《个人信息保护法》实施

系列法律织密隐私安全“保护网”

■中国城市报记者 朱俪娜 张阿嫱

手机APP过度索权、被垃圾营销短信轰炸、出入小区必须人脸识别、被平台大数据杀熟……当下，个人信息泄露已经成为人们关注的重点话题。

11月1日，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）开始实施。这是一部保护公民个人信息的专门法律，与《民法典》《网络安全法》《数据安全法》等法律共同编织成一张消费者个人信息“保护网”。

《个人信息保护法》提出了哪些和我们日常生活紧密相关的新规定？记者做了以下梳理：

手机APP不得过度索权

在百度搜索框输入“APP权限”，记者发现“APP强制要求各种权限”“APP要电话权限安全吗”“手机软件APP咋需要这么多权限”等各种搜索问题。其中，“APP强制要求各种权限”的相关结果约1亿个，“APP要电话权限安全吗”的搜索结果量也超过4400万个。

今年9月，海南省网信办对该省用户量大、与民众生活密切相关的7款App收集使用个人信息情况进行了技术检测。其中，名为“猫扑运动”的APP下载量高达3907.5万，该APP在用户安装时申请了许多敏感权限，涉及身份证号、银行账号、行踪轨迹等信息，却并未提供实际功能。

诸如此类手机APP要求权限过多、过度搜集信息的现象普遍存在，是人们吐槽的技术霸凌“重灾区”。

对此，《个人信息保护法》中明确规定，经营者不得过度收集消费者个人信息。除了产品或者服务所必需的个人信息，如果消费者不同意提供非必要的个人信息，手机APP不能以此为理由，拒绝用户使用基本功能的服务。

另外，《个人信息保护法》还有一个新亮点，即“撤回同意”制度。该法第十五条规定，基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

也就是说，如果用户不想授权经营者处理其个人信息了，可以撤回同意。

不得非法推送商业信息

“您好，请问您需要办理某银行信用卡吗？”“本行新推出一款理财产品，您有兴趣吗？”“我们这里在出售某商业街旺铺，您想购买吗？”“最近营养师报考火爆，现在报名优惠多多，考虑一下吧。”

不止一位受访者向中国城市报记者表示，曾接到过这类商业推销电话。而且他们都很疑惑，对方是如何知道自己手机号码的？个人信息又是在何时何地泄露的呢？

2020年4月，公安部公布了10起侵犯公民个人信息违法犯罪典型案件。其中，江苏省徐州市挖掘出一个以电信运营商、银行内部员工为源头的买卖公民个人手机信息、征信信息等信息的犯罪网络。

在45名犯罪嫌疑人中，电信运营商、银行等部门有20余名内部人员涉案。该案查获各类公民个人信息43万余条，涉案资金达120余万元。

同年10月，江苏省公安厅发布一起非法获取车辆维保数据案件。该案源于一款为汽车服务的APP应用软件，受害人下载该软件后，无需任何授权，只需输入车架号并支付几十元的费用，就可以查询到自己车辆的各种维保信息，包括维修记录、碰撞历史、保养记录等等。

经过警方调查发现，多家汽车4S店工作人员系“内鬼”，为涉案APP所属公司提供后台数据查询服务。该公司负责人以每月500元至6000元不等的价格“收买”4S店工作人员多达上百人，涉及国内大部分汽车品牌，涉案金额超1000万元。

此外，还有垃圾营销短信轰炸、简历信息被贩卖……这些问题令人们不堪其扰。

不过，《个人信息保护法》规定，经营者要切实落实“告知-同意”规则。这意味着，今后要想收集消费者的个人信息，经营者必须保证消费者知情，同时需要征得消费者本人的同意。

除了不能非法收集、使用、加工、传输消费者个人信息，该法律还明确禁止非法买卖、提供或者公开消费者个人信息。这有力地打击了经营者利用一揽子授权、强制同意等方式违规处理消费者个人信息的行为。

不能强制业主或消费者进行人脸识别

目前，人脸识别已经越来越多地融入到人们的生活当中，但支付密码、账号密码等关系着每个人的安全问题。

今年“3·15”晚会曝光了人脸数据被违规收集的社会现象。期间提到，科勒卫浴、宝马等多家知名门店所安装的监控摄像头具有人脸识别功能，一旦顾客进入店里，人脸信息就会在不知情的情况下，被摄像头偷偷抓取。

