当人脸成为数据：关于隐私问题的伦理思考

唐慧敏

（51205902133 信息学部 软件工程）

摘要：时代变迁，机器赋能。人脸识别作为新兴科技产物，给人们的生活带来了极大的便利。如今，我们随处可见人脸通过“刷脸”来办理日常业务。在水果店买了一箱苹果，通过“刷脸”就可以完成扣款支付；在银行办理业务，通过“刷脸”就可以确认身份进行取款；过年回家在火车站也不需要再用身份证取票，“刷脸”即可进站。在这个大数据共享、科技进步的“刷脸”时代，我们只要带着一张脸，就可以行走江湖。然而人脸识别技术背后的安全隐患也同样值得被关注。近些年来，人脸数据被滥用、被销售的案例层出不穷，这无疑是对个人隐私的威胁和侵害。究其根本原因，一是因为大众的隐私保护和维权意识薄弱，二是因为科技时代，侵犯隐私权的手段更加智能，更加隐蔽；三是因为行业监管缺失、标准参差不齐、数据安全防范不足，让一些企业个体钻了空子，四是因为缺少相关法律法规的严格限制，让侵权方过分猖狂。在本文中，我们首先对大数据下主体隐私权受侵的相关案例进行分析，并给出主体隐私权受到侵害的主要表现，其次对隐私权受侵的原因进行详细的探究，最后在目前现有法律法条和相关规定的基础上，给出一些建设性的建议，让大众了解到如何安全地享受科技给我们带来的便利，对科技发展下隐藏的伦理问题有所掌握。

关键词：人脸识别；隐私保护；大数据；法律法规；

1.引言

随着人工智能、物联网等前沿技术的迅速发展，智能时代已悄然到来，“刷脸”逐渐成为了新的风潮。人脸识别技术作为新兴科技产物，给人们的生活带来了极大的便利。然而，随着人脸识别技术在金融、公共安全、军事、教育、交通等领域的广泛应用，出现了企业、媒体、公共机构等对人脸的非法收集、滥用、泄露等问题，这给个人隐私安全和群体隐私安全带来了一定的隐患。

人脸识别，是基于人的脸部特征信息进行身份识别的一种生物识别技术，是一种跨学科的身份认证技术，涉及到计算机图像学、计算机视觉、比对鉴定识别等多学科技术，有些时候还需要夜间红外侦测技术、自动调整曝光技术、影像方法技术等作支持。人脸识别最初在 20 世纪 60 年代已经有研究人员开始研究，真正进入初级的应用阶段是在 90 年代后期，发展至今其技术成熟度已经达到较高的程度。整个发展过程可以分为机械识别、半自动化识别、非接触式识别及互联网应用阶段。

大数据给人脸识别技术应用带来了机遇和挑战，过去几年里，在需求的推动下，人脸识别厂商和技术研发人员从架构、产品、技术等方面进行探索，取得了一定的成效。大数据环境下人脸识别技术的工作流程如下:

人脸检测：人脸检测是人脸识别的基础，只有准确获取到人脸信息后，才能实现后续的识别和认证。从工作流程上来说，人脸检测可分为检测、定位和跟踪三个部分。检测指的是，软件通过特定程序对图像或视频信息进行初步处理，确定图像或视频中是否有人脸存在。定位则是在捕捉到人脸信息或疑似人脸信息后对图像和视频信息进行分割，找到人脸在其中的相对位置，并指出人脸的

大小、状态等相关信息。而跟踪主要指在受到光源、噪声等因素影响时，通过持续检测和定位实现准确人脸信息捕捉。

特征提取：在完成人脸检测后，则需要对图像或视频中获取到的人脸信息进行特征提取，这是实现身份认定的重要环节。从技术层面上来说，人脸识别指的是将现实空间映射到机器空间的过程，即现实信息想数据信息的转化过程。由于人脸特征受到基因和后天因素影响，因此人脸特征具有唯一性和多样性，也正是由于人脸特征的唯一性，才能准确描述人脸图像，才能实现有效的身份认证。人脸特征提取是人脸识别中技术难度最高的环节，其中有几个难点，首先人脸图像包含的信息量极大，为了提高人脸识别的速度，那么必须要对捕捉到的人脸图像进行压缩和降维，以最少的信息准确反映人脸信息，也就是捕捉人脸的特征。

