

《个人信息保护法》实施两周年 观察报告



数据安全共同体计划
DATA SECURITY COMMUNITY



CCIA数据安全工作委员会
CCIA DATA SECURITY WORKING COMMITTEE



对外经济贸易大学
数字经济与法律创新研究中心



TSINGLAW
清律律师事务所

2023 年 11 月

前 言

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，并于 2021 年 11 月 1 日正式施行，开启我国个人信息保护法治建设新篇章。

《个人信息保护法》共八章 74 条，坚持发展与安全并重，对内总结我国数十年治理经验，对外吸收借鉴国际立法，以个人信息权益保护与个人信息合理利用为内在平衡，明确我国个人信息保护原则、个人信息处理活动规则、个人信息跨境提供规则、个人信息处理者义务、个人信息主体权益保障、个人信息保护机制等重点内容，为个人信息保护提供了更具系统性、针对性和可操作性的法律遵循，回应广大人民群众最关心最直接最现实的利益问题，有效推进依法治网和依法用网，推动营造良好数字生态，护航数字经济健康繁荣发展。

徒法不足以自行，法律的生命在于实施。《个人信息保护法》的颁行意味着有法可依的问题总体上解决了，个人信息保护相关立法工作告一段落，但仍然需要在实践中通过执法、司法、守法等各环节推进个人信息保护法治的实施，维护法律的权威。本报告围绕制度推进、行政执法、司法实践、公众感知等方面，多维度观察《个人信息保护法》实施两周年以来的主要进展。

目录

一、 制度进展观察	1
(一) 个人信息出境监管制度正式出台	1
(二) 重点制度配套实施细则稳步推进	6
(三) 个人信息保护技术标准扎实推进	10
二、 执法重点观察	14
(一) 网信部门	14
(二) 电信行业主管部门	17
(三) 公安部门	19
(四) 市场监督管理部门	20
(五) 其他主管部门	22
三、 司法实践观察	24
(一) 审判实践	24
(二) 检察实践	27
四、 公众感知观察	31
(一) 用户个人信息保护感知度问卷调查	31
(二) 个人信息保护数据统计分析	42

一、制度进展观察

《个人信息保护法》十年磨一剑，从基本法层面奠定了我国个人信息保护法治的顶层设计，与此同时，《个人信息保护法》也通过法律授权方式，授权国家网信部门等履行个人信息保护职责的部门制定相关个人信息保护规则、标准，细化《个人信息保护法》确立的各项制度。《个人信息保护法》实施两年来，国家网信部门等履行个人信息保护职责的部门，坚持促进发展和监管规范两手抓、两手都要硬，在深入贯彻《个人信息保护法》的基础上，基于法律授权，针对各界关切、百姓关切的突出问题，加快推进《个人信息保护法》相关配套制度的细化落实，保障《个人信息保护法》有效实施。

（一）个人信息出境监管制度正式出台

《个人信息保护法》第三章专章规定了个人信息跨境提供的规则，并在第 38 条构建安全评估、认证、标准合同和其他条件等多种个人信息出境路径，满足个人信息处理者多样化的个人信息出境需求。《个人信息保护法》实施以来，为进一步规范数据出境活动，保护个人信息权益，维护国家安全和公共利益，促进数据跨境安全、自由流动，国家互联网信息办公室先后推动《数据出境安全评估办法》《个人信息出境标准合同办法》两部部门规章，并联合国家市场监督管理总局发布《关于实施个人信息保护认证的公告》及《个

人信息保护认证实施规则》。

2023 年 9 月 28 日，国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》，对《数据出境安全评估办法》、《个人信息出境标准合同办法》等数据出境规定的施行作出细化调整，预示着国家网信部门将结合数据出境监管实践，持续探索保障国家数据安全与保护个人权益的平衡范式、规范和促进数据依法有序自由流动方面的中国方案。

1. 个人信息出境安全评估机制

2022 年 5 月 19 日，国家互联网信息办公室通过《数据出境安全评估办法》，自 2022 年 9 月 1 日起施行。《数据出境安全评估办法》共 20 条，坚持事前评估与持续监督相结合、风险自评估与安全评估相结合，明确了数据出境安全评估的具体适用情形、数据安全评估的主要评估内容、数据出境安全评估的具体流程等重点事项，防范数据出境安全风险，保障数据依法有序自由流动。

就个人信息出境安全评估的具体适用情形，《数据出境安全评估办法》凝聚各方共识，细化《个人信息保护法》第 40 条规定数量门槛，明确关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息、自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息需要

申报安全评估。

就个人信息出境安全评估的主要评估内容，《数据出境安全评估办法》聚焦个人信息出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险，统筹考虑多重因素，将评估重点落脚于六大评估因素，包括个人信息出境的合法性、正当性、必要性，境外接收方的数据保护水平是否达到我国同等水平，境外接收方所在国家或地区法律和网络安全环境对数据安全保障能力的影响，数据安全和个人信息权益能否得到充分保障；境内处理者对境外接收方的约束能力，境内处理者和境外接收方对我国法律遵守情况等，并规定国家网信部门认为需要评估的其他事项作为兜底情形，以便适应技术、商业、国内外环境的发展和变化。

就个人信息出境安全评估程序，《数据出境安全评估办法》坚持事前评估与持续监督相结合、风险自评估与安全评估相结合，明确了“处理者自评估——申报安全评估——省级网信部门接收申报——国家网信部门受理与组织评估”的科学流程，同时规定了异议复评与重新评估程序。

2. 个人信息保护认证机制

2022年11月4日，国家市场监督管理总局、国家互联网信息办公室联合发布《关于实施个人信息保护认证的公告》及附件《个人信息保护认证实施规则》，决定实施个人信息保护认证，鼓励个人信息处理者通过认证提升个人信息保护

能力，细化落实《个人信息保护法》第 38 条个人信息保护认证跨境路径和第 62 条个人信息保护认证服务内容。

与出境安全评估、标准合同侧重于具体出境需求的场景化分析不同，跨境个人信息保护认证侧重于以个人信息处理者、境外接收方双方主体为对象，对双方组织层面个人信息保护能力、合规水平的认证，通常适用于合规建设较为完善、境内外主体间长期稳定合作的情形。

对于开展跨境处理活动的个人信息处理者，认证依据包括 GB/T 35273《信息安全技术 个人信息安全规范》和 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》，认证模式为“技术验证+现场审核+获证后监督”。认证实施由个人信息处理者作为认证委托人发起认证委托，技术验证机构按照认证方案实施技术验证并出具技术验证报告，然后由认证机构进行现场审核并出具现场审核报告，最后经综合评价后由认证机构作出认证决定。

对于符合认证要求的，由认证机构颁发认证证书，并在认证 3 年有效期内通过认证机构的获证后监督，保持认证证书的有效性，到期需延续使用的，认证委托人应当在有效期届满前 6 个月内提出认证委托，符合认证要求的由认证机构换发新证书。对于不符合认证要求的，则可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

3. 个人信息出境标准合同备案机制

2023 年 2 月 24 日，国家互联网信息办公室发布《个人信息出境标准合同办法》及附件《个人信息出境标准合同》。

《个人信息出境标准合同办法》共 13 条，细化落实《个人信息保护法》第 38 条个人信息标准合同路径，对通过订立标准合同的方式开展个人信息出境的活动作出具体制度安排。与出境安全评估、个人信息保护认证路径不同，标准合同方式具有便捷化、成本低的特点，更加适用于低风险、小规模个人信息出境场景，便利中小个人信息处理者跨境业务合作需求。

