从“中国人脸识别第一案”看个人信息保护

2020-12-30

我们经常折服于科技的力量，也时常对于科技带来的变革深感恐惧。随着信息技术的快速发展和互联网应用的普及，越来越多的组织大量收集、使用个人信息。在给人们生活带来便利的同时，也出现了对个人信息的非法收集、滥用、泄露等问题，个人信息安全面临严重威胁。

个人信息的“不可再生性”和“稀缺性”远胜于其他一般信息，因此作为交易相对方的信息收集者（控制者、使用者）对其有更强的交易欲望，并愿意为此承担更高的法律风险。商家有足够的动力去用、用户缺乏控制和维权能力、一旦出现个人信息泄漏和滥用可能造成财产安全、人身安全、隐私安全、网络安全等多方面严重后果，这使得新技术的应用在效率和安全两端出现了明显的失衡，需要法律发挥作用来调和矛盾。

一、个人信息（权）的概念

个人信息（Personal Information），是指与特定自然人相关联的、反映个体特征的具有可识别性的系统符号，包括个人身份、职业、家庭、财产、健康、教育、行踪等各方面的信息[1]。根据我国《民法典》相关规定，以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等可认定为个人信息，且应当受到法律保护[2]。

具体来说，作为个人信息所识别的特定人享有：
1）信息控制权。即有权直接支配个人信息并排斥他人的不法干涉，决定是否同意他人收集、处理自己的个人信息；
2）信息知情权。即有权了解他人收集（处理）自己个人信息的规则、目的、方式和范围[3]，且有权向信息控制着依法查阅、抄录或者复制其个人信息[4]；
3）信息完整权。具体而言：a.发现他人收集的信息有错误的，有权提出异议并请求更正[5]；b.有权禁止信息收集者篡改其收集（存储）的个人信息[6];
4）安全维护请求权。即有权请求信息收集（控制）者采取技术措施和其他必要措施，确保其收集（存储）的个人信息安全，防止信息泄露、篡改、丢失，且发生或者可能发生个人信息泄露、篡改、丢失的，有权请求信息收集（控制者）及时采取补救措施，并依照规定告知当事人并向有关主管部门报告[7]；
5）信息清除权（也称被遗忘权）。在出现法律规定或者当事人约定不应继续保留个人信息的情形时，个人信息权人有权请求信息收集（控制）者及时删除。[8]

二、个人信息的收集（处理）的原则与规则

个人信息（权）属于支配权（或称具有支配性的受保护法益），权利人享有信息自决权，具体包括上述五项权能。根据我国法律法规，在实施收集、处理[9]个人信息的行为时，须遵循特定的原则与规则。

(一) 合法原则

第一，收集信息的主体须合法。法律授权的主体（如国家机关），无论个人信息权人是否同意，有权在法律授权的范围内依法收集

（处置）个人信息；法律授权以外的主体，需经个人信息权人同意，才有权收集（处理）个人信息。
第二，收集信息的手段须合法。[10]

(二) 正当原则

第一，不能超越法律规定或者当事人约定的目的范围收集（处理）。
第二，收集（处理）的目的一旦实现，应当立即删除收集（处理）的个人信息。

(三) 必要原则

信息收集（处理）人在从事以特定活动时，应确定是否有收集（处理）个人信息的必要性。若不具备必需性或具备低标准可替代性，应尽量不收集（处理）或尽可能少量收集。另外，对于收集一般信息即可满足必要性要求的情况，则应当不收集敏感信息[11]。

(四) 知情同意规则

具体而言，包括：
第一，公开收集（处理）信息的规则。[12]
第二，明示收集（处理）信息的目的、方式和范围。[13]
第三，除依法无须同意外，须经个人信息权人或其监护人的同意。[14]
第四，未经被收集者同意，不得向他人非法提供个人信息，但是经过加工无法识别特定个人且不能复原的除外。[15]

(五) 维持信息安全规则

第一，收集信息（处理）人应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失。
第二，发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，并履行报告义务。[16]

(六) 维持信息完整规则

第一，信息收集人不得篡改其收集（处理）的个人信息。
第二，个人信息被收集者发现收集（处理）的信息有错误的，有权提出异议并请求及时采取更正等必要措施。[17]

