海问·观察 |《个人信息保护法》尘埃落定，五大最新亮点实务观察

2021年8月20日，全国人大常委会审议并通过《个人信息保护法》。《个人信息保护法》成为我国个人信息保护领域的基础性法律，与《数据安全法》《网络安全法》《民法典》共同构建了我国的数据治理立法框架。《个人信息保护法》的三次审议均引发了社会的高度关注，正式发布版更是细致入理、诸多新意，例如：对大型、小型个人信息处理者进行区别制度设计，增加人力资源管理所必需作为处理个人信息的合法性基础，明确高额罚款、停业整顿等处罚只能由省级以上履行个人信息保护职责的部门作出，增加对App个人信息保护的专门性规定等。

本文结合《个人信息保护法》正式发布版中对社会运行和企业治理影响较大、且在实务中需落地合规体系的五大亮点——大数据杀熟、儿童个人信息保护、数据出境、个人信息转移权、违法救济体系，逐一提出实务观察。

一.“大数据杀熟”：差别待遇不一定违法，需关注合法前提

“大数据杀熟”现象，以“千人千价”、“生客优惠”等情形为用户熟知，伴随数据在平台经济等领域的经济价值凸显而备受反垄断、反不正当竞争、电子商务等不同层面的立法监管关注。《个人信息保护法》从个人信息保护角度，整合其他层面的规制经验，意在引导大数据定价行为的合规开展，条件包括[1]：（1）保证自动化决策的透明度和结果的公平公正；（2）不得在相同交易条件下通过自动化决策实行不合理的差别待遇；（3）事先开展个人信息保护影响评估（“PIA”）。

由此可见，差别待遇不一定违法，需关注合法前提。“大数据杀熟”现象与数据使用行为直接相关，但其规制并不限于数据使用环节。差别待遇的合法前提覆盖使用管理、用户告知、结果公平、合规评估。

一. 使用管理前提：实现合理的差别待遇

目前法律法规（包含近日发布的《禁止网络不正当竞争行为规定（征求意见稿）》）已针对何谓“合理的差别待遇”有所讨论，包括正例[2]及反例[3]各三类，具体情形及对应实例如下表所示：

序号	法规规定情形	实例
正例		

[1] 《个人信息保护法》第二十四条、第五十五条。

[2] 包括《反垄断法》第十七条、《国务院反垄断委员会关于平台经济领域的反垄断指南》第十七条、《深圳经济特区数据条例》第六十九条、《价格违法行为行政处罚规定（修订征求意见稿）》第十三条。

[3] 《禁止网络不正当竞争行为规定（征求意见稿）》第二十一条。

	根据交易相对方的实际需求且符合正当的交易习惯和行业惯例而实行不同交易条件	会员分级优惠
	面向新用户在合理期限内开展优惠活动	新用户促销
	基于公平、合理、非歧视规则实施随机性交易	抽奖返券
反例		
	通过交易信息（交易历史及依赖程度、支付意愿及能力、习惯偏好、信用状况等），对交易条件相同的交易相对方不合理地提供不同的交易信息	对 1 个月内下单 5 次以上的消费者提高配送费
	通过浏览内容及次数，对交易条件相同的交易相对方不合理地提供不同的交易信息	仅因短期频繁查看页面而价格上涨
	通过交易时使用的终端设备的品牌及价值等，对交易条件相同的交易相对方不合理地提供不同的交易信息	对使用苹果手机、安卓手机的用户设置不同价格

总体而言，现有判断标准允许“基于成本或正当营销策略”，或“符合正当交易习惯、行业惯例”的情况下，对交易条件相同的交易相对人实施差别待遇。该等判断标准存有较大模糊性。举例而言，针对不活跃用户的派券促活行为是常见的营销策略且符合行业惯例，但能否满足合理性认定，则仍存在较大争议。较为明确的是，根据用户个人信息开展的关乎人格尊严、价值判断的价格歧视行为则明确被禁止，例如通过浏览次数判断用户是否具备较强购买欲望、通过交易所持设备或过往交易历史判断用户经济水平等，以此提供的差别待遇。

二. 用户告知与结果公平：保证自动化决策透明度、公平性

结合《个人信息保护法》的规定[4]，个人信息处理规则中应明确开展自动化决策的必要信息，例如处理目的、数据类型、对用户的影响、投诉方式等，同时应当保证决策的结果公平公正。