就标准合同路径适用范围，《个人信息出境标准合同办法》对标《数据出境安全评估办法》，以排除法限定标准合同适用于未达到安全评估基线的个人信息出境场景，也即非关键信息基础设施运营者且达到规定数量的低风险、小规模个人信息出境场景。对于满足标准合同路径适用范围的个人信息出境场景，个人信息处理者可以与境外接收方签订标准合同，承诺遵守标准合同各条款约定的权利义务，在标准合同生效后即可开展个人信息出境活动，以标准合同生效后 10 个工作日内向所在地省级网信部门履行备案手续替代出境安全评估、个人信息保护认证等事前审核，借助自主缔约便利个人信息出境需求。

就出境风险防范，《个人信息出境标准合同办法》借助

于个人信息保护影响评估制度，从微观层面实现对具体个人信息出境活动的风险防范与控制。在标准合同路径中，个人信息保护影响评估成为事先识别和防范个人信息出境风险的首要手段，个人信息保护影响评估报告同样作为备案材料提交，敦促个人信息处理者重视并切实开展个人信息保护影响评估，避免发生个人信息安全事件导致问责。

就出境后个人信息保护水平，《个人信息出境标准合同办法》借助于境内处理者与境外接收方义务传导，明确规定了境外接收方应当遵守的各项义务，实现出境后同等保护水平。就出境后个人信息主体权益保障，《个人信息出境标准合同办法》明确个人信息主体作为第三方受益人，其可基于受益第三人身份，依据《个人信息出境标准合同》向个人信息处理者或境外接收方任何一方或双方提出权利主张，并可向违约方请求违约损害赔偿，境内处理者与境外接收方依法承担连带责任，极大地便利了个人信息主体权利行使与救济。

（二）重点制度配套实施细则稳步推进

《个人信息保护法》实施以来，国家网信部门围绕《个人信息保护法》各项重点制度，加快推进配套制度细化落实。截至目前，《网络数据安全条例》《个人信息保护合规审计管理办法》《人脸识别技术应用安全管理规定（试行）》等配套实施细则正在制定并已面向社会公开征求意见，各项重点制度细化方案雏形初现。

1. 《网络数据安全条例（征求意见稿）》

2021 年 11 月 14 日，国家互联网信息办公室发布《网络数据安全条例（征求意见稿）》，向社会公开征求意见。

《网络数据安全条例（征求意见稿）》共九章 75 条，包括总则、一般规定、个人信息保护、重要数据安全、数据跨境安全管理、互联网平台运营者义务、监督管理、法律责任、附则。该条例是《数据安全法》《个人信息保护法》施行后数据治理领域首部面向社会公开征求意见的行政法规，相较于《数据安全管理办法（征求意见稿）》，不仅法律位阶更高，内容也更加丰富。整体上看，该条例立足于《网络安全法》《数据安全法》《个人信息保护法》三部上位法授权，从行政法规层面对规范要求、责任界定、惩罚措施等进行了明确、细化和补充，进一步增强了数据安全法律法规的完备性和可操作性。就个人信息保护而言，该条例第三章进行了集中规定：一方面衔接《个人信息保护法》的具体规定进行了细化规定，如细化了个人信息处理合法、正当、必要原则，个人有效同意判定要件，个人信息删除权、转移权行使要件等规定；另一方面合理吸纳近几年 App 个人信息保护治理中的有益经验，如个人信息处理规则清单式展现方式、个人信息主体权利诉求响应时效等要求，将其上升为法律规则。2023 年 6 月，国务院公布《国务院 2023 年度立法工作计划》，该条例也被纳入拟审议的行政法规草案，有望

加快出台进度。

2. 《个人信息保护合规审计管理办法（征求意见稿）》

2023 年 8 月 3 日，国家互联网信息办公室发布《个人信息保护合规审计管理办法（征求意见稿）》及附件《个人信息保护合规审计参考要点》，向社会公开征求意见。《个人信息保护合规审计管理办法（征求意见稿）》共 16 条，《个人信息保护合规审计参考要点》共 31 条，对《个人信息保护法》第 54 条、64 条中提出的定期审计、监管审计两种合规审计制度进行细化，更好指导与规范个人信息处理者开展个人信息保护合规审计，提升个人信息处理者内部合规体系建设，完善个人信息保护监管抓手。就定期审计，明确个人信息处理者定期审计的最低频次，以处理个人信息规模为界，处理超过 100 万人个人信息的个人信息处理者最低频次为每年至少开展一次，其余个人信息处理者最低频次为每二年至少开展一次。就监督审计，明确个人信息处理者应当选定专业机构进行，原则上应当在 90 个工作日内完成，并按照专业机构给出的整改建议进行整改，并将合规审计报告、专业机构复核后的整改情况报送履行个人信息职责的部门。就专业机构，明确实施个人信息保护合规审计专业机构推荐目录，实施动态调整，鼓励个人信息处理者优先选择推荐目录中的专业机构开展个人信息保护合规审计活动。为保障专业机构的独立性和客观性，明确专业机构连续为同一审计对象开展

个人信息保护合规审计不得超过三次，且不得转包委托第三方开展个人信息保护合规审计。此外，《个人信息保护合规审计参考要点》更进一步明确了开展个人信息合规审计的相关参考要点，极大便利个人信息处理者推进内部个人信息合规审计制度建设与实施。

3. 《人脸识别技术应用安全管理规定（试行）（征求意见稿）》

2023年8月8日，国家互联网信息办公室发布《人脸识别技术应用安全管理规定（试行）（征求意见稿）》，面向社会公开征求意见。《人脸识别技术应用安全管理规定（试行）（征求意见稿）》共25条，依据《个人信息保护法》第62条授权，延续人脸信息规范一般规定的基础上，从人脸识别技术应用安全管理基本原则、场景化要求、具体合规义务等三个维度，针对人脸识别技术使用者、人脸识别技术产品或服务提供者两类主体，细化人脸识别技术应用规范要求，并明确相应的监督检查、举报投诉等事项。就人脸识别技术应用安全管理基本原则，明确合法性、最小必要、自主选择等基本原则，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可使用人脸识别技术处理人脸信息，在实现相同目的或者达到同等业务需求时，如果存在其他非生物特征识别技术方案的，应当优先选择非生物特征识别技术方案，个人对是否接受人脸识别技术处理人脸

信息享有自主选择权，除非法律、行政法规另有规定，应当取得个人的单独同意或者书面同意。就人脸识别技术应用的典型场景，区分隐私场所、公共场所、经营场所、组织内部场所、物业管理场所等提出差异化规范要求。就人脸识别技术应用合规要求，针对人脸识别技术使用者细化个人信息保护影响评估内容，明确年度风险检测评估义务，新增公共场所及存储超过1万人人脸信息的人脸识别技术使用者备案义务。针对人脸识别产品或服务提供者，提出技术系统等保三级以上要求，并采取相应技术措施。

（三）个人信息保护技术标准扎实推进

“安全发展，标准先行”，标准化工作是个人信息保护法律法规落地的重要抓手。在《个人信息保护法》出台前，《信息安全技术 个人信息安全规范》（GB/T 35273-2020）等国家标准在指导企业开展个人信息保护工作方面发挥了重要作用。《个人信息保护法》出台后，作为负责网络安全国家标准的专业技术组织，全国信息安全标准化技术委员会（TC260）也持续推进多项个人信息保护国家标准研制工作，细化个人信息保护重点条款及要求，为《个人信息保护法》落地实施提供支撑。

针对个人信息保护一般要求，已发布《信息安全技术 个人信息安全工程指南》（GB/T 41817-2022）、《信息安全技术 公有云中个人信息保护实践指南》（GB/T