三、“中国人脸识别第一案”：郭某诉杭州野生动物世界有限公司服务合同纠纷

案情简述：2019年4月，郭某支付1360元购买野生动物世界“畅游365天”双人年卡，确定指纹识别入园方式。郭某据此留存了姓名、身份证号码、电话号码等，并录入指纹。后野生动物世界将年卡客户入园方式从指纹识别调整为人脸识别，并更换了大堂告示。2019年7月、10月，野生动物世界两次向郭某发送短信，通知年卡入园识别系统更换事宜，要求激活人脸识别系统，否则将无法正常入园。此后，双方就入园方式、退卡等相关事宜协商未果，郭某遂提起诉讼，要求确认野生动物世界店堂告示、短信通知中相关内容无效，并以野生动物世界违约且存在欺诈行为为由要求赔偿年卡卡费、交通费，删除个人信息等。

2020 年11 月 20 日，本案正式宣判。判决野生动物世界赔偿郭某合同利益损失及交通费共计1038元，删除郭兵办理指纹年卡时提交的包括照片在内的面部特征信息。

争议焦点：经营者处理消费者个人信息，尤其是指纹和人脸等个人生物识别信息行为的评价和规范问题。

案件分析：本案中，消费者在办理年卡时，野生动物世界告知购卡人需提供部分个人信息，未对消费者作出不公平、不合理的要求，此时郭某的信息知情权和对信息控制权并未受到侵害。郭某随即依此作出真实意思表示，行使信息控制权，同意提供指纹等个

人信息而成为年卡客户。据此，野生动物世界在经营活动中收集郭某指纹等个人信息的行为并未违反前述合法、正当原则及规则的要求。

但是，野生动物世界在合同履行期间将原指纹识别入园方式变更为人脸识别方式，要求收集郭某及其妻子的照片信息，由于指纹识别已经可以满足对于入院人员身份的识别功能，故另行要求消费者提供额外生物信息超出了法律意义上的必要原则要求，不具有正当性。此外，此行为属于单方变更合同的违约行为，店堂告示和短信通知的相关内容不构成双方之间的合同内容，对郭某不具有法律效力，郭某作为守约方有权要求野生动物世界承担相应法律责任。

若在上述服务合同中，未约定指纹信息的采集，仅要求消费者提供一般个人信息，如姓名、出生日期等，那么此时野生动物园是否有权主张郭某进一步补充生物信息的采集？

首先，根据合法原则，法律授权以外的主体即公园等公共场所，需经个人信息权人同意，才有权收集（处理）个人信息。反之，未经当事人同意，公园无权对个人敏感信息进行采集，相应的只能依照既有约定采取核对姓名等个人信息的方式进行身份核查。

第二，即使当事人同意，个人信息的收集（处理）也应当符合必要原则。根据商业惯例和交易习惯，公园提供年卡服务通常要求合同相对方消费者身份明确，且在合同履行的过程中，公园仅针对合同相对方提供服务，即实名制办卡、用卡，消费者不得进行转让、转借、转租等行为。据此，为保证对持卡者身份的有效识别，要求消费者提供可供识别的生物信息，则可根据个案认定是否具有必要性。例如，如客流量较大的公共场所，低效的查验证件方式无法满足身份核查的需求，那么经消费者同意，采取生物样本作为识别标本可认定为具有必要性。再如，展销会等低频次活动，即使需要核查参会者信息，由于活动具有为年度或季度性，个人敏感信息的采集的必要性则需要进一步推敲。

四、关于合法原则的探讨

在2020 年上半年，数家互联网公司日以继夜地工作，通过自己的数据和技术能力，给有关部门提供了大量的数据支撑，为传染源人员的筛查、追踪、控制和隔离作出了巨大的贡献。然而，在个人信息保护法理中，无论是收集信息还是改变信息使用目的，均需要有合法性基础。

如何判断数据共享行为的合法性，换句话说，即使是无需个人信息权人同意仍有权收集（处理）信息的法律授权的主体，其法律授权范围为何？

对此，《网络安全法》并没有作出相应的答案；国家标准《个人信息安全规范》中关于同意的例外规定[18]对此有所回应，但是由于此规范没有法律强制力，仍无法解决合法性欠缺的相关问题。然而，《传染病防治法》和《突发公共卫生事件应急条例》[19]却赋予了人民政府、卫生行政部门、疾病预防控制机构、医疗机构非常强的信息收集、发现的权利。据此，人民政府可以在“突发公共卫生事件应急预案”中将信息收集、发现的权力再次授权给相关部门、机构、组织，这其中就可能包括公安部门、基层一线工作人员；任何单位和个人均应该配合，包括相关信息的提供。基于特别法优于一般法原则，即使《网络安全法》没有相关规定，依据上述《传染病防治法》和《突发公共卫生事件应急条例》，疫情期间的个人信息收集（处理）仍符合合法原则。