在涉及差别待遇的场景下，经营者落实透明度要求时存在实践困惑，即：自动化决策规则可能涉及商业秘密，应如何掌握展示尺度。除在隐私政策披露必要信息外，还需在具体场景触发时展示必要的判定规则说明及文字提示，说明差别待遇的考虑要素。以信用评价类产品为例，微信支付分、蚂蚁信用芝麻分均对赋分所关注的用户行为考察要素进行公示[5]。

判断决策结果是否公平公正的标准并不明确。无论如何利用大数据分析，基于交易成本合理定价的原则仍应坚守。向依赖程度高、支付能力强、价格不敏感的用户提供不合理高利润率定价，显然不符合公平、公正原则；反之，在真实的经营者让利场景下，根据大数据分析而给予用户不同程度优惠，则至少可确保不会损害消费者利益。

---

[4] 《个人信息保护法》第二十四条。

[5] 微信支付分：进入微信，点击“我“ “支付 “” 钱包 “” 支付分 “” 了解分数 “，可查阅微信支付分构成要素，包括身份特质（实名信息、身份信息的稳定性）、支付行为（使用微信支付的活跃度）、使用历史（使用微信支付分服务的按时支付情况）。
蚂蚁信用芝麻分：进入支付宝，搜索“蚂蚁信用 “，在界面内可查阅芝麻分构成要素，包括用户守约记录、行为积累、资产证明、身份证明、人脉关系。

三. 合规评估前提：对应**PIA**工作落地

根据《个人信息保护法》要求[6]，PIA内容应包括：（1）个人信息的处理目的、处理方式等是否合法、正当、必要；（2）对个人权益的影响及安全风险；（3）所采取的保护措施是否合法、有效并与风险程度相适应。针对自动化决策涉及的差别待遇场景，结合《个人信息安全影响评估指南》的要求[7]，评估要素应包括：

- 是否向用户说明通过自动化决策给予差别待遇的基本原理、运行机制；
- 是否定期对通过自动化决策进行差别待遇的合理性进行评价；
- 是否对自动化决策所使用的数据源、算法等提供持续优化；
- 是否向用户提供针对自动化决策结果（差别待遇）的投诉渠道；
- 是否支持对自动化决策结果（差别待遇）的人工复核。

经营者可选择由本方或者第三方完成上述PIA工作，并形成PIA报告。PIA报告需依规定至少留存三年[8]，供运营过程中内部评估更新参考、应对监管部门调查上报等需要[9]。

二. 儿童个人信息的增强保护：身份识别及产品隐私设计的实践范例

《个人信息保护法》将不满十四周岁未成年人（“儿童”）的个人信息作为敏感个人信息，除了获取单独同意外，还要求个人信息处理者对此制定专门的个人信息处理规则以加强保护[10]，彰显了国家保护儿童合法权益，为儿童健康成长创造良好网络环境的决心。该等理念与2019年国家互联网信息办公室出台的《儿童个人信息网络保护规定》（“《保护规定》”）一脉相承。从现行规范结合域外立法经验和实操来看，理解和适用《个人信息保护法》有关儿童个人信息保护的规定需要特别关注适用范围、识别儿童身份以及产品的隐私设计三个方面。

一. 儿童个人信息增强保护的适用范围

《个人信息保护法》延续了《保护规定》严格充分保护儿童个人信息的立场，具有广泛的适用范围，即只要在中国境内事实上从事了针对儿童的个人信息处理活动，无论数量多少，都要适用特殊规定，从而为儿童提供最大程度的保护。

《保护规定》在适用范围方面也为企业留出了一定的空间。通过计算机信息系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，不适用《保护

6 《个人信息保护法》第五十六条。

7 《GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南》附录A。

8 《个人信息保护法》第五十六条。

9 《GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南》第4.3条。

10 《个人信息保护法》第三十一条。

规定》有关增强儿童个人信息保护的规定[11]。正是由于存在这个“开口”，对于并非针对儿童用户开发且无法识别用户年龄的网络产品，业内常见的做法是在产品的隐私政策中设置未成年人条款，禁止未成年人在未得到监护人同意的情况下使用产品或服务。但是，仅凭设置未成年人条款无法充分保护儿童个人信息。

