透过“人脸识别”看个人信息保护

◆王娇娇

(广西大学，广西 南宁 530000)

【摘要】随着“人脸识别”技术的广泛应用，由此滋生的法律问题也越来越多。本文透过“人脸识别第一案”，总结了人脸识别技术中存在的侵犯隐私权、兜售个人信息泛滥、无法删除“人脸数据”等问题。本文结合现行法律规定，对个人信息保护的路径进行了探讨，提出了进一步完善相关法律法规、建立以“合法、正当、必要”为原则的技术准入审查机制、信息收集者应严格遵守“知情＋同意”处理规则、对举证责任进行协调、加入惩罚性赔偿制度等建议。

【关键词】人脸识别；个人信息；保护

以数据作为支撑的现代经济背景下，一大批崭新的科技在促进生活进步的同时，也给人们的安全带来了一定的影响。首先需要重点注意的就是“人脸识别”技术。人脸识别，指的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。用摄像机或摄像头采集含有人脸的图像或视频，并自动在图像中检测和跟踪人脸，进而对检测到的人脸进行面部识别的一系列相关技术。不论是乘坐高铁、飞机等交通设备，还是办理银行业务、行政事务，抑或是在购物环境下，这项新兴技术无时无刻都在影响着我们。但是不可否认的是，“人脸识别”这项新兴技术的广泛使用，已经产生了一定的安全隐患，也给监管部门带来了前所未有的挑战，更对当前相关立法设计带来了冲击。如何有效地保护“人脸识别”主体的相关权益，成了法学界重点关注的问题。本文通过对“人脸识别第一案”，对“人脸识别”所承载的个人信息保护问题进行了思考。

一、透过“人脸识别第一案”看普遍问题

2019年，郭某作为浙江理工大学特聘副教授，购置了杭州野生动物世界的双人年卡，所签订的合同确认进入方式是指纹识别。同年，野生动物世界曾两次要求郭某将进入的方式变更为“人脸识别”，但后者认为属于高度隐私不同意变更并要求动物世界退卡，后双方协商无法达成一致。郭某在2019年10月28日将动物世界告上法庭，之后经过一审、二审审理，最终杭州中院作出了终审判决，要求赔偿损失共计1038元，并要求杭州野生动物世界删除当初所采集拍摄的面部照片，并增判了一项，要求野生动物世界删除当时采集的郭某的指纹识别信息。这便是所谓的“人脸识别第一案”。虽然费尽周折后仅获得门票价格的赔偿数额，但是也吹响了“人脸识别”所承载的信息保护的号角。但是需要注意的是，这个案件只是个人信息被侵犯类案的冰山一角，人脸识别技术为我们带来便利的同时，对社会大众的安全也带来了冲击和隐患，具体还包括如下情形。

其一，人脸识别对隐私权的冲击。人脸识别“隐蔽性”的优势在快捷支付、刑事侦查过程中体现得淋漓尽致，方便快捷、隐藏性强且可结合大数据可实现快速查找，是人脸识别的特性。但是正因为该种性质，也导致使用“人脸识别”侵犯隐私权的情形常常发生。通过“人脸识别”技术加上“AI”技术，使数据处理能力大为提升，这对于隐秘信息的合成更加迅速。在实践中更是出现了诸如“航班信息”“住址信息”等私人信息的泄露，这对于隐私权的冲击是毋庸置疑的。

其二，兜售“人脸数据”在内的各种个人信息相关行为泛滥。这类行为对于人们的生活、工作不仅带来的是不便，更重要的是威胁了生命、财产安全。很多电信诈骗、网络诈骗案件的发生，就是从犯罪人员通过不法分子购买个人信息开始的，犯罪人员一旦掌握一个人的准确信息，就可以快速突破受害人的防备，获得信任，从而方便进一步实施诈骗。

其三，人们无法要求删除自己的“人脸数据”。在生活中，能掌管“人脸数据”的主体不光是行政机关，还有很多民营企业。这些企业以“提供便利性”为理由或者通过加装“摄像头”，在客户无意识间肆意收集“人脸数据”之后，是否按照约定或规定使用数据，人们无从得知，甚至无法要求删除自己的“人脸数据”。

二、现行法律法规的相关规定

随着人脸数据的广泛应用，民众关于个人信息滥用的担忧也在不断加深。对此，学界亦达成共识，即有必要加强个人信息的保护。同时，个人信息保护的法律法规也在不断地完善。当然，“人脸识别”所指向的是人们的个人信息，因此，现行法律法规对于个人信息的规定，均适用于“人脸识别”所承载的信息。