41574-2022）、《信息安全技术 个人信息处理中告知和同意的实施指南》（GB/T 42574-2023）、《信息安全技术 个人信息去标识化效果评估指南》（GB/T 42460-2023），并推进《信息安全技术 个人信息合规审计指南》等国家标准研制工作，细化个人信息告知同意、受托人个人信息保护、个人信息自动化决策、可携带权、个人信息合规审计等制度要求。

针对敏感个人信息保护，推进《信息安全技术 敏感个人信息处理安全要求》标准研制工作，细化敏感个人信息通用和特殊安全要求。同时，针对生物识别信息保护，发布一系列专门标准，包括《信息安全技术 生物特征识别信息保护基本要求》（GB/T 40660-2021）、《信息安全技术 人脸识别数据安全要求》（GB/T 41819-2022）、《信息安全技术 基因识别数据安全要求》（GB/T 41806-2022）、《信息安全技术 步态识别数据安全要求》（GB/T 41773-2022）、《信息安全技术 声纹识别数据安全要求》（GB/T 41807-2022），明确各类生物识别信息收集、存储、使用、提供、公开、删除等处理活动安全要求。

针对个人信息跨境提供规则，聚焦个人信息认证制度，先后发布《网络安全标准实践指南 个人信息跨境处理活动安全认证规范 V1.0》、《网络安全标准实践指南 个人信息跨境处理活动安全认证规范 V2.0》，并推动国家标准《信息

安全技术 个人信息跨境传输认证要求》研制工作，明确跨境处理个人信息应遵循的基本原则、个人信息处理者和境外接收方在个人信息跨境处理活动的个人信息保护、个人信息主体权益保障等方面内容。

针对移动应用程序个人信息保护，发布《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》

（GB/T41391-2022）、《信息安全技术 移动互联网应用程序（App）个人信息安全测评规范》（GB/T 42582-2023 ）

《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》（GB/T 42884-2023 ），编制《信息安全技术 移动互联网应用程序（App）SDK 安全指南》《信息安全技术 应用商店的 App 个人信息处理规范性审核与管理指南》《信息安全技术 移动智能终端 App 个人信息处理活动管理指南》

《信息安全技术 智能手机预装应用程序基本安全要求》，细化移动应用程序全链条个人信息保护要求。

针对互联网平台个人信息保护，编制《信息安全技术 互联网平台及产品服务隐私协议要求》，细化互联网平台及产品服务个人信息保护规则的编制程序、具体内容、发布形式，并就隐私协议可读性、透明性、争议解决等问题提出了要求；推进《信息安全技术 大型互联网企业内设个人信息保护监督机构要求》研制工作，细化《个人信息保护法》中有关大型互联网企业内设个人信息保护监督机构的设立、成员、职

责、工作机制等内容，指导提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者建立主要由外部成员组成的个人信息保护监督机构。

二、执法重点观察

《个人信息保护法》第六章专章规定了“履行个人信息保护职责的部门”，立足我国个人信息保护治理实践，在第60条明确我国个人信息保护监管顶层设计，构建网信部门统筹协调与各部门共同协力的监管机制。实践中，在《个人信息保护法》出台前，中央网信办、工业和信息化部、公安部、市场监管总局等四部门从落实《网络安全法》《消费者权益保护法》的要求，自2019年开始持续组织开展App违法违规收集使用个人信息专项治理，切实保障个人信息安全，维护广大网民合法权益。本部分以国家网信部门、电信行业主管部门、公安部门、市场监管部门的主要执法行动为主线，梳理《个人信息保护法》实施以来的主要行政执法实践。

（一）网信部门

《个人信息保护法》进一步明确国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。《个人信息保护法》实施两年来，网信部门加大个人信息保护等领域执法力度，依法打击侵害公民个人信息等违法行为，切实推进个人信息保护出境监管制度落地实施，并在网络安全审查工作中强化个人信息保护，切实维护国家网络安全、数据安全和公共利益，有力保障广大人民群众合法权益。

2022年7月7日，国家互联网信息办公室发布《数据出境安全评估办法》，自2022年9月1日起施行，并为施行

前已经开展的数据出境活动留有 6 个月整改期。为了指导和帮助数据处理者规范、有序申报数据出境安全评估，国家互联网信息办公室编制了《数据出境安全评估申报指南（第一版）》，对数据出境安全评估申报方式、申报流程、申报材料等具体要求作出了说明。同时，国家互联网信息办公室和各地网信办陆续开通数据出境安全评估申报受理咨询电话。2023 年 1 月 18 日，北京市互联网信息办公室公告首都医科大学附属北京友谊医院与荷兰阿姆斯特丹大学医学中心合作研究项目通过数据出境安全评估，成为全国首例数据合规出境的案例。目前，各地网信办已陆续公告辖区内通过数据出境安全评估案例，涉及汽车、金融、零售、医疗、电商平台、物流、安防、通信等众多领域，标志着个人信息出境安全评估工作有序推进。

2023 年 2 月 22 日，国家互联网信息办公室发布《个人信息出境标准合同办法》，自 2023 年 6 月 1 日起施行。为了指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同，2023 年 5 月 30 日，国家互联网信息办公室发布《个人信息出境标准合同备案指南（第一版）》，对个人信息出境标准合同备案方式、备案流程、备案材料等具体要求作出了说明。同时，各地网信办积极开展落地实施筹备工作，制定并发布本辖区推进个人信息出境标准合同备案工作的相关指引或通知。2023 年 6 月 25 日，北京市互联网信息办

公室联合北京国际大数据交易所、北京 CBD 跨国企业数据流通服务中心，指导首批企业先行落实标准合同备案有关工作要求积极推进个人信息出境标准合同备案制度落地，北京德亿信数据有限公司与香港诺华诚信有限公司签订的个人信息出境标准合同已通过北京市网信办组织的备案审核，实现北京市与香港特别行政区间征信数据的合规出境，成为全国首家通过订立标准合同实现个人信息合规出境的企业，标志着个人信息出境标准合同备案工作正式开展。

2022 年 1 月 4 日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局等十三部门联合修订发布《网络安全审查办法》，拓展网络安全审查范围，新增“掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”要求，并且将“大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险”列为网络安全审查重点评估的国家安全风险因素，进一步保障网络安全和数据安全，维护国家安全。在后续开展的网络安全审查相关行政处罚决定中，国家互联网信息办公室根据网络安全审查结论及发现的问题和线索，并依据《个人信息保护法》对相关网络平台运营者违法处理个人信息行为作出处罚，

维护国家网络安全、数据安全和社会公共利益，保障广大人民群众合法权益。

（二）电信行业主管部门

《个人信息保护法》出台前，工业和信息化部紧扣行业管理职责定位，聚焦群众反映强烈和社会高度关注的侵犯用户权益行为，开展 **APP** 侵害用户权益专项整治工作，针对用户反映突出问题，强化治理。《个人信息保护法》实施以来，工业和信息化部纵深推进 **APP** 侵害用户权益治理工作，巩固和深化前期工作成果，部署开展信息通信服务感知提升行动，从正面推动行业重点企业以更高标准提升服务能力，大力推动提升移动互联网应用服务能力，保护用户合法权益，营造健康服务生态，推进《个人信息保护法》等上位法要求在信息通信行业领域落实落细。