我国网民规模达8.54亿，其中使用手机上网的比例达99.1%，手机和APP已成为生活必备品。通过对相关软件监控，有关部门、企业等可以获得大量的个人信息，包括交易/支付信息、火车票/机票/汽车票等行程信息、住宿信息、行车/导航记录信息、收货地址信息等相关购物信息等。广泛收集个人信息的背后，势必存在一少部分的管理与使用不当等现象。对个人信息的保护不力将直接影响到后续信息采集过程中公众、机构对采集方的信任问题导致效率、精度等下降。但由于法的滞后性，相关法律法规并未及时跟上技术的日新月异。我国尚未制定《个人信息保护法》，实践中，相关机构、组织主要根据各领域相关法律法规中的概括性规定对个人信息进行收集（处理）。对于有权收集（处理）相关个人信息的明确主体、权力边界、合法收集（处理）信息的手段、个人数据保护的方法、侵权救济等一些列具体问题仍未得到明确的回应，立法实践中可参考域外司法实践的相关经验并结合我国立法环境特点，颁布实施《个人信息保护法》进行完善。

五、关于必要原则的进一步论述：存储个人信息的必要性

两个现象：

现象1：2020 年，新冠疫情全球肆虐，幸运的是我国采取了强有力的手段，迅速控制了各地的疫情，社会生活也随之快速重回正轨。对于疫情控制十分重要的一项举措就是个人信息的监控与追溯。无论是健康宝，还是每日体温检测都可以帮助有关部门迅速锁定疑似病例，并采取有效的行动。然而，在我们配合体温测量的同时，各种检测方式对于个人信息采集的程度却有所不同。如地铁、火车等大型人口密集型场所采用的红外感应测量无需核对个人身份，仅需通行者通过指定闸门，即可获得其的体温信息；然而，多数办公场所，则采取使用手持体温计测量体温，并进行相关信息的登记的方式（包括：姓名、身份证号码、电话号码、往来地址等信息）进行核查。前者对个人信息的采集未同步存储，而后者则具有存储性质。

现象2：由于网络交易的便捷性与经济性，网购已经成为了人们生活的一部分。但与此同时我们的个人信息却一直被电商平台收集、处理。例如，在使用淘宝等APP 检索特定产品后，上述检索的相关商品信息将自动推送。更有甚者其关联 app 也会进行相关产品的推送。网络用户基于消费的需要，输入商品的关键字，电商平台有权基于本次消费者同意进行数据库内商品检索。但是，平台是否有权对此数据进行存储，并持续处理则仍需探讨。（上述电商平台的数据共享行为，本节暂不做讨论。）

笔者认为，必要原则不仅局限于数据是否采集以及采集的范围，除此之外，对于所采集个人信息的处理时限、处理方式的认定也属于必要原则的认定范围。另外，收集（处理）的目的一旦实现，应当立即删除收集（处理）的个人信息，这也是正当原则的要求。对于在个案中，个人信息采集是否需要存储、存储的时长等问题，应当根据具体情形作出认定。根据国家市场监督管理总局、国家标准化管理委员会2020 年发布的GB/T 35273-2020《信息安全技术个人信息安全规范》，针对个人生物识别信息的收集，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意；对于生物识别信息的存储，明确：第一，个人生物识别信息要与个人身份信息分开存储；第二，原则上不应存储原始个人生物识别信息，可采取的措施包括但不限于：仅存储个人生别信息的摘要信息；在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。上述新规提出了个人信息保护新思路，即采集与存储相分离的模式，这能否为个人信息安全系上一道“锁”，让我们拭目以待。

六、结语

“中国人脸识别第一案”虽属普通民事合同纠纷，但却备受社会各界关注，显然在大数据、人工智能、5G时代来临的同时，对于个人信息安全保护人们产生了相应的不安、焦虑情绪。技术创新的本质在于改变生活方式，为消费者提供更有效率、更愉快的消费体验，但首要前提是不能突破法律的底线，消费者的合法利益可以得到全面、适当的保护。为此，首先，立法者应当明确个人信息保护立法态度，制定特别法以此完善立法体系，为信息采集者提供行为规范，也为个人信息权利人提供法律武器；第二，信息采集（处理）者也应设立相应的自我管控和审核规范，在法律的红线内，合法采集、处理用户信息；第三，个人信息权利人更应提高权利意识，根据实际需求及必要性原则提供个人信息，切勿贪图一时之便利盲目跟从，必要时应留存有关证据便于在权益受损时及时维权。也许“中国人脸识别第一案”能进一步唤醒社会大众对个人信息保护之重视，警示信息收集者、处理者审慎使用生物信息，但个人信息保护之路仍将任重道远。