人脸识别：人脸识别是身份信息认证的过程，指的是将提取到的人脸特征与已保存在人脸库中的人脸特征进行比对，找到相同或相似的人脸，并根据人脸信息调取人员身份信息，从而进行识别，这是最基本的也是最狭义的人脸识别过程。广义的人脸识别主要分为两大类，身份信息确认和身份辨认，两者的区别在于定向和不定项的差异。身份确认是狭义的人脸识别，即上述的最简单的人脸识别。其是一对一的人脸比对和确认。而身份辨认则更倾向于身份晒帅，其是一种人身信息检索，是一种不特定对象的人脸识别，指的是根据人脸特征确定身份信息，这种人脸识别在案件侦破和科幻电影中较为常见。

2. 人脸识别技术应用下的伦理问题

2.1 人脸识别技术带来的伦理问题

人脸识别技术带来的最直接的伦理危机是个人隐私权问题。由于人工智能与物联网的快速发展，“刷脸”业务呈爆炸性增长，人们的隐私数据有可能在不知不觉间就会被采集到。在一张“人脸”信息的采集图像中，人们不仅仅只暴露了“人脸”信息，人们的生活环境、日常爱好、家人朋友等个人隐私也会一起被采集到。人脸识别技术的广泛应用带来了对个人隐私问题的隐忧，也带来了个别组织对数据的滥用或垄断。在这个信息爆炸、信息共享的时代，个人隐私问题似乎被逐渐弱化。甚至可以说，我们正在主动向互联网提供自己的隐私信息，自己却毫不知情，而当骚扰电话、垃圾短信突然增多时，我们才察觉到生活被偷窥的危险气息。

个人稳私权的伦理问题首先涉及的是人脸信息采集权的问题。我们出门都会带着一张脸，而且大多情况不会进行遮挡。而人脸信息的采集技术非常成熟，人脸采集设备在大街小巷随处可见，在你不知不觉的时候，也许只需一两秒的时间就会把你的人脸信息采集完成。而从人脸信息就可以分析到你的身份信息、生活轨迹信息等等，都在我们不知情的情况下被记录和储存下来。而这一切我们毫不知情。

个人稳私权的伦理问题另外一个重要问题是人脸信息的使用。虽然人脸信息属于“弱隐私”，但也是人类独一无二的生物特征。人脸识别技术为数据的采集提供了方便的技术手段，而大数据共享形成了从“人脸信息”到“身份信息”再到“个人信息”的一个全方位的监控，构成了立体天罗地网的关系网。利用现代智能技术，可以在无人的状态下每天 24 小时全自动、全覆盖地全程监控，毫无遗漏地监视着人们的一举一动。在随处可见的人脸抓拍设备，我们的一切活动都被智能设备时时刻刻盯梢着，跟踪着。而我们的人脸信息，以数据编码的形式保留下来，它可通过互联网快速传遍各种组织世界并存储于数据云端，易传播，易存储，一旦进入网络就很难于彻底清除，因此也就