2021 年 11 月 1 日，《个人信息保护法》正式施行当日，工业和信息化部发布《关于开展信息通信服务感知提升行动的通知》，聚焦影响用户感知的信息通信服务关键环节，开展信息通信服务感知提升行动。在个人信息保护方面，行动依据《个人信息保护法》的相关规定，在 **APP** 专项治理行动的基础上，进一步要求企业优化隐私政策和权限调用展示方式，并建立个人信息保护“双清单”，保障用户知情权、选择权等个人信息权益。对于隐私政策和权限调用展示方式，要求企业以简洁、清晰、易懂的方式，向用户提供 **APP** 产品

隐私政策摘要，并在涉及敏感权限调用时，以适当方式告知用户调用目的，便于用户阅读、理解，更加明确地作出主动性选择。对于已收集个人信息和与第三方共享个人信息“双清单”，要求企业在 APP 二级菜单中展示，对标解决企业告知不清晰、用户不清楚的信息收集、共享情况等问题，极大便利了用户查询和了解相关信息。行动开展之初，首批 39 家主要互联网企业及主要产品已经设立“双清单”，并优化隐私政策和权限调用，用户获得感、幸福感和安全感进一步提升。

2023 年 2 月 6 日，工业和信息化部发布《关于进一步提升移动互联网应用服务能力的通知》，在《个人信息保护法》等法律法规现有制度基础上进一步完善可操作性实施细则，增强法律法规的适用性、针对性和可操作性。就加强个人信息保护，聚焦超范围收集使用个人信息、规则告知不充分、过度索取权限等群众反映突出的问题，从坚持合法正当必要原则、明示个人信息处理规则、合理申请使用权限等方面，进一步明确相关措施要求。同时，围绕移动互联网应用全流程提出优化改善措施，并围绕互联网行业上下游全链条各主体，提出强化管理要求，重点针对 APP 开发运营者、分发平台、SDK（软件开发工具包）、终端和接入企业等 5 类移动互联网服务关键主体提出具体规范要求，通过各链条联防联控，推动行业治理走深走实。2023 年 9 月 8 日，工业和信息

化部发布《关于开展移动互联网应用服务能力提升优秀案例征集工作的通知》，通过征集优秀案例方式，推动提升移动互联网应用全流程服务感知及全链条管理能力，营造争先创优、互促共进的良好环境。

（三）公安部门

公安机关作为治安行政管理部门和刑事侦查部门，高度重视保护公民个人信息安全，持续重拳打击整治侵犯公民个人信息违法犯罪活动，同时坚持打击与整治并重，强化安全监督检查和行政执法。

针对非法采集、提供、买卖公民个人信息等违法犯罪行为，2016年以来，公安部每年部署“净网”专项行动，持续重拳打击整治侵犯公民个人信息违法犯罪活动。《个人信息保护法》实施以来，公安机关进一步加大对侵害个人信息的违法犯罪活动的打击力度。2021年和2022年，公安机关侦办侵犯公民个人信息类案件数同比均快速上升，破获案件数量和抓获人数连续突破新高，领域覆盖政府、医疗、教育、房地产、物流、电商等多个行业。针对AI换脸等新型犯罪，公安机关联合国家重点实验室等单位，开展人脸识别与活体检测技术安全测评，覆盖境内用户量大、问题隐患突出的即时通讯、网络直播、网络社交、电商平台、金融支付等重点APP，及时发现人脸识别验证系统存在的风险隐患，通报运营主体升级安全保护措施和人脸识别算法。依托“净网”行

动，组织专项会战，严打泄露身份证照片等图像信息的犯罪源头，有效遏制犯罪势头。

与此同时，公安机关立足网络安全监管职责，坚持打击与整治并重，开展常态化网络安全监督检查和行政执法工作，组织对关键信息基础设施、重要信息系统网络安全监督检查，及时发现并督促整改网络安全问题隐患，指导监督互联网企业依法履行安全保护责任和义务，完善用户数据采集、存储、使用制度。同时，对网络违法犯罪案件实行“一案双查”，在对侵犯公民个人信息等网络违法犯罪案件开展侦查调查工作时，同步启动对涉案企业网络安全义务履行情况的监督检查，依法严厉查处拒不履行网络安全义务、为网络违法犯罪活动提供帮助的行为，从源头遏制侵犯公民个人信息案件发生。

（四）市场监督管理部门

作为市场监管综合执法部门，国家市场监管总局一方面立足保护消费者合法权益职责，针对侵害消费者个人信息违法行为组织开展执法工作，保护消费者合法权益，营造安全放心消费环境；另一方面，立足认证监督职责，与国家互联网信息办公室联合推进个人信息保护认证制度落地，发挥规范和引导作用，完善个人信息保护治理制度建设，服务数字经济发展。

市场监管部门高度重视消费者个人信息保护工作，严厉

打击侵害消费者个人信息违法行为，保护消费者合法权益。国家市场监督管理总局以“打击侵害消费者个人信息违法行为”为主题开展2019年“守护消费”专项执法行动，针对房产租赁、小贷金融、教育培训、保险经纪、美容健身、装饰装修、旅游住宿、快递、电话营销、网站或APP运营等侵害消费者个人信息违法行为多发高发的行业和领域，就未经消费者同意，收集、使用消费者个人信息违法行为，泄露、出售或者非法向他人提供所收集的消费者个人信息违法行为以及未经消费者同意或者请求，或者消费者明确表示拒绝的，向其发送商业性信息违法行为，开展执法稽查工作。行动期间，国家市场监督管理总局积极组织指导各地市场监管部门开展大案要案查办，加强督查督办，推动专项执法行动不断向纵深开展。《个人信息保护法》出台后，各地市场监督管理部门聚焦消费场景下个人信息滥用和过度索取乱象，持续开展消费领域个人信息权益保护专项执法行动，惩戒侵害消费者个人信息权益的违法行为，推动经营者主动履行个人信息保护义务。如2023年上海市市场监督管理局、上海市网信办启动“亮剑浦江·消费领域个人信息权益保护专项执法行动”，聚焦餐饮店、停车扫码、房产中介、商超购物等八大消费场景，开展专项执法行动。

《个人信息保护法》后，国家市场监督管理总局与国家互联网信息办公室联合推进个人信息保护认证制度落地，发

挥规范和引导作用，完善个人信息保护治理制度体系建设，服务数字经济发展。认证认可是国际通行的质量管理手段和技术性贸易措施，也是市场有效运行的质量基础设施。针对数据安全和个人信息保护，国家市场监督管理总局联合国家互联网信息办公室已陆续推进移动互联网应用程序（APP）安全认证、数据安全认证等认证制度。根据《个人信息保护认证实施规则》，我国个人信息保护认证以个人信息处理者开展的个人信息处理活动为认证对象，认证范围涵盖个人信息处理活动所涉组织范围、业务范围、系统范围，涉及个人信息处理活动的组织管理、制度措施、技术处理等方面。目前，中国网络安全审查技术与认证中心作为认证机构，已经上线了个人信息保护认证申办系统并发布认证申请书模板，着手实施个人信息保护认证工作，并受理个人信息处理者认证委托。

（五）其他主管部门

《个人信息保护法》出台后，金融、邮政、住建等国务院有关部门也立足主职主业，立足自身监管领域，依照《个人信息保护法》和有关法律、行政法规的规定，在职责范围内积极推进个人信息保护和监督管理工作。

2022 年原银保监会（现国家金融监督管理总局）在业内发布《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》，要求各银行保险机构深入查找本机构在个

人信息保护方面存在的问题，进行全面自查整改并强化整治问责，强化金融消费者权益保护。

针对邮政快递领域信息安全问题，国家邮政局在 2022 年、2023 年，连续两年与公安部、中央网信办联合开展邮政快递领域个人信息安全治理专项行动，推广快件隐私面单等去标识化技术运用，加强寄递服务用户个人信息安全管理，保护用户合法权益。

