springer, 2016, pp. 382–405.
- [62] T. Orekondy, B. Schiele, and M. Fritz, "Towards a visual privacy advisor: Understanding and predicting privacy risks in images," in *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, 2017, pp. 3686–3695.
- [63] T. Orekondy, M. Fritz, and B. Schiele, "Connecting pixels to privacy and utility: Automatic redaction of private information in images," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018, pp. 8466–8475.
- [64] D. Gurari, Q. Li, C. Lin, Y. Zhao, A. Guo, A. Stangl, and J. P. Bigham, "Vizwiz-priv: A dataset for recognizing the presence and purpose of private visual information in images taken by blind people," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 939–948.

- [65] UNCTAD, "Data protection and privacy legislation worldwide," <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>, online; accessed 18 January 2023.
- [66] G. Greenleaf, "Global tables of data privacy laws and bills (January 2021)," 169 *Privacy Laws & Business International Report*, 6-19, *UNSW Law Research*, 2021.
- [67] —, "Now 157 countries: Twelve data privacy laws in 2021/22," 176 *Privacy Laws & Business International Report* 1, 3-8, *UNSW Law Research*, 2022.
- [68] M. Forti, "The deployment of artificial intelligence tools in the health sector: privacy concerns and regulatory answers within the GDPR," *Eur. J. Legal Stud.*, vol. 13, p. 29, 2021.
- [69] A. Goldstein, G. Ezov, R. Shmelkin, M. Moffie, and A. Farkash, "Data minimization for GDPR compliance in machine learning models," *AI and Ethics*, pp. 1–15, 2021.
- [70] A. Act, "Health insurance portability and accountability act of 1996," *Public law*, vol. 104, p. 191, 1996.
- [71] LewisRice, "U.S. state privacy laws," <https://tinyurl.com/mwmedz27>.
- [72] R. Nosowsky and T. J. Giordano, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule: implications for clinical research," *Annu. Rev. Med.*, vol. 57, pp. 575–590, 2006.
- [73] High-Level Expert Group on Artificial Intelligence, "Ethics guidelines for Trustworthy AI," <https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf>.
- [74] European Commission, "Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts," <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>.
- [75] I. Hupont, S. Tolan, H. Gunes, and E. Gómez, "The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems," *Scientific Reports*, vol. 12, no. 1, p. 10688, 2022.
- [76] M. Wang, Y. Zhang, and W. Deng, "Meta balanced network for fair face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, 2021, vol. 44, no. 11, pp. 8433–8448.
- [77] V. V. Ramaswamy, S. S. Kim, and O. Russakovsky, "Fair attribute classification through latent space de-biasing," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021, pp. 9301–9310.
- [78] K. Karkkainen and J. Joo, "Fairface: Face attribute dataset for balanced race, gender, and age for bias measurement and mitigation," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, 2021, pp. 1548–1558.
- [79] S. Moschoglou, A. Papaioannou, C. Sagonas, J. Deng, I. Kotsia, and S. Zafeiriou, "Agedb: the first manually collected, in-the-wild age database," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2017, pp. 51–59.
- [80] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [81] D.-H. Lee *et al.*, "Pseudo-label: The simple and efficient semi-supervised learning method for deep neural networks," in *International Conference on Machine Learning (ICML) Workshops*, 2013, vol. 3, no. 2, p. 896.
- [82] A. Tuan Tran, T. Hassner, I. Masi, and G. Medioni, "Regressing robust and discriminative 3D morphable models with a very deep neural network," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 5163–5172.
- [83] F.-J. Chang, A. T. Tran, T. Hassner, I. Masi, R. Nevatia, and G. Medioni, "Deep, landmark-free fame: Face alignment, modeling, and expression estimation," *International Journal on Computer Vision (IJCV)*, vol. 127, pp. 930–956, 2019.
- [84] "Findface," <https://intechlab.com/>, 2016.
- [85] "Face++," <https://www.faceplusplus.com/>, 2017.
- [86] "Social mapper," https://github.com/Greenwolf/social_mapper, 2021.
- [87] S. T. Gnanasekar and S. Yanushkevich, "Face attributes and detection of drug addicts," in *IEEE International Conference on Emerging Security Technologies (EST)*, 2019, pp. 1–6.
- [88] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *IEEE Symposium on Security and Privacy*, 2011, pp. 247–262.