容易永久保存，不易消逝。而人脸信息与其他数据进行交叉、重组、关联等操作，就会把个人的大量稳私信息被挖掘出来。

2.2 个人隐私权被侵犯的相关表现

（一）通过整合隐私数据来挖掘商业价值

大数据时代不可忽视的便是数据，一切以数据为核心。然而如今，随着大数据规模的日益强大，我们已经可以根据相关数据分析对个人进行全方位识别和分析。以前我们不知道坐在电脑对面的是人还是聪明的动物，可现在通过我们的一系列行为数据，我们能被准确识别，我们的隐私越来越无处可藏。与此同时，隐私数据不再是我们的独占资源，价值化的特点逐渐凸显，大数据所蕴含的价值，是所有企业、商家都不愿放弃的巨大金矿，它是可以用来交易的商品。为了迎合受众、获取利益，我们随时随地被各种方式记录下来的数据被数据挖掘公司卖给需要的企业、商家，这些数据包含我们的浏览记录、购物刷卡记录、社交分享、GPS 定位等。我们的一切数据都能被商家价值化，哪怕在我们看来毫无用处的数据，在商家手中也可以被价值最大化。

（二）通过提供个性化服务以消费用户隐私

大数据时代，我们享受着各种便利的个性化服务。但是，在享受的同时，我们也在牺牲自己的隐私。当你使用社交工具发表言论、分享照片视频时，网络运营商已经在明确规划应该向你推荐的资源和广告；当你为了体验某种新奇的应用而不得不授权“允许查看隐私内容”时，应用后台并不会错过收集数据的绝佳时机；当你认为有监控的地方最有安全感时，却忽略了你的一举一动也暴露在了镜头下，而监视人员是否别有用心，这就不得而知了。

（三）侵犯手段更为智能、更为隐蔽

大数据本身具有奇特的魅力，多维数据、数据关联以及交叉复现，将看似毫无联系却环环相扣的数据挖掘出来。大数据时代，我们以透明体的姿态生存着，甚至不知道自己在什么时间、什么地点、以什么方式直接或间接地泄露着自己的隐私。大数据时代，隐私泄露悄无声息却又无处不在。全球复杂网络研究权威、无尺度网络的创立者在《爆发》一书中提出，未来人们会接受匿名的隐私泄露。但就这一问题，相关计算机的专家已经表明即便是匿名，也可以准确归属到具体的人。谷歌的一名工程师在被问到“手机与人的名字相关的信息”时表示，谷歌记录网民搜索、位置和网上行为的大型数据库中已经形成大量数据，这足以使谷歌间接地了解一个人。有网络工程师曾经表示：某些网络公司会在网页上动手脚、加代码，通过服务器收集用户信息，用户的年龄、职业、受教育程度等隐私信息都可能被窥探，对此，用户却根本无法察觉。

3.人脸识别技术应用下隐私伦理问题的归因

3.1 信息主体隐私保护意识薄弱

受社会发展和多元价值观的影响，人们的个人隐私观日益开放，个人可接受的隐私泄露底线逐渐向前推移，我们已进入到一个“弱隐私”时代。如今，通过各种网络途径向他人分享自己的生活、经历已成为人们日常生活与社交的一部分，而这些数据往往涉及个人隐私，如家庭住址、生活轨迹等，为隐私问题的滋长提供了土壤。这些信息是以数字化信息的形式存贮的，而数字化信息的特点是极易传播和扩散。信息主体隐私保护意识薄弱，甚至忽视隐私泄露的风险，有可能导致大量的个

人信息碎片被积聚、关联，形成完整的个人数字画像，最终将会暴露出个人的深度隐私。人脸识别技术的生活化应用大大削弱了人们的隐私防护意识。

3.2 信息获取配合度要求较低

传统的生物识别技术在提取特征信息过程中对信息主体的配合程度要求较高，否则可能导致无法获取特征信息或无法获得高质量特征信息，从而影响识别率。例如，指纹识别在指纹提取过程中需要信息主体提供纹路清晰的手指并按要求移动手指以保证所采集指纹的完整性。与传统的生物识别技术相比，人脸识别技术获取人脸特征信息的方式相对便捷，这归功于人脸识别技术特征信息提取配合度要求低。它不仅可以近距离获取人脸特征信息，也可通过摄像头或者遍布大街小巷的监控探头，在无需信息主体配合的情况下远距离抓取人脸生物特征而不被信息主体察觉。监控摄像大量地记录着人们的相貌特征、行为特征、生活轨迹等信息，尽管人脸识别时非接触性的无感收集已经简化了采集程序、降低了信息采集难度、加快了采集进度、减弱了对被采集者的配合要求，但其利用监控海量收集人脸信息，不仅增加了个人面部信息被非法采集的风险，在心理上也更容易使信息主体忽视其背后蕴藏的隐私风险。