针对部分房地产经纪机构滥用客户个人信息等问题，2023 年住房和城乡建设部、国家市场监督管理总局发布《关于规范房地产经纪服务的意见》，要求房地产经纪机构加强个人信息保护，依法严厉查处侵犯个人信息合法权益等违法违规行为。

三、司法实践观察

《个人信息保护法》出台前，我国在《刑法》中已经规定了侵犯公民个人信息罪，2017年最高人民法院、最高人民检察院发布《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，各级人民法院、人民检察院持续依法惩治侵犯公民个人信息犯罪活动，刑事司法实践成效显著。《个人信息保护法》的出台，进一步填补和丰富个人信息保护请求权、个人信息保护公益诉讼等多元保护机制，本部分聚焦民事司法审判、个人信息保护公益诉讼等视角，梳理《个人信息保护法》实施两周年以来的相关司法实践。

（一）审判实践

在《个人信息保护法》出台前，为贯彻实施《民法典》，最高人民法院修订《民事案件案由规定》，将“个人信息保护纠纷”作为单独适用的民事案由，通过适用《民法典》中个人信息保护条款，为个人信息提供民事司法保护。《个人信息保护法》生效后，人民法院充分发挥司法审判职能作用，加强个人信息保护，适用《个人信息保护法》的相关裁判规则也日益清晰。

从《个人信息保护法》生效后相关民事司法裁判整体情况而言，案件数量总量上升但趋于稳定，并以京、沪、广地区较多。以“个人信息保护法”为关键词进行裁判文书检索，截至2023年10月30日，以“个人信息保护法”为关键词、

通过公开渠道进行裁判文书检索,《个人信息保护法》生效后审结案件的民事裁判文书共计 124 份,¹包括 112 份判决书和 12 份裁定书,其中 2021 年 11 件、2022 年 67 件、2023 年 46 件,案件总量有所上升但趋于稳定。从适用案由来看,涉及人格权纠纷、合同/合同纠纷、知识产权与竞争纠纷、侵权责任纠纷、劳动争议/人事争议等具体案由,适用“个人信息保护纠纷”案由共 32 件,就以个人信息为单独案由提起的诉讼案件数量来看,在 2021、2022 年有明显上升,同样在 2023 年有所回落。从案件审理法院级别来看,以基层人民法院居多(67.74%),其中北京互联网法院以 25 件案件数位居榜首。从案件审理地域来看,北京、上海、山东、广东为审理案件较多地区,北京审理案件占比 41.46%。从审理级别来看,一审案件居多,占比 69%,二审为 28.23%,再审为 2.42%;从裁判结果来看,一审全部或部分支持诉讼请求居多,占比为 40.98%,一审驳回全部诉讼请求占比 22.13%,仅 3.28%驳回起诉;二审维持原判为 22.13%,再审维持原判 2.46%。

就具体案件适用具体条文而言,涉及《个人信息保护法》第 2 条、第 4 条、第 6 条、第 10 条、第 13 条、第 47 条、第 69 条居多,各地法院在个案中对《个人信息保护法》的

¹ 鉴于裁判文书公开具有滞后性,以及基于《最高人民法院关于人民法院在互联网公布裁判文书的规定》的相关规定,存在案件审结但不公开裁判文书的问题,因此,目前在网公布可供查询的裁判文书数量与实际司法实践情况,客观上会存在一定差异。但经法院认可宜在互联网公布可供查询的裁判文书具有行为指引意义,能够用以观察和反映《个人信息保护法》生效后的整体实施情况,本统计数据仍然具有一定的参考价值。

理解与适用进行了有益探索,丰富和细化裁判规则。如就《个人信息保护法》第13条规定各项个人信息处理合法性基础的适用,杭州中院二审重申《个人信息保护法》第13条虽然规定了豁免信息主体知情同意的合法性事由,但在具体适用订立、履行合同所必需、履行法定职责或法定义务所必需作为个人信息处理合法性事由时,需要确保其个人信息处理行为符合对应规则的要求。²就《个人信息保护法》第24条规定利用个人信息进行自动化决策的合法边界,杭州互联网法院认定,个人信息处理者在进行自动化时,如事先通过隐私政策取得个人信息主体概括性同意,并提供事后拒绝方式,个人信息处理者通过隐私政策取得个人概括性同意+事后拒绝方式,可视为对个人知情同意权的保障,具有合法性基础。³就《个人信息保护法》第45条规定的查阅、复制权的行使,广州中院、北京互联网法院明确查阅、复制个人信息范围限于个人信息处理者收集的信息及处理情况,就查阅、复制个人信息的实现形式,两地法院均认可个人提出获取信息副本的请求,而未认可个人信息处理者通过APP交互页面的方式满足个人查阅信息的抗辩。⁴就《个人信息保护法》第49条规定的死者个人信息保护事项,北京互联网法院认定个人信息处理者仍负有对死者个人信息的保护义务,死者近亲属虽

² 杭州互联网法院(2021)浙0192民初2929号、杭州中院(2021)浙01民终12780号。

³ 杭州互联网法院(2021)浙0192民初5626号。

⁴ 广州市中级人民法院(2022)粤01民终3937号、北京互联网法院(2022)京0491民初2138号。

有权查阅、复制死者相关个人信息，但同时也应当符合合法、正当、必要原则，从而驳回死者近亲属要求直接登录死者生前网络账号的请求，平衡死者近亲属与死者、第三方可能的利益冲突。⁵就《个人信息保护法》第 50 条适用，杭州互联网法院明确个人信息权利请求权诉权行使的前置条件，认定个人信息主体的诉权以个人信息处理者拒绝个人行使权利的请求为前提，就个人信息主体未向个人信息处理者行使个人信息权利请求，径行向法院请求救济的情形，驳回信息主体起诉，避免少数个人信息主体滥用个人信息保护诉权而造成不必要的诉累。⁶

（二）检察实践

《个人信息保护法》生效后，各级检察机关充分履行检察职能，切实推进个人信息保护公益诉讼落地，加强个人信息公益保护，维护国家和社会公共利益。同时，各级检察机关在积极稳妥推进涉案企业合规改革工作中，推动探索数据企业事前合规，制定发布数据合规指引，引导数据企业强化个人信息保护。

《个人信息保护法》第 70 条明确将个人信息保护纳入检察公益诉讼法定领域，由检察机关作为第一顺位主体推进个人信息保护公益诉讼。《个人信息保护法》生效后，各级检察机关切实加大办案力度，持续跟进监督个人信息保护领

⁵ 北京互联网法院“郭某等诉上海某科技公司等个人信息保护纠纷案”

⁶ （2022）浙 0192 民初 4330 号

域公益损害突出问题。在《个人信息保护法》出台前，检察机关积极稳妥推进公益诉讼制度，探索办理个人信息保护等领域公益损害案件，并发布检察机关个人信息保护公益诉讼典型案例，回应民生关切。2021年8月21日，在《个人信息保护法》公布次日，最高人民检察院下发《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》，对准确理解适用个人信息保护法公益诉讼条款、切实推动个人信息保护公益诉讼检察工作提出了要求，将敏感个人信息、特殊人群个人信息、重点领域个人信息、大规模个人信息、特定对象个人信息作为个人信息保护办案重点。《个人信息保护法》生效后，检察机关充分发挥检察一体化优势，以检察一体化应对个人信息公益损害网络化，畅通检察机关内部线索审查移送机制，在涉及个人信息保护的刑事、民事、行政相关案件中同步发现公益诉讼案件线索，加强全流程查处、全链条打击。与此同时，检察机关也注重加强与行政机关、人民法院的协作与沟通。检察机关在线索移送、信息共享、专业咨询、办案辅助等方面，加强与行政机关的协作配合，健全行政执法与公益诉讼检察衔接机制，并加强与人民法院的沟通协调，就案件管辖、诉讼请求、判决执行等方面达成共识，深化个人信息保护公益诉讼的制度探索。根据近两年最高人民检察院工作报告显示，2021年全国检察机关办理个人信息保护领域公益诉讼2000余件，2022年全国检察