注：

[1]我国《民法典》中规定具体人格权的条文均采用“某某权”之表述，而在《民法典》第1034 条中，却采用了“个人信息”的表述。这表明，对于个人信息的定位系为一种“受保护的人格法益”，尚未上升到“具体人格权”的高度。这意味着，在个案中认定加害行为是否成立对个人信息（权）的侵害，须严格其构成要件，谨慎裁判。详见《钟秀勇讲民法之精讲》第五编第二章第十节，第584页。

[2]《民法典》，第 1034 条。

[3]《民法典》，第 1035 条 第一款。
[4]《民法典》，第 1037 条 第一款。
[5]《民法典》，第 1037 条 第一款。
[6]《民法典》，第 1038 条 第一款。
[7]《民法典》，第 1038 条 第二款。
[8]《民法典》，第 1037 条 第二款。
[9]注：根据《民法典》第 1035 条第二款的规定，个人信息的“处理”包括：使用、加工、传输、提供、公开等。
[10]《民法典》，第 1035 条 第一款。
[11]一般信息，指不涉及自然人私生活秘密的信息。如姓名、出生日期、电话号码等信息。敏感信息，指涉及自然人私生活秘密的信息。如基因、病例、财产状况、性行为等信息。相比于一般信息，敏感信息应当受到更高程度的保护。
[12]《民法典》，第 1035 条 第二款。
[13]《民法典》，第 1035 条 第三款。
[14]《民法典》，第 1035 条 第一款。
[15]《民法典》，第 1038 条 第一款。
[16]《民法典》，第 1038 条 第二款。
[17]《民法典》，第 1037 条 第二款。
[18]《个人信息安全规范》，第五条第六款。
[19]《中华人民共和国传染病防治法》（2013年修订）总则第十二条：在中华人民共和国领域内的一切单位和个人，必须接受疾病预防控制机构、医疗机构有关传染病的调查、检验、采集样本、隔离治疗等预防、控制措施，如实提供有关情况。疾病预防控制机构、医疗机构不得泄露涉及个人隐私的有关信息、资料。卫生行政部门以及其他有关部门、疾病预防控制机构和医疗机构因违法实施行政管理或者预防、控制措施，侵犯单位和个人合法权益的，有关单位和个人可以依法申请行政复议或者提起诉讼。总则的这条规定，配合第三章“疫情报告、通报和公布”中第三十二、三十三条要求疾病预防控制机构“应当主动收集、分析、调查、核实传染病疫情信息”等，以及第四章“疫情控制”中第三十九至四十一条要求医疗机构和疾病预防控制机构采取的措施，可以解释成当：疾病预防控制机构、医疗机构为了疫情管控，具备改变个人信息使用目的的法定授权。
《突发公共卫生事件应急条例》（2003年制定））第三章“报告与信息发布”中的第二十一条：任何单位和个人对突发事件，不得隐瞒、缓报、谎报或者授意他人隐瞒、缓报、谎报。这条规定，配合第二章“预防与应急准备”第十、十一条中国务院和省、自治区、直辖市人民政府制定、实施“突发事件应急预案”，以及“突发事件应急预案”中应包含“（二）突发事件的监测与预警；（三）突发事件信息的收集、分析、报告、通报制度；（四）突发事件应急处理技术和监测机构及其任务”等内容的要求，再配合第四章“应急处理”第四十四条的规定：在突发事件中需要接受隔离治疗、医学观察措施的病人、疑似病人和传染病病人密切接触者在卫生行政主管部门或者有关机构采取医学措施时应当予以配合；拒绝配合的，由公安机关依法协助强制执行。可以解释成：人民政府在突发事件应急预案中，可以将除了卫生行政机构、疾病预防控制机构和医疗机构之外的部门、机构、组织、个人纳入，并赋予其信息收集。

来源：

作者：张继志 杨嘉碧

相关标签

信息技术、电信、传媒与娱乐