3.3 行业监管缺失与相关立法滞后

行业监管不力、标准参差不齐、数据安全防范不足，从而导致人脸信息泄露，这是人们抵触人脸识别技术大范围应用的重要原因之一。目前有关人脸识别技术的行业标准尚未成体系，仅存在一些对人脸识别技术中的部分技术的统一标准。在人脸识别技术商用过程中人脸信息的采集和保管全靠商家自律，因此，在人脸识别技术应用实践中保护人脸信息主体的信息安全存在诸多障碍。相较于人脸识别技术进步与突破的速度，有关人脸识别技术应用以及人脸信息保护的立法明显出现滞后。当前涉及人脸信息隐私保护的窘境在于:对人脸识别技术的应用场景，人脸信息的采集、存储、使用环节以及权力归属还没有严格的法律限制。

4.针对人脸识别技术应用下隐私伦理问题提出的建议

4.1 加强宣传工作

信息主体的隐私观念淡薄是隐私问题产生的重要原因之一，要维护自身隐私不受侵犯还需依靠信息主体隐私安全防护意识的提升。

第一，加强潜在隐私风险教育。网络信息的发展、各项智能产品的发明拓宽了人们认识世界、改变世界的道路，同时也增加了隐私泄露的风险，譬如，非必要场合的人脸信息读取、网站注册中的详细个人信息填写、智能软件中的多种权限请求等。因此，在实际生活中，要认清各种行为背后潜藏的隐私风险，从源头杜绝个人隐私的泄露，对于有争议或不信任的软件，尽量做到少用或不用。

第二，加强数据遗忘与数据销毁意识宣传。隐私信息的数据化是当今时代的一种常态，人们的生活轨迹、行为偏好等产生的信息都能以数字形式存储，若是被大量存储与整合，那后果将不可估量，因此数据销毁与遗忘十分必要。

4.2 健全人脸识别技术隐私保护机制

首先，增加人脸识别技术设计阶段的伦理建构。从本质上看，人脸识别是携有不确定性风险的实践活动。因此，为保障其更好地为人类服务，在尊重其发展规律的基础上，可在人脸识别技术设计阶段构建技术设计伦理原则，使之成为人脸识别技术的内在标准。譬如，不伤害、公正、尊重、审慎等。其次，尝试建立人脸信息使用伦理审查系统。为数据库人脸信息集设置守门人，建立一个用于审查人脸数据集访问与使用的系统，以此保护数据库中人脸数据主体的安全与权益，进一步规范人脸信息的使用行为。系统主要关注请求者使用该数据的场合与目的，并要求数据使用者遵循数据使用的伦理合理性;如若隐瞒或者歪曲意图，则需要承担相关责任，譬如，失去数据库的访问与使用权限、赔偿巨额罚款等。这就使得你无论决定要做什么时，都把前因后果考虑进去。最后，寻求与发展人脸识别新业态。尽管人脸识别技术已初具人类视觉的基本样态，但人类视觉功能的复杂性是单一的人脸识别技术无法比拟的。随着不断出现的新的需求与变化，人脸识别技术在精准识别中难以达到人们的理想目标，很可能出现错误识别的状况。在识别过程中，人脸识别技术不如人类视觉器官的最大原因就是人类大脑拥有比人脸数据库更全面的目标特征信息，它包含但不限于声音、体型、习惯等，人类视觉器官正是在这些基础上进行识别判定。基于此，我们可以模仿人类大脑的功能，在人脸数据库的基础上增加其他特征的数据库，发展集人脸识别、声音识别、指纹识别等于一体的复合识别技术。