机关办理个人信息保护公益诉讼 9109 件，彰显了检察公益诉讼的制度优势和发展潜力。从最高人民检察院发布个人信息保护检察公益诉讼典型案例来看，涉及民事公益诉讼、行政公益诉讼以及刑事附带民事公益诉讼，并以行政公益诉讼居多。

合规改革是检察机关充分发挥职能作用，以更优检察履职营造法治化营商环境的重要举措。最高人民检察院自 2020 年起探索涉案企业合规改革试点，对依法可不捕、不诉的，责成涉案企业作出合规承诺、切实整改。2022 年，最高人民检察院在深入总结检察机关涉案企业合规改革试点工作情况，对在全国检察机关全面推开改革试点工作作出具体部署，积极稳妥推进涉案企业合规改革。从最高人民检察院发布涉案企业合规典型案例来看，其中不乏数据企业的案件，推进数据企业守法经营，从源头上保障个人信息主体权利。一方面，检察机关在探索涉案数据企业合规改革工作中，强调个人信息保护，充分论证确保合规考察的必要性，数据企业合规改革通常以未涉及侵犯公民个人信息违法犯罪行为为前提。在上海检察机关所办理全国首例数据合规典型案例中，涉案数据企业所获取的数据不涉及个人信息是检察机关决定启动合规不起诉制度程序的首要理由，表明对侵犯公民个人信息违法犯罪行为的严惩态度，不论是对具体涉案企业还是其他数据企业合规改革，都具有重要参考价值，切实推进

企业从源头上重视个人信息保护。另一方面，检察机关在探索涉案数据企业合规改革工作中，除了在个案中引导涉案企业加强个人信息保护外，还注重由点及面推动行业治理。在深圳市人民检察院、上海市杨浦区人民检察院、杭州市西湖区人民检察院等在推进数据企业合规工作中，均从个案治理向行业合规延伸，以《个人信息保护法》等法律法规为依据，积极制定并发布《企业数据合规指引》，引导企业建立依法依规收集使用个人信息的管理制度和企业文化，指导企业及其员工的经营管理行为符合个人信息保护等法律法规要求，提升企业数据安全保障意识和犯罪预防意识，强化诉源治理。

四、公众感知观察

“网络安全为人民，网络安全靠人民”，个人信息保护也是广大人民群众最关心的利益问题，《个人信息保护法》的出台承载着社会各方殷切希望，通过各项制度安排回应个人信息权益保护的迫切需求。与此同时，切实落实个人信息权益保护，不仅需要国家通过立法、执法、司法活动推进个人信息保护要求落地，同时也需要加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。本部分聚焦用户个人信息保护感知度问卷调研、个人信息保护数据统计分析，以期探求《个人信息保护法》实施两周年来社会公众感知情况。

（一）用户个人信息保护感知度问卷调查

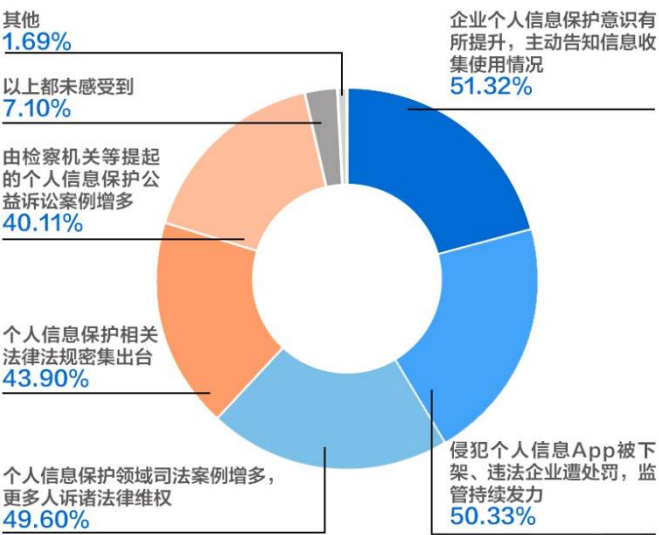
“用户个人信息保护感知度问卷调研”聚焦个人信息保护现状感知度、对个人信息泄露及维权看法、个人信息保护技能知悉程度、个人信息权利行使情况、个人信息保护意识评价、人群特征分析等六个维度，共设计 20 道调研问题，通过企鹅有调等进行问卷投放，共回收有效问卷 3139 份。本部分将结合问卷调查数据分析，剖析社会公众感知情况。

1. 《个人信息保护法》实施两周年整体感受

就受访者对于《个人信息保护法》实施两周年以来的变化，问卷从制度细化、行政执法、司法救济、公益诉讼、企业合规等多方面进行问题设计，调研发现公众感知占比最多

的是“企业个人信息保护意识有所提升，主动告知信息收集使用情况”（51.32%）。与此不相上下的是，“侵犯个人信息 App 被下架、违法企业遭处罚，监管持续发力”（50.33%）和“个人信息保护领域司法案例增多，更多人诉诸法律维权”（49.60%），一定程度上表明《个人信息保护法》实施以来，社会公众对企业合规、行政执法、司法救济都有清晰感知。

《个保法》实施两周年以来，
你是否感受到下列变化？

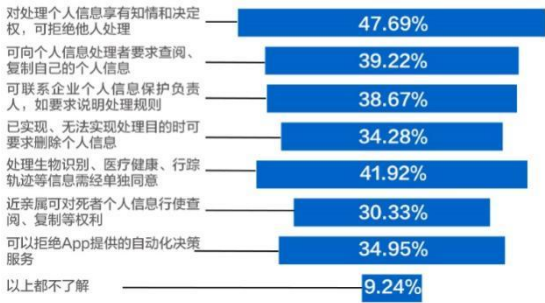


另外，有少数受访选择“以上都未感受到”（7.10%），并反映在工作和生活中遇到“仍有企业抱着侥幸心理，未尽信息收集告知义务”、“营销电话更多了，而投诉渠道少”、有的则表示“人脸识别技术被滥用场景增多”“被诈骗的数量和损失金额不断增加、政府泄露公民个人信息的情况增多”等等现象。

2. 个人信息权利感知及行权意愿

《个人信息保护法》第四章专章规定了个人在个人信息处理活动中的各项权利，包括查阅、复制、更正、删除等权利。调研结果显示，受访者对于《个人信息保护法》赋予的各项权利均有所了解，仅有不到 10%的人完全不知。

你是否了解《个保法》赋予公民个人的以下权利？



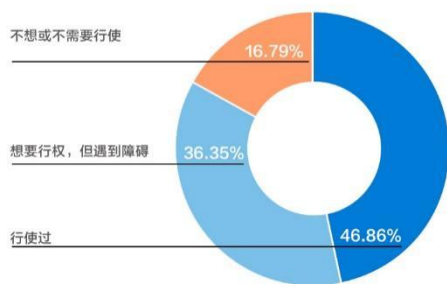
同时结合用户个人信息保护意识自评分析，可以看到，不同意识层次受访者认知程度最高的权利为“对处理个人信息享有知情和决定权，可拒绝他人处理”（知情同意权），其次为“处理生物识别、医疗健康、行踪轨迹等信息需经单独同意”。其中，“意识较弱”者对于“知情同意”权利的认知占比甚至达到 76.6%，而对于其他权利认知占比仅为 6% 至 11% 区间。可见，个人信息主体的知情同意权深入人心，但其他个人信息权利仍有必要进一步宣传和科普。