- [89] G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," in *Workshop on Faces in 'Real-Life' Images: Detection, Alignment, and Recognition*, 2008.
- [90] Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep learning face attributes in the wild," in *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, 2015, pp. 3730–3738.
- [91] "Ethics guidelines, CVPR 2022," <https://cvpr2022.thecvf.com/ethics-guidelines>, 2022.
- [92] K. Ricanek and T. Tesafaye, "Morph: A longitudinal image database of normal adult age-progression," in *IEEE International conference on Automatic Face and Gesture Recognition (FG)*, 2006, pp. 341–345.
- [93] C. V. Lab, "Caltech 10k web faces," https://www.vision.caltech.edu/datasets/caltech_10k_webfaces/, online; accessed 26 January 2023.
- [94] N. Kumar, P. Belhumeur, and S. Nayar, "Facetracer: A search engine for large collections of images with faces," in *European conference on computer vision*. Springer, 2008, pp. 340–353.
- [95] A. Ryan, J. F. Cohn, S. Lucey, J. Saragih, P. Lucey, F. De la Torre, and A. Rossi, "Automated facial expression recognition system," in *IEEE International Conference on Security Technology*, 2009, pp. 172–177.
- [96] N. Kumar, A. C. Berg, P. N. Belhumeur, and S. K. Nayar, "Attribute and simile classifiers for face verification," in *IEEE International Conference on Computer Vision (ICCV)*, 2009, pp. 365–372.
- [97] R. Singh, M. Vatsa, H. S. Bhatt, S. Bharadwaj, A. Noore, and S. S. Nooreyzedan, "Plastic surgery: A new dimension to face recognition," *IEEE Transactions on Information Forensics and Security (TIFS)*, 2010, vol. 5, no. 3, pp. 441–448.
- [98] S. Gupta, K. R. Castleman, M. K. Markey, and A. C. Bovik, "Texas 3D face recognition database," in *IEEE Southwest Symposium on Image Analysis & Interpretation (SSIAI)*, 2010, pp. 97–100.
- [99] Y. Wong, S. Chen, S. Mau, C. Sanderson, and B. C. Lovell, "Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2011, pp. 74–81.
- [100] M. Grgic, K. Delac, and S. Grgic, "Sface—surveillance cameras face database," *Multimedia tools and applications*, 2011, vol. 51, no. 3, pp. 863–879.
- [101] L. Wolf, T. Hassner, and I. Maoz, "Face recognition in unconstrained videos with matched background similarity," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2011, pp. 529–534.
- [102] D. Riccio, G. Tortora, M. De Marsico, and H. Wechsler, "Ega—ethnicity, gender and age, a pre-annotated face database," in *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings*, 2012, pp. 1–8.
- [103] W. A. Bainbridge, P. Isola, and A. Oliva, "The intrinsic memorability of face photographs," *Journal of Experimental Psychology: General*, vol. 142, no. 4, p. 1323, 2013.
- [104] S. M. Mavadati, M. H. Mahoor, K. Bartlett, P. Trinh, and J. F. Cohn, "Disfa: A spontaneous facial action intensity database," *IEEE Transactions on Affective Computing*, 2013, vol. 4, no. 2, pp. 151–160.
- [105] S. Setty *et al.*, "Indian movie face database: a benchmark for face recognition under wide variations," in *National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)*, 2013, pp. 1–5.
- [106] T. F. Vieira, A. Bottino, A. Laurentini, and M. De Simone, "Detecting siblings in image pairs," *The Visual Computer*, 2014, vol. 30, no. 12, pp. 1333–1345.
- [107] P. Hancock, "Stirling/ersc 3d face database," <http://pics.stir.ac.uk/ESRC/>, online; accessed 26 January 2023.

- [108] E. Eiding, R. Enbar, and T. Hassner, "Age and gender estimation of unfiltered faces," *IEEE Transactions on Information Forensics and Security (TIFS)*, 2014, vol. 9, no. 12, pp. 2170–2179.
- [109] B.-C. Chen, C.-S. Chen, and W. H. Hsu, "Cross-age reference coding for age-invariant face recognition and retrieval," in *European Conference on Computer Vision (ECCV)*, Springer, 2014, pp. 768–783.
- [110] H.-W. Ng and S. Winkler, "A data-driven approach to cleaning large face datasets," in *IEEE international conference on image processing (ICIP)*, 2014, pp. 343–347.