4.3 加强立法工作

4.3.1 我国对隐私权现行立法的规定与不足

（一）现行立法规定

目前，我国《宪法》及部分部门法中有关于保护隐私权的相关规定，然而都是采用间接保护、概括保护的方式。例如：

《宪法》第三十八条至四十条的规定中，通过“禁止用任何方法对公民进行侮辱、诽谤和诬告陷害；禁止非法搜查或者非法侵入公民的住宅；除因国家安全或者追查刑事犯罪的需要由公安机关或者检察机关依照法律规定的程序对通信进行检查外，禁止任何组织或者个人以任何理由侵犯公民的通信自由和通信秘密”的规定，对公民的隐私权予以保护。

《刑法》中通过对侵犯隐私权的严重行为处以刑罚，为公民隐私权的保护提供了有力保障。

《民法》方面，在 2009 年 12 月 26 日由全国人民代表大会常务委员会通过的《侵权责任法》中，“隐私权”这三个字第一次出现在我国的法律法规中。

（二）不足之处

1. 缺乏针对性、系统性的保护体系

在大数据时代，我国针对保护隐私权制定的相关法律法规虽然不在少数，但仍然存在较为分散且缺乏针对性、系统性的问题，尚未形成系统化的保护机制。由于缺少专门性的法律规定，难免会

导致在具体操作中出现执行难的问题。

2. 对隐私权的保护不具体

首先，对隐私权的侵权主体方面并未全面涵盖，大数据时代侵权主体更为多元化，在网络用户、网络服务提供者之外，当企事业单位、政府机构等人员在开展信息收集、社会监控等工作时，由于技术失当、管理欠佳、侥幸心理等造成对公民隐私权的侵犯时，同样应成为追责对象。其次，对侵犯隐私权的行为规范，划分得并不详细。例如，对公民的隐私权保护方面常常受到“特殊情况”的限制，这并不是说不容许特殊情况的存在，但是当考虑到现实操作问题时，还是应当对“特殊情况”界限划分、明确范围等方面给出更为准确、更为具体的规定。

3. 对隐私权的救济不到位

我国对隐私权的救济主要集中在《侵权责任法》，如第三条规定，“被侵权人有权请求侵权人承担侵权责任”，但是从整体来看，我国法律法规在大数据时代对网络隐私权的法律保护仍然很薄弱。首先，救济制度总量较少，对具体的程序、内容方面的阐述十分简单。其次，救济方式较为单一，大数据时代侵犯隐私权的后果已经不局限于精神方面，物质方面的影响也不容忽视。大数据时代的隐私已经被价值化，而目前我国并未就隐私权的物质赔偿标准方面作出更为细致的规定。

4.3.2 大数据时代隐私权保护制度的完善

在分析完大数据时代我国隐私权问题的法律保护现状及存在的不足后，应从以下几个方面完善隐私权法律保护制度：

（一）加强隐私权保护立法的系统性

一个国家的法律应该是一个统一体，具有一定的系统性和针对性。如果说之前互联网的发展、大数据时代的态势尚在可控范围内，那么如今随着网络隐私权问题的日益凸显，隐私权保护体系的完善自然应当受到重视。首先，要完善我国民法体系中的相关规定，如在大数据时代来临时，关于网络隐私权的概念虽然已经在学者界达成共识，但还需立法上的明确界定。其次，《侵权责任法》也要结合大数据时代对隐私权保护提出的挑战不断改进、完善。最后，要根据相关法律法规的规定，全面构建我国对网络隐私权的保护体系，增强保护的针对性以应对日益复杂的大数据时代侵犯隐私权的问题。