如何在保护儿童个人信息利益与控制社会成本之间取得平衡是国家和企业在制定和适用相关规范时都会面临的挑战。美国《儿童在线隐私保护法》（“**COPPA**”）可作参考。COPPA的适用范围包括两类网络运营者，即“针对”儿童提供服务的网络运营者和并非“针对”儿童提供服务，但确实知道其用户中包含儿童的的网络运营者。在判断是否“针对儿童”时，监管机构会采取相对宽泛的认定标准，即“部分”针对儿童的网络运营者也要适用COPPA。监管机构会考虑不同因素，如网站的主题、内容、代言人、广告、语言特征等，如果存在卡通形象等与儿童具有关联性的要素，就可能被认为是“针对儿童”提供网络服务。而对于并非“针对”儿童提供服务的网络运营者，也不意味着就可以高枕无忧。如果此类运营者确实知道存在儿童用户（例如，已经收到过儿童监护人投诉），则其也应当履行COPPA之下的义务。[12]

二. 如何识别儿童身份

识别儿童身份是履行加强儿童个人信息保护合规义务的重要前提。用户既包含成年人也包括儿童的网络运营者，需要使用年龄识别技术识别出儿童用户并针对儿童用户履行《保护规定》的合规义务，但《保护规定》并未明确网络运营者须尽到何种程度的识别义务。

目前业内实践广泛使用的是“告知+儿童自觉获得监护人同意”或者由儿童自觉填报真实年龄等模式，其合规性有待进一步明确。从域外经验来看，2020年1月21日英国信息专员办公室（ICO）颁布的《儿童适龄化设计准则》对此提出了建议[13]，而国内部分企业也已经开始类似实践。

1. 自我声明：仅通过用户陈述确定年龄，适用于低风险数据处理活动或与其他技术结合使用。例如，通过分析用户与企业服务交互的方式来估计用户的年龄，与其陈述年龄进行比对并基于对比结果采取必要措施。国内游戏产业为防止青少年沉迷，已有部分公司将实名校验确认为成年人，但游戏内行为特征却疑似未成年人的用户，以人脸识别方式加强核验用户身份[14]；又如，如果用户在首次自我声明年龄时被拒绝访问企业的服务，则产品将阻止其立即重新提交年龄以获得服务。

---

[11] 《儿童个人信息网络保护规定》第二十八条。

[12] Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions, 2021-08-18.

[13] ICO: “How can we establish age with an appropriate level of certainty?”, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/, 2021-08-18.

[14] “腾讯游戏开启人脸识别验证 防未成年人沉迷”，http://www.sohu.com/a/278352041_114774, “腾讯推出游戏未保“双减双打”新措施：非节假日在线时长降至1小时”，https://baijiahao.baidu.com/s?id=1707055066699349295&wfr=spider&for=pc， 2021-08-18.

2. 账户持有人确认：由已知是成年人的账户持有人设置或者确认有关儿童的信息。例如，国内幼儿App和部分航空公司会员即采取此模式，由成年人开设账号后设置儿童个人信息及子账号，并赋予成年人对子账号的管控权利。

3. 提供硬性标识符：即提供身份证件或其他“硬性标识符”（例如护照）来确认年龄。但是这个方法对隐私的刺探较强，ICO的《儿童适龄化设计准则》不建议强迫用户提供硬性标识符，除非企业数据处理活动中因存在固有风险而确实需要，例如航空旅客运输服务。

三. 产品的隐私设计要求

《保护规定》主要着眼于信息处理者的告知义务以及监护人的同意和权利行使。准确且高效地获取监护人的授权同意一直是个难题，企业可以通过完善产品设计，实质提升儿童个人信息保护水平，例如：[15]

1. 采取更简明、显著、清晰且适合儿童的语言向用户提供隐私政策、其他规则或政策，例如搭配视频、卡通或图示；

2. 将网络服务默认设置为“高水平隐私保护”。例如，儿童的个人信息默认无法为其他的用户访问；个人信息处理者仅能就其核心服务功能使用儿童信息。

3. 地理位置信息、用户画像等功能应默认关闭，不使用助推技术以引导或鼓励儿童提供不必要的个人信息或关闭隐私保护功能等。

三. 个人信息出境的国际视角：我国加入跨境数据流动的全球治理行列

《个人信息保护法》进一步完善个人信息出境的保护规则，明确要求个人信息处理者在向境外提供个人信息时，应当采取必要措施保障境外接收方处理个人信息的活动符合《个人信息保护法》的保护标准；《个人信息保护法》还进一步规定，若我国缔结或者参加的国际条约、协定对向境外提供个人信息的条件有规定的可以按照其规定执行[16]，体现了我国对于个人信息出境保护的高度重视和前瞻认知。个人信息出境不可避免，需从两个角度予以考虑：其一是保护个人权益、国家安全利益免受侵害；其二是推动我国参与跨境数据流动的全球治理。

长期以来，美欧主导了全球数据跨境流动规则制定的话语权。作为全球第二大数字经济体，我国在全球数据跨境流动领域具有广泛和庞大的商业、经济和政治利益，输出数据跨境流动领域的“中国标准”是应有之义。

美国主张个人数据跨境自由流动，利用数字产业全球领导优势主导数据流向，将亚太经济合作组织（APEC）的跨境隐私规则（CBPR）体系，构建成一项政府支

---

[15] ICO: “Age appropriate design: a code of practice for online services”, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/, 2021-08-18.