科勒卫浴门店安装的人脸识别系统由苏州万店掌公司提供，其负责人表示，顾客不戴口罩时，人脸识别的准确率高达95%，即使戴口罩，准确率也在80%-85%之间。

另一位负责人表示，目前已经收集了上亿个人脸识别数据。该系统不仅能抓取顾客的人脸信息，还能分析出顾客的性别、年龄，甚至此时此刻的心情。

人脸信息属于个人独有的生物识别信息，如此重要的个人隐私正在不知不觉间被一些第三方公司所掌握。由于用户没有办法改变自己的人脸信息，一旦泄露，用户的财产、隐私等安全将受到严重威胁。

今年10月，公安部发布消息，安徽警方破获了全省首例利用人脸识别犯罪案。该团伙利用AI人工智能技术，伪造他人人脸动态视频，从而绕过手机卡注册过程中的人工审核环节。

比如每成功注册一张手机卡，依据绕过难度收费10元至20元不等，进而达到非法牟利的目的。这些开通的手机卡大量流入犯罪团伙手中，大多会被用于电信网络诈骗、网络赌博、洗钱等多类违法犯罪活动中。

在《个人信息保护法》中，明确规定了经营者不能为了商业目的非法收集消费者的人脸识别信息。同时，小区、经营场所不能强制业主或者消费者进行人脸识别。

该法律还提到，因为很难采取严格的措施对人脸识别信息进行保护，小区物业、经营场所没有必要把人脸识别作为出入的唯一验证方式。

这表明，今后业主和消费者可以自主选择通过何种方式验证身份信息。小区物业和经营场所可以采取一些替代性方式，比如向手机发送短信验证码。

平台经营者不能利用消费者个人信息“杀熟”

商家针对不同用户使用不同的价格，这样的事情几乎每天都在发生。

“我之前经常使用某款网约车软件，有一次与朋友一起游玩，相同的距离，我们的手机显示的价钱却并不相同，我的价格总是会稍贵一些。在另一款APP上，仍然存在这个问题。”经常打车出行的张先生告诉记者。

另一位用户也表示，“我使用某个旅行APP的频率比较高，于是开通了会员，但是之后的花费反而更高了。这太让人难以接受了！”

据浙江在线消息，今年7月，绍兴市柯桥区法院审理了胡女士诉上海携程商务有限公司侵权纠纷一案。胡女士曾多次通过该公司APP预定机票、酒店，在平台上消费了10余万元，成为该平台的钻石贵宾客户。

去年7月，胡女士像往常一样通过携程APP订购了某酒店房间，支付价款2889元。但在退房时，胡女士发现酒店的挂牌房价加上税金总价仅1377.63元，自己不仅没有享受到星级客户应当享受的优惠，反而多支付了一倍的房价。

最终，柯桥区法院判处上海携程商务有限公司赔偿原告订房差价，并按房费差价部分的三倍支付赔偿金。此案成为绍兴首例消费者在质疑遭遇“大数据杀熟”后成功维权的案例。

《个人信息保护法》明确提出，禁止“大数据杀熟”行为，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

也就是说，从11月1日开始，平台的经营者不能再根据消费者的个人特征提供选择，也不能利用平台所掌握的消费者经济状况、消费习惯以及对价格的敏感程度等信息，对消费者在交易价格等方面实行歧视性的差别待遇。《个人信息保护法》为消费者维权提供了更多法律依据。

同时，当平台经营者再向消费者推送信息或者进行商业营销时，消费者可以选择拒绝，并且平台要提供便捷的拒绝方式。平台如果依旧继续这些不公平、不公正的行为，将会承担相应的法律责任。

江苏镇江：面对面征询民生服务意见

日前，江苏省镇江市和平路街道金湖社区开展“我为群众办实事——民生服务征询意见面对面”活动，社区党员干部来到新建成启用的“睦邻家园”，与小区居民面对面，零距离倾听群众有关民生服务、文化活动、社会保障等方面的意见和建议。

人民图片