(一)《民法典》

《民法典》第1935条对处理个人信息予以了规定。此

条可以说是在《网络安全法》第41条的基础制定的，继承了其合法、正当、必要原则的精神，但《民法典》扩大了适用此条例的主体，即有能力处理个人信息的主体都必须受到此条例的限制。在处理个人信息的过程中，规定必须征得自然人监护人的同意，指的是个人信息涉及无民事行为能力人或者限制民事行为能力人的，须征得其监护人的同意，否则构成侵害个人信息的行为。同时，《民法典》将收集、使用个人信息改称为处理，并增设尾款“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等”，将数据生命周期的全过程均纳入规制的范围。

虽然在有些情形下，收集者没有经过个人信息被收集者的同意，也不一定必然导致侵权的结果，收集者无需承担侵权责任，这在《民法典》第1036条有所规定，即免责事由。《民法典》列举了三种免责事由，包括已经知悉并同意后的合理使用行为，自行公开或者已经公开的个人信息，为维护被收集人的合法利益或者为维护国家、公共利益而收集使用的行为。这是因为《民法典》需要保证在正常的社会交往中合理处理个人信息，兼顾个人信息自由流动的规则。但是，某些国家或者地区的公法规定的个人信息处理应有豁免。从本质上讲，《民法典》规定的合理限制是基于目的限制的原则，超出对个人信息原始处理的目的是不合理的，属于非法处理个人信息的行为。但仍需注意的是，在实践中，还需进一步明确本条款的具体适用场景。如果对此不作说明，滥用该条款可能会导致其他条款浮出水面。

（二）《个人信息保护法》

为了进一步保护个人信息权益，规范个人信息利用活动，《个人信息保护法》于2021年11月1日正式实施，确立了个人信息保护方面的一些基本原则和具体规则，我国关于个人信息保护的法律体系得到进一步完善。但这不意味着个人信息保护中的现实问题均得到了解决。

《个人信息保护法》目前存在以下几个问题：其一，在内容上，《个人信息保护法》以原则性规定为主，缺乏进一步可操作化的详细规定，比如第66条关于“法律责任”部分规定：“对于违法处理个人信息的个人信息处理者，经责令改正拒不改正的，可以并处一百万元以下罚款。情节严重的，可以并处五千万元以下或者上一年度营业额5%以下罚款……”。对于违法的个人信息处理者设定了高额的罚款，却没有相应的裁量权的行使基准，在具体应用中很容易造成同案不同判等不公平现象的发生。其二，在范围上，《个人信息保护法》以规制私主体的个人信息活动为主，故有人认为其应当归属于民事法律规范，若真如此，个人信息的行政保护力度势必会大打折扣。在个人信息采集和使用的过程中，个人和行政机关之间可能会存在两种关系：（1）行政机关代表国家和个人之间的管理和被管理的关系；（2）个人求助于行政机关保护其信息权益的保护和被保护关系。前者可能出现的是侵权，后者可能出现的是行政不作为，均归《个人信息保护法》规范。故需要合理界定公权力利用个人信息的权利，进一步规范行政机关收集人脸信息的适用情形。

三、保护路径探析

“人脸识别”技术对生活品质的提高作用毋庸置疑，对未来构建智能社会共同体也具有不可或缺的作用，如何在社会生产效率和社会安定之间做好平衡，是当代法律共同体需要重点考虑的问题和方向。本人认为，对“人脸识别”中的个人信息保护应当从以下几个方面入手。

（一）进一步完善相关法律法规

如前文所述，《个人信息保护法》仍存在条款原则化，缺乏进一步可操作化的详细规定、行政属性不明等问题，故有必要进一步统一执法标准、约束行政机关等公权力。首先，需要加强顶层设计，完善关于人脸识别或者个人信息保护的法律、法规体系。可以结合司法实践需求和地方性行政法规的经验，制定更加细化、完善的法律或者行政法规。其次，需要统一违法行为类型、违法情节的认定标准。有利于行政机关结合实际作出公平合理的处罚，防止“同案不同判”情形的发生。最后，需要扩大规范范围，将对公权力的约束纳入进来。

（二）建立以“合法、正当、必要”为原则的技术准入审查机制

以“人脸识别”技术为代表的生物识别技术，由于对人们的人身安全、财产安全带来了威胁，因此，有必要建立“人脸识别”的技术准入审查机制。本人认为，该审查机制必须以“合法、正当、必要”为原则，由专门的行政机关进行严格审查，充分保障人们的合法权益。若不符合上述原则不得准入，或者在“人脸识别”技术使用过程中违背了上述原则，也应当进行相应的惩罚。具体而言，可以从以下几个方面入手。