（二）明确界定隐私权的保护范围

就目前我国对隐私权的立法保护不难发现，散见于各种实体法、部门法中涉及隐私权的规定都只是具备原则性，没有明确网络隐私权的保护范围，没有作出具体界定，在实际操作中还是会遇到各种问题，如果单纯依靠法官自由心证，过于原则的规定会造成同一案件不同法官的不同判决，在受理案件时分歧便已经存在，因此明确界定隐私权的保护范围势在必行。然而不得不加以重视的是，大数据时代隐私权也有了新的发展。大数据时代下，隐私呈现数据化的特点，这使得我们在界定隐私权的保护范围时应充分考虑到大数据时代的特点，相应地扩充隐私权的保护范围。比如说在包含个人生活自由权、个人生活情报秘密权、个人通讯秘密权、个人隐私利用权的基础上，可以尝试纳入赋予公民对个人数据信息支配选择的权利、对个人数据信息的知情权与同意浏览权、对个人数据信息安全的请求权与必要时获得合理赔偿的权利，网络数据信息方面的相关内容均应纳入隐私权的保护范围，以便由消极的防御变为积极的保护。

（三）完善追责与权利救济机制

如果没有有效的追责机制及合理的权利救济机制，公民享有的权利再多、再大，也难以保证其得以实现。大数据时代，我们的隐私正在通过更为隐匿的途径被窃取。与大数据相伴而生的侵犯隐私的案件及滋生的信息诈骗等案件并不在少数，但是不少人却自认倒霉，甚至会将隐私泄露全部归

结于自己没有加强防范上。殊不知，在大数据时代数据整合的强大已经让隐私泄露防不胜防，单纯以个人之力难以切实保障自己的权利。鉴于侵权主体的广泛性、复杂性，以及侵权方法、手段的多样性、多变性，想要通过公民个人防范的方式杜绝隐私侵权现象已不太可能。想要切实保护隐私权，改进追责与权利救济机制显得尤为重要。对此，一方面，必须要从源头入手，以网络用户、网络服务提供者、政府、企事业机关等容易侵犯公民隐私权的主体为对象，建立持续监管机制并确定明确易操作的追责机制。明确侵犯隐私权的法律后果，如禁止相关企业在一定期限内进入本行业内从业、处以一定金额的罚款等。另一方面，可以探索检察机关提出的针对互联网巨头等侵犯隐私权行为的公益诉讼制度，并不断修改完善权利救济规则与标准，如被告确立规则、举证规则、侵害隐私权的赔偿标准等。这样一来，不仅从源头上有效降低了网络侵权的可能性，而且也大幅度提高了公民维权的成功率。

参考文献：

[1] 秦鸿，李泰峰，郭亨艺，等.人脸识别技术在图书馆的应用研究[J].大学图书馆学报，2018(6):49－54.

[2] 庞德．法理学:第 3 卷[M]．廖德宇，译．北京:法律出版社，2008:45.

[3] 李正风，丛杭青，王前．工程伦理［M］．北京:清华大学出版社，2016:255.

[4] 德沃金．认真对待权利［M］．北京:中国大百科全书出版社，1998:6.

[5] 国家市场监督管理总局，国家标准化管理委员会．信息安全技术个人信息安全规范:GB/T35273—2020［S］．北京:中国质检出版社，2020.

[6] 毕玉谦，洪霄．民事诉讼生成权利规制探析:以“人脸识别第一案”为切入点［J］．法学杂志，2020(3):53－62.

[7] 甘绍平．伦理学的当代建构［M］．北京:中国发展出版社，2015:2－5.

[8] 王俊秀．数字社会中的隐私重塑:以“人脸识别”为例［J］．探索与争鸣，2020(2):86－90.

[9] 巴拉巴西．爆发:大数据时代预见未来的新思维［M］．马慧，译．北京:中国人民大学出版社，2012:8.

[10] 刘宏恩．人群基因数据库法制问题之研究:国际上发展与台湾现况之评析［J］．律师杂志，2004(303):71－94.

[11] 张虹，熊澄宇.用户数据:作为隐私与作为资产?———个人数据保护的法律与伦理考量[J].编辑之友，2019(10):74－79.