- [111] P. Tresadern, C. McCool, N. Poh, P. Matejka, A. Hadid, C. Levy, T. Cootes, and S. Marcel, "Mobile biometrics (mobio): Joint face and voice verification for a mobile platform," *IEEE Pervasive Computing*, 2012, vol. 99.
- [112] V. LoBue and C. Thrasher, "The child affective facial expression (cafe) set: Validity and reliability from untrained adults," *Frontiers in psychology*, 2015, vol. 5, p. 1532.
- [113] L. Lenc and P. Král, "Unconstrained facial images: Database for face recognition under real-world conditions," in *Mexican International Conference on Artificial Intelligence*, Springer, 2015, pp. 349–361.
- [114] Z. Niu et al., "Ordinal regression with multiple output CNN for age estimation," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 4920–4928.
- [115] R. Rothe, R. Timofte, and L. Van Gool, "Deep expectation of real and apparent age from a single image without facial landmarks," *International Journal of Computer Vision (IJCV)*, 2018, vol. 126, no. 2, pp. 144–157.
- [116] S. Bianco, "Large age-gap face verification by feature injection in deep networks," *Pattern Recognition Letters*, 2017, vol. 90, pp. 36–42.
- [117] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *ACM Conference on Fairness, Accountability, and Transparency*, PMLR, 2018, pp. 77–91.
- [118] A. Sepas-Moghaddam, V. Chiesa, P. L. Correia, F. Pereira, and J.-L. Dugelay, "The ist-eurecom light field face database," in *International Workshop on Biometrics and Forensics (IWFBI)*, 2017, pp. 1–6.
- [119] Z. Zhang, Y. Song, and H. Qi, "Age progression/regression by conditional adversarial autoencoder," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 5810–5818.
- [120] V. Kushwaha, M. Singh, R. Singh, M. Vatsa, N. Ratha, and R. Chellappa, "Disguised faces in the wild," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2018, pp. 1–9.
- [121] B. Maze, J. Adams, J. A. Duncan, N. Kalka, T. Miller, C. Otto, A. K. Jain, W. T. Niggel, J. Anderson, J. Cheney et al., "IARPA Janus Benchmark-C: Face dataset and protocol," in *IEEE International Conference on Biometrics (ICB)*, 2018, pp. 158–165.
- [122] F. Wang, L. Chen, C. Li, S. Huang, Y. Chen, C. Qian, and C. C. Loy, "The devil of face recognition is in the noise," in *Proceedings of the European Conference on Computer Vision (ECCV)*, 2018, pp. 765–780.
- [123] M. Alvi, A. Zisserman, and C. Nellåker, "Turning a blind eye: Explicit removal of biases and variation from deep neural network embeddings," in *Proceedings of the European Conference on Computer Vision (ECCV) Workshops*, 2018.
- [124] M. Wang et al., "Racial faces in the wild: Reducing racial bias by information maximization adaptation network," in *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019, pp. 692–702.
- [125] A. Dantcheva, F. Bremond, and P. Bilinski, "Show me your face and I will tell you your height, weight and body mass index," in *International Conference on Pattern Recognition (ICPR)*, 2018, pp. 3555–3560.
- [126] J. Cheng et al., "Exploiting effective facial patches for robust gender recognition," *Tsinghua Science and Technology*, 2019, vol. 24, no. 3, pp. 333–345.
- [127] S. Shi, C. Guo, L. Jiang, Z. Wang, J. Shi, X. Wang, and H. Li, "Pv-rcnn: Point-voxel feature set abstraction for 3d object detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2020, pp. 10529–10538.
- [128] I. Kalra, M. Singh, S. Nagpal, R. Singh, M. Vatsa, and P. Sujit, "Dronesurf: Benchmark dataset for drone-based face recognition," in *IEEE International Conference on Automatic Face & Gesture Recognition (FG)*, 2019, pp. 1–7.
- [129] H. Katti and S. Arun, "Are you from north or south India? a hard face-classification task reveals systematic representational differences between humans and machines," *Journal of Vision*, 2019, vol. 19, no. 7, pp. 1–1.
- [130] P. Majumdar, S. Chhabra, R. Singh, and M. Vatsa, "Subclass contrastive loss for injured face recognition," in *IEEE International Conference on Biometrics: Theory, Applications, and Systems*, 2019, pp. 1–7.