首先，通过国家强制力，以专项法律或行政法规的形式强制要求在技术适用前进行全面的技术检测和信息安全影响评估，并禁止豁免评估的例外情形。其次，设立合法、正当、必要三重审查维度。人脸识别技术应用中的个人信息处理应从严贯彻“合法、正当、必要”原则。最后，人脸信息存储安全应作为准入审查重点。人脸识别技术的实践无可避免地需要筛选捕捉人脸图像进行数据库比对。因此，人脸识别数据库势必包含大量人脸信息样本。面对海量人脸信息存储需求，人脸识别技术中的存储安全设置必须作为事前准入评估重点。

（三）信息收集者应严格遵守“知情＋同意”处理规则

《民法典》第1035条和《个人信息保护法》第14条规

定了“知情＋同意”的个人信息处理规则，运用到人脸识别技术中，内容具体如下：首先，充分履行告知义务。 任何主体(包括组织或者机构甚至自然人)如果要使用“人脸识别”技术，必须将包含所收集的个人信息范围、储存位置、联系方式、安全条款、信息收集目的等全面告知，应当做到通俗易懂、言简意赅和不能保留的原则，并且应当给被告知人选择权，而非不同意就不能使用其他功能或者服务内容。同时，如果告知的内容存在预备格式和条款，则应当对该条款在相关部门进行备案，不得随意对条款进行变更。 其次，限制概括同意的适用情形。 通常情况下，人脸识别的适用存在以下两种情况：其一，法律法规允许收集的情形，譬如涉及公共利益、国家安全等情形；其二，法律法规不禁止收集，但是应当经过被收集人书面同意的情形。 对于第二种情形，一般要求对于告知条款表述非常详尽，但对于第一种情形却不尽然，通常只需要概括同意即可。 这种情况下应当严格把控，严防借“公共利益、国家安全”的名义擅自使用人脸数据。

(四)考虑对举证责任进行协调

在实践中，遇到“人脸识别”等技术侵犯个人信息权的情形，受害者往往难以证明受到的实际损害，更难以或者无法证明侵权人的过错。 例如，在郭某案中，动物园将其入园方式从指纹识别修改为人脸识别，很难说其给郭某造成了什么实际的损害。 即使真造成了实际损害，也可能存在多种原因，难以认定所诉的信息处理者的责任份额具体为几成，导致侵权者以已经尽到法律法规相关义务而逃脱应当承担的责任。 所以在侵权行为发生时，受害者因为无法证明信息泄露环节发生在收集、储存、使用的哪个过程，也无法证明是以什么方式泄露的，所以必然承担举证不利后果，最后只能承担败诉的结果。 因此，在涉及个人信息侵权案件时，立法者应当对举证责任做好协调和平衡，充分保护被害者的合法权益。

(五)加入惩罚性赔偿制度

当前侵权责任采用的是“衡平”机制，即赔偿范围以受害者既有的损失范围为准，但是由于信息在当前的数字社会产生了越来越大的商业价值，受害者一方面很难证明自己的既有损失范围，另一方面也很难证明侵权人的获利范围，因此，所得到的赔偿款非常有限。 正是在这样侵权成本如此低廉的背景下，当今个人信息侵权案件屡禁不止，对不法商家无法产生足够的威慑。 因此，本人建议加入惩罚性赔偿制度，一旦侵权行为成立则适用该制度，通过社会监督的方式进一步迫使个人信息收集的不法商家付出应有的代价，以使得“个人信息”保护更加完善和稳定。

人脸信息是我们个人身份的显著标识，可以直接关联到我们的银行账户和行程轨迹，且由于人脸信息具有唯一性和不可修复性，一旦我们的人脸信息被泄露可能会造成无法预估的损失和风险。 面对新技术带来的新问题，我们需要在法律层面上不断完善，设定公平合理、切实可行的条款，以更好地满足社会需求和发挥法律功效。

参考文献：

[1]张新宝.论个人信息保护请求权的行使[J].政法论坛,2023,41(02):26-37.

[2]冯静.个人信息立法保护问题研究[D].兰州:兰州大学,2009.

[3]王毓莹.人脸识别中个人信息保护的思考[J].法律适用,2023(02):15-24.

[4]孙佳倩.个人信息立法保护问题探讨[J].长江技术经济,2021,5(S1):161-163.

[5]刘双阳.数据法益的类型化及其刑法保护体系建构[J].中国刑事法杂志,2022(06):37-52.

[6]蔡一博,郭福卿.隐私与个人信息区分下的衔接保护[J].学术交流,2022(12):105-118.

[7]吴文芳.劳动法典中的个人信息保护[J].北方法学,2022,16(06):44-48.

作者简介：

王娇娇(1993－),女,汉族,河南驻马店人,硕士研究生,研究方向:刑法学。