你是否了解《个保法》赋予公民个人的以下权利？

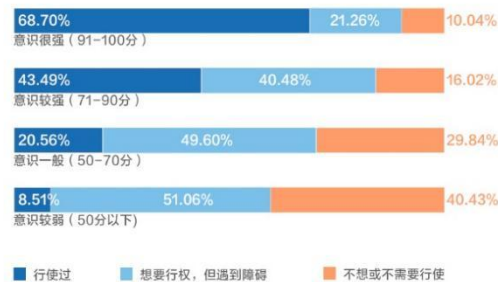
	意识很强 (91-100分)	意识较强 (71-90分)	意识一般 (50-70分)	意识较弱 (50分以下)
对处理个人信息享有知情和决定权，可拒绝他人处理	51.60%	48.37%	41.13%	76.60%
可向个人信息处理者要求查阅、复制自己的个人信息	44.87%	40.66%	26.81%	6.38%
可联系企业个人信息保护负责人，如要求说明处理规则	44.34%	40.66%	24.19%	8.51%
已实现、无法实现处理目的时可要求删除个人信息	40.81%	34.22%	24.60%	8.51%
处理生物识别、医疗健康、行踪轨迹等信息需经单独同意	46.69%	43.67%	30.04%	10.64%
近亲属可对死者个人信息行使查阅、复制等权利	36.22%	30.54%	20.77%	6.38%
可以拒绝App提供的自动化决策服务	36.54%	36.87%	28.02%	8.51%
以上都不了解	4.27%	6.63%	22.38%	61.70%

在了解个人信息权利之外，就个人信息权利行使情况，问卷特别加入“是否行使过这些个人权利”的问题。结果，仅有 46.86% 的受访者给出肯定答案，另有 16.79% 的人表示“不想或不需要行使”，“想要行使，但遇到障碍”的人数居中，占比 36.35%。结合用户个人信息保护意识自评情况交叉比对，可以发现，意识越强的用户，维权乃至诉讼的行动力越强；而意识较弱的受访者中，“不打算维权”占比则高达 25.53%，与其他三类用户 10% 的比例形成鲜明对比。

你是否行使过《个保法》赋予的个人权利？

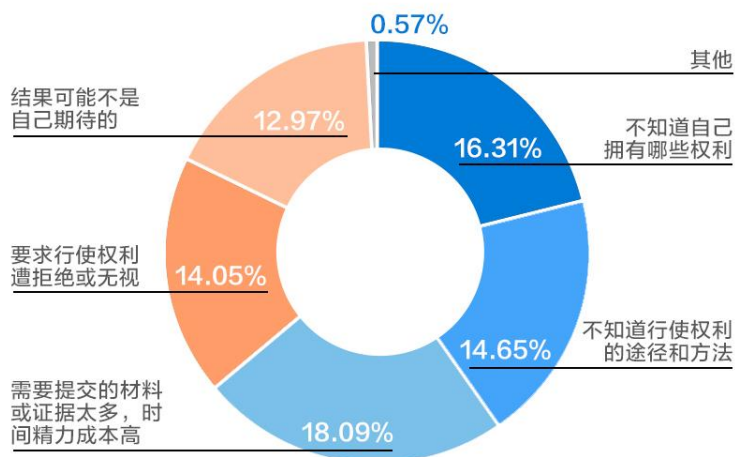


你是否行使过《个保法》赋予的个人权利？



就行使个人信息权利遇到的障碍，最多最多受访者反馈行使权利要提交的材料或证据太多，时间精力成本高，占比达到 18.09%。而“不知道行使权利的途径和方法”，“行使权利过程中被拒绝或无视的”，也各自占比超过 14%。还有 12.97%的受访者认为，结果不如预期，也是影响他们行使权利的一项障碍。

你在行使权利时遇到了哪些障碍？



3. 个人信息权益救济感知

就个人信息被侵犯后的具体情况，问卷列举了八类常见情形，调研显示，53.15%受访者曾经“多次收到无关的骚扰

或推销电话”，占比最高；居次的情形是“使用网络产品时被强制或频繁索取无关个人信息”，占比 42.5%。“进入某小区、写字楼等遇到强制刷脸”以 34.69%的占比排在第三；遭遇电信诈骗的受访者也不在少数，占比 33.39%，为第四大类情形。而从未遭遇过上述侵犯个人信息情形的受访者仅有 229 人，占比 7.3%。根据整体数据测算，平均每位受访者都曾遭遇过 2.36 类个人信息泄露事件。

在“其他”自行补充选项中，不少受访者透露了自己曾遭遇色情营销短信、酒店超范围收集个人信息、餐厅或厕所强制扫码等诸多与给定情形相似的经历，但也有受访者表示遭遇过被人监听监控，或是健康码被滥用赋红码等严重侵犯个人隐私、人身自由等公民基本权利的行为。

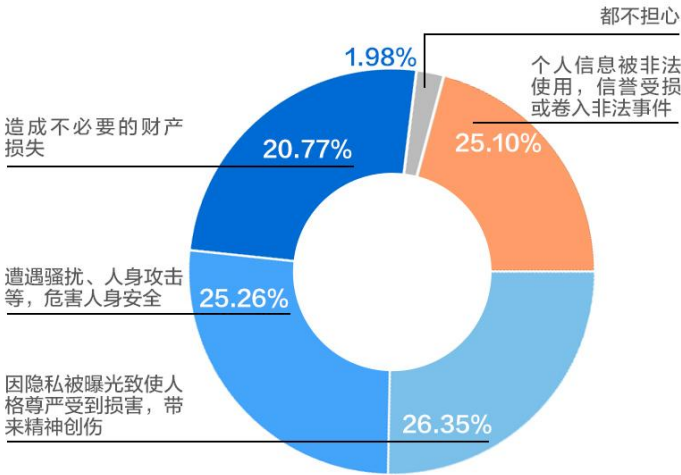
你是否遇到以下个人信息被侵犯的情况？



就个人信息泄露可能带来的隐患，调研发现受访者最担心个人信息泄露导致人格尊严受损，带来精神创伤；其次是担忧人身安全，再者是怕个人信息被非法使用、信誉受损或卷入非法事件，排在第四位的是担心造成不必要的财产损失。

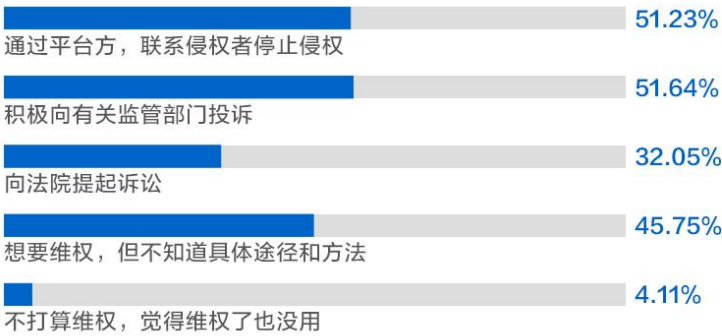
从占比情况看，这四项的占比均在 20%以上，可见受访者对这些信息泄露的隐患都存有担心。这在选择“其他”选项的 17 位受访者反馈中也得以体现，他们之中有人表示，“上述都担心”，“每个选项细思都触目惊心”，有的称，“虽然是概率事件，但就像一颗定时炸弹随时会爆炸”；还有的直言，这种担心已变成事实，深受困扰。