- [131] M. Afifi and A. Abdelhamed, "Afif4: Deep gender classification based on Adaboost-based fusion of isolated facial features and foggy faces," *Journal of Visual Communication and Image Representation*, 2019, vol. 62, pp. 77–86.
- [132] J. P. Robinson et al., "Face recognition: too bias, or not too bias?" in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2020.
- [133] A. Morales, J. Fierrez, R. Vera-Rodriguez, and R. Tolosana, "Sensitivenets: Learning agnostic representations with application to face images," *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, 2020.
- [134] C. Hazirbas, J. Bitton, B. Dolhansky, J. Pan, A. Gordo, and C. C. Ferrer, "Towards measuring fairness in AI: the casual conversations dataset," *IEEE Transactions on Biometrics, Behavior, and Identity Science (TBIO)*, 2021.
- [135] P. Terhörst, D. Fähmann, J. N. Kolf, N. Damer, F. Kirchbuchner, and A. Kuijper, "Maad-face: a massively annotated attribute dataset for face images," *IEEE Transactions on Information Forensics and Security (TIFS)*, 2021, vol. 16, pp. 3942–3957.
- [136] U. Cheema and S. Moon, "Sejong face database: A multi-modal disguise face database," *Computer Vision and Image Understanding (CVIU)*, 2021, vol. 208, p. 103218.
- [137] S. Jaeger, S. Candemir, S. Antani, Y.-X. J. Wáng, P.-X. Lu, and G. Thoma, "Two public chest x-ray datasets for computer-aided screening of pulmonary diseases," *Quantitative imaging in medicine and surgery*, 2014, vol. 4, no. 6, p. 475.
- [138] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and R. M. Summers, "Chestx-ray8: Hospital-scale chest x-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 2097–2106.
- [139] G. Shih, C. C. Wu, S. S. Halabi, M. D. Kohli, L. M. Prevedello, T. S. Cook, A. Sharma, J. K. Amorosa, V. Arteaga, M. Galperin-Aizenberg et al., "Augmenting the national institutes of health chest radiograph dataset with expert annotations of possible pneumonia," *Radiology: Artificial Intelligence*, 2019, vol. 1, no. 1, p. e180041.
- [140] J. Irvin, P. Rajpurkar, M. Ko, Y. Yu, S. Ciurea-Ilcus, C. Chute, H. Marklund, B. Haghighi, R. Ball, K. Shpanskaya et al., "Chexpert: A large chest radiograph dataset with uncertainty labels and expert comparison," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2019, vol. 33, no. 01, pp. 590–597.
- [141] A. Bustos, A. Pertusa, J.-M. Salinas, and M. de la Iglesia-Vayá, "Padchest: A large chest x-ray image dataset with multi-label annotated reports," *Medical image analysis*, 2020, vol. 66, p. 101797.
- [142] M. D. L. I. Vayá, J. M. Saborit, J. A. Montell, A. Pertusa, A. Bustos, M. Cazorla, J. Galant, X. Barber, D. Orozco-Beltrán, F. García-García et al., "Bimcv covid-19+: a large annotated dataset of rx and ct images from covid-19 patients," *arXiv preprint arXiv:2006.01174*, 2020.
- [143] J. P. Cohen, P. Morrison, L. Dao, K. Roth, T. Q. Duong, and M. Ghassemi, "Covid-19 image data collection: Prospective predictions are the future," *arXiv 2006.11988*, 2020.
- [144] E. Bagdasaryan, O. Poursaeed, and V. Shmatikov, "Differential privacy has disparate impact on model accuracy," *Advances in Neural Information Processing Systems*, vol. 32, 2019.
- [145] H. Qiu, B. Yu, D. Gong, Z. Li, W. Liu, and D. Tao, "Synface: Face recognition with synthetic data," in *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, 2021, pp. 10880–10890.

- [146] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, D. Lawatsch, F. Domin, and M. Schaubert, “Gandifface: Controllable generation of synthetic datasets for face recognition with realistic variations,” *arXiv preprint arXiv:2305.19962*, 2023.
- [147] M. Kim, F. Liu, A. Jain, and X. Liu, “Dcfacex: Synthetic face generation with dual condition diffusion model,” in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2023, pp. 12 715–12 725.