[16] 《个人信息保护法》第三十八条。

持、强调以市场为主导、以跨境数据流动为目标的数据隐私认证。欧盟则提出“相同保护水平”要求，即个人数据接收国需要达到流出国相同的数据保护水平，通过“充分性认定”确定数据跨境自由流动白名单国家。对于没有取得欧盟“白名单”国家资格的相关法域的个人信息跨境传输，也有相应的替代性手段，包括采取特定的保障措施如“具有约束力的集团企业规则（BCR）”、“欧盟颁布的标准合同条款（SCC）”等。

2020年11月15日，东盟十国、中国、日本、韩国、澳大利亚、新西兰等15个国家正式签署《区域全面经济伙伴关系协定》（RCEP），即标志着我国迈出全球数据跨境流动规则体系构建的重要一步。**RCEP**作为区域贸易安排，虽未就数据跨境制定专门体系，但在电子商务的框架下规定了服务贸易的数据跨境流动原则，明确各成员方不能将设施本地化作为在其领土内开展业务的条件，也不能阻止为实现业务需要而开展的数据跨境流动活动。同时鼓励成员方之间就金融服务中的跨境数据流动问题进行对话。

我国个人信息跨境领域的规则生成和实践经验积累正处于蓬勃发展的状态，多地也正在开展数据跨境传输安全管理的地方试点工作。本次《个人信息保护法》的出台无疑促进了我国个人信息跨境领域规则的完善和成熟，我们有理由相信我国可以探索出一条符合中国国情兼具国际视野的规则道路。

四．个人信息转移权：于激发数据创新意义深远，需明确规定条件、探索技术实现

《个人信息保护法》确立了个人对其个人信息处理活动的一系列权利，包括知情、决定、限制或拒绝处理、查阅、复制、更正、补充、删除等权利，并对传统的查阅复制权进行扩张，新增了有限的转移权——个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。[17]

个人信息转移权的设立意义深远。从个体权利的视角，其进一步增强了个人对其个人信息的控制力。从数字经济的视角，其试图打破平台巨头的数据垄断、促进数据流通与利用、激发市场竞争与创新。但与此同时，这也可能引发泄露个人信息、加剧数据集中、增加中小企业合规负担等方面的忧虑。[18]

《个人信息保护法》从原则上确立了个人信息转移权，并作出了“符合国家网信部门规定条件”的限定，有待将来出台细化规定。与之相似的权利是欧盟《通用数据保护条例》（“**GDPR**”）下的数据可携权（Right to Data Portability），GDPR及《关于数据可携权的指南》最早对数据可携权进行阐释，并在落地过程中提供了实践参考。鉴于个人信息转移权的复杂性，监管机构应充分考虑个人权益、平台权益、第三人权益的平衡，将其限制在合理范围；而企业应充分考虑用户知情与数据安全，切实保障权利的行使。

---

[17] 《个人信息保护法》第四十五条。

[18] 丁晓东：《论数据携带权的属性、影响与中国应用》，《法商研究》Vol.37 No.1（2020）。

1. 数据范围：欧盟的数据可携权仅适用于和个人相关的、通过自动化手段执行的（不含纸质文件）数据，且受限于下列条件：（1）该等数据的处理基础是个人同意或合同履行，不包括出于公共利益等其他情形；（2）该等数据由个人主动提供（如设立账户时填写的信息），或是从个人活动中观察到的原始数据（如网页浏览记录），不包括用户画像等经过加工的衍生数据；（3）数据可携权的行使不能影响他人的权益，例如，个人可以获得包含第三人信息的数据副本（如邮件通讯录、银行转账流水），但接收该等数据的第三方控制者不得将第三人的信息用于建立用户档案、画像或营销等目的。[19]

   个人信息转移权并不意味着个人与平台、平台与平台的对立冲突。用户数据是平台的经营成果与重要资源，平台对此享有正当利益；个人信息转移权请求是用户主动发起的、个体性的行为，属于用户的正当权利。而类似于“新浪诉脉脉案”[20]中大规模抓取、使用用户的账号信息、好友关系、微博内容的行为，则可以通过反不正当竞争法进行规制。

2. 技术实现：转移权的实践难点还在于个人信息如何在处理者之间进行转移，因为不同处理者的信息系统、数据结构、数据格式等往往不同。对此，欧盟的数据可携权要求以一种结构化、普遍使用、机器可读的形式来提供或传输个人数据，如XML、JSON、CSV等常用的开放数据格式；并且，GDPR鼓励数据控制者探索具有互操作性的数据格式，但其无须为响应数据可携权而特意采用在技术上兼容的处理系统。[21]

   目前，欧洲互操作性框架尚未落地。根据2019年的实证研究，企业提供数据副本的格式迥异，其中大部分格式无法满足GDPR的要求（详见下图）。[22]在美国，谷歌、脸书、微软、推特、苹果等科技巨头建立了数据可携权平台，以实现相互之间的数据直接转移[23]。而中小企业往往对互操作性、跨平台迁移束手无策，甚至在数据格式上面临考验。因此，个人信息转移权的落地首先面临技术实现问题，即如何形成一种通用的、且成本可控的数据格式，以实现跨平台的个人信息转移。

---

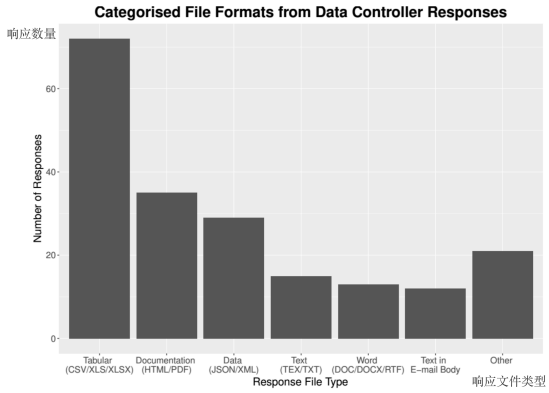
[19] 欧盟《通用数据保护条例》（General Data Protection Regulation）第20条。
欧盟第29条工作组《关于数据可携权的指南》（Guidelines on the Right to Data Portability）。

[20] 北京淘友天下技术有限公司等与北京微梦创科网络技术有限公司不正当竞争纠纷，北京知识产权法院（2016）京73民终588号二审民事判决书。

[21] 欧盟《通用数据保护条例》（General Data Protection Regulation）第20条、序言第68条。
欧盟第29条工作组《关于数据可携权的指南》（Guidelines on the Right to Data Portability）。

[22] Janis Wong, Tristan Henderson: The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR. International Data Privacy Law, 9(3):173–191, 2019.

[23] Data Transfer Project, https://datatransferproject.dev/.



文件格式 File Format	结构化？ Structured?	普遍使用？ Commonly Used?	机器可读？ Machine-Readable?
Email body	NO	YES	NO
CSV	YES	YES	YES
DOC/DOCX	NO	YES	NO
EML	YES	YES	YES
HTML	?	YES	?
ICS	YES	YES	YES
JPEG	NO	YES	NO
JSON	YES	YES	YES
KMZ	YES	NO	YES
MBOX	YES	YES	YES
MP4	NO	YES	NO
PDF	?	YES	?
PNG	NO	YES	NO
RTF	NO	YES	NO
TEX	YES	YES	YES
TXT	?	YES	?
VCS	YES	YES	YES
WAV	NO	YES	NO
XLS/XLSX	YES	YES	?
XML	YES	YES	YES

3. 用户知情：个人信息转移权是一种新型的人造权利，对用户而言比较陌生。因此，企业首先应当对用户进行充分的告知与教育，使其了解自己的权利。例如，在隐私政策中对个人信息转移权的内涵、数据范围、行使方式等进行介绍，并在产品设计中嵌入相应的功能按钮。[24]

4. 安全保障：转移权使个人信息离开原处理者的掌控，从而增加了安全风险，但企业仍应在其能力范围内保障个人信息安全。例如，在转移个人信息前，应采取强化的身份认证措施，以免个人信息的盗用；在个人信息传输时，应强化加密等措施，以免传输过程中的攻击与泄露；对于敏感个人信息，还应向个人及数据接收方提示关于存储、使用该等数据的建议。[25]

五．个人信息救济体系：三位一体的保护与救济体系，需关注行刑衔接标准

《个人信息保护法》为个人信息的保护提供了民事、行政、刑事三位一体、相互衔接的救济体系，强调人民群众、行政机关、司法机关之间的协调与配合，体现了我国保护个人信息的决心与智慧。

1. 民事救济：当数据处理活动侵害个人权益时，一方面，个人作为个人信息权利的主体、产品或服务合同的主体，有权直接提起民事诉讼，如侵权之诉、合同之诉，且侵权责任采用过错推定原则。正式发布版新增了个人信息处理者拒绝个人行使权利请求时，个人可依法起诉的规定。另一方面，个人信息处理活动往往牵涉甚广，当其侵害众多个人的权益时，检察院或其他经授权的组织，可以依法提起公益诉讼，从而大大降低个体维权的成本。[26]

2. 行政救济：一方面，履行个人信息保护职责的部门（“个保部门”）有权对涉嫌

[24] 欧盟第29条工作组《关于数据可携权的指南》（Guidelines on the Right to Data Portability）。

[25] 欧盟第29条工作组《关于数据可携权的指南》（Guidelines on the Right to Data Portability）。

[26] 《个人信息保护法》第五十条、第七十条。

违法的个人信息处理活动主动开展调查，并对违法行为进行行政处罚。另一方面，个保部门应当公布接受投诉、举报的联系方式，任何组织、个人有权对违法活动进行投诉、举报，个保部门应及时处理，并将处理结果告知投诉、举报人，通过群众路线强化行政监管。[27]

3. 刑事救济：违反《个人信息保护法》而构成犯罪的，依法追究刑事责任。[28]我国《刑法》规定了侵犯公民个人信息罪、非法获取计算机信息系统数据罪等涉及个人信息处理活动的罪名，司法实践中也产生了魔蝎科技[29]等典型案例，企业面临高额罚款、直接责任人面临有期徒刑。

4. 行刑衔接：《个人信息保护法》正式发布版增加规定，个保部门在履行职责中发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关。[30]在行刑过渡地带，一方面，情节严重的犯罪行为应当受到及时的刑事追诉与适当的刑事责任；另一方面，鉴于刑法的谦抑性原则，普通的违法行为不应动辄得刑。因此，刑事案件的移送标准尤为重要。

   在实践中，如2021年的科勒人脸信息案，科勒公司未经个人同意，通过门店摄像头获取并存储人脸信息220万余条，用于精准统计到店的客流。该案经央视315晚会曝光后，由上海市静安区市监局立案，并移送区公安分局，但被公安退回，最终作出罚款50万元的行政处罚。[31]

   又如2020年的浙荣贷款推销案，浙荣公司从房屋销售跑盘、企查查App等多个渠道获取18万余条个人信息，用于电话推销其贷款中介业务，最终被责令停止违法行为、并罚款12万元。[32]对此，杭州市江干区市监局认为，为合法经营活动而非法购买、使用个人信息，其社会危害小，适用行政处罚；如果后续用于诈骗或造成其他犯罪后果的，则由公安机关追究刑事责任。[33]

《个人信息保护法》在全社会的共同关注下尘埃落定，开启了我国个人信息保护的新纪元。顶层制度设计已逐渐明朗，但我国的个人信息保护才刚刚起步。接下来，有待于各部门细化配套规定、履行监管责任，有待于企业革新产品设计与内部管理、

---

27 《个人信息保护法》第六十一条、第六十五条。

28 《个人信息保护法》第七十一条。

29 杭州魔蝎数据科技有限公司、周江翔、袁冬侵犯公民个人信息罪，浙江省杭州市西湖区人民法院（2020）浙0106刑初437号一审刑事判决书。

30 《个人信息保护法》第六十四条。

31 关于科勒（中国）投资有限公司涉嫌未经消费者同意收集个人信息案，上海市静安区市场监督管理局，沪市监静处〔2021〕062021000787号行政处罚决定书。

32 杭州浙荣商务信息咨询有限公司侵害消费者依法得到保护的个人信息权利案，杭州市江干区市场监督管理局，杭江市监稽罚处字〔2019〕21号行政处罚决定书。

33 冯浩浩：《查办侵害个人信息案需要注意三个方面》，《中国市场监管报》，http://www.cmrnn.com.cn/flfg/content/2020-07/01/content_128309.html，最后访问日期：2021年8月20日。

落实数据合规义务，有待于广大群众发挥主体地位、广泛参与个人信息的保护与治理。路在脚下，大有可为。