你最担心个人信息泄露带来的隐患是？



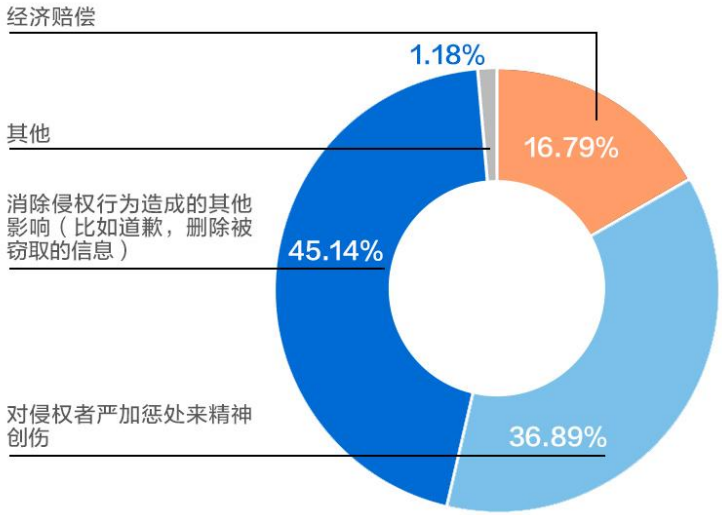
“个人信息被侵犯会怎么做”时，超过一半的人选择积极向有关监管部门投诉，或通过平台方联系侵权者停止侵权，选择向法院提起诉讼的占比为 32.05%。值得一提的是，受访者中“想要维权但不知具体途径和方法”的选择比例达到了 45.75%，还有少数人表态“不打算维权，觉得维权了也没用”。这说明，当前有关维权途径仍需进一步明晰，用户维权难的困境仍待解决。

如果打算维权，你更看重获得什么处理方式？



就具有维权意愿的主体而言，调研显示 45.14% 的受访者选择“消除侵权行为造成的其他影响（比如道歉，删除被窃取的信息）”，36.89% 的人希望对侵权者严加惩处，16.79% 的人则希望获得经济赔偿。

如果打算维权，你更看重获得什么处理方式？



4. 隐私政策阅读情况

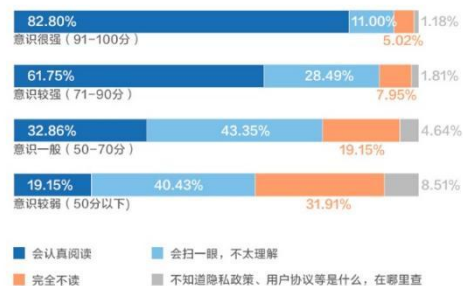
对个人信息收集和处理规则的知情、了解，往往是克服恐惧和忧虑最为重要的方式。自中央网信办、工信部、公安

部、市场监管总局联合开展 APP 违法违规收集使用个人信息专项治理以来，隐私政策成为 APP 标配。此次问卷调研通过个人信息收集和处理规则阅读情况、个人信息保护意识自评情况，交叉比对分析发现个人信息安全保护意识越高的用户，越了解隐私政策和用户协议，对于企业使用个人信息的接受程度也越高。反之，“意识较弱”者对于企业采集行为的反感程度最高，达到 48.94%。

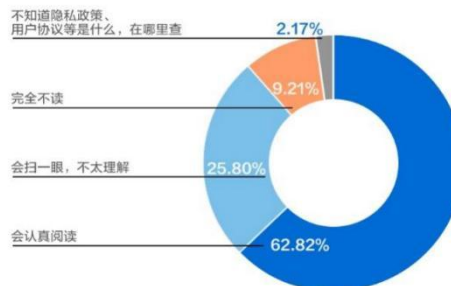
就个人信息收集和处理规则阅读情况，有 62.82% 的受访者表示，会认真阅读企业提供的个人信息收集和处理规则。25.8% 的受访者称“会扫一眼，不太理解”，而“完全不读”“不知何为隐私政策及在哪查看”的受访者各占 9.21% 和 2.17%。从占比情况看，公众对于隐私政策的了解度和接受度，相较于以往有所提升。

结合用户“个人信息保护意识”自评情况对个人信息收集和处理规则阅读情况进行交叉分析，可以发现，对于企业收集个人信息的行为，个人信息安全保护意识（以自评为准）越高，“认真阅读”隐私政策和用户协议的比例越高；意识越弱，“完全不读”比例也随着增高。但即便如此，在“意识较弱”群体中仍有 19.5% 会认真阅读隐私政策。综合来看，用户在学习了解相关信息后，能够对数据收集行为“心中有数”，因此心理接纳程度有所提升。用户是一支不可忽视的外部监督力量。

你会阅读企业提供的个人信息收集和处理规则吗？



你会阅读企业提供的个人信息收集和处理规则吗？



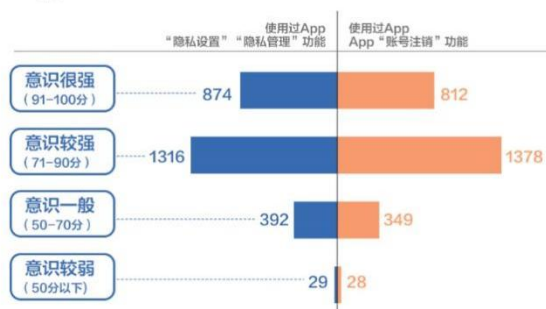
5. 用户个人信息保护技能掌握情况

为落地《个人信息保护法》中个人信息主体权利保护要求，APP 普遍推出隐私设置或隐私管理功能、注销账号功能和个性化推荐关闭功能。调研发现，受访者对于此类功能设置持正向态度，且使用意愿较高。

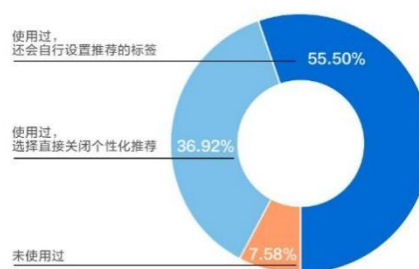
就隐私设置或隐私管理功能、注销账号功能，调研发现，有接近 9 成受访者表示用过“隐私管理”功能、81.78% 用户使用过注销功能。同时结合用户个人信息保护意识自评情况交叉分析，可以发现对于 App 普遍提供的隐私设置和账号注销功能，用户使用比例也与意识程度呈现递增关系。自认为个人信息保护意识较弱的受访者，几乎都不曾使用过 App 的隐私设置功能和注销账号功能。

就个性化推荐设置功能，使用过 App 个性化推荐设置的用户高达 92.54%。其中有接近四成用户选择直接关闭个性化推荐，在此基础上还会自行设置推荐标签的用户则高达 55.5%。

App功能使用情况



你是否使用过App个性化推荐的设置功能？



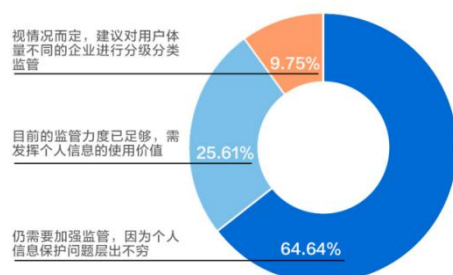
6. 个人信息保护展望

针对用户对个人信息保护当前监管力度和未来展望部分，问卷设计个人信息保护监管态度、个人信息强化举措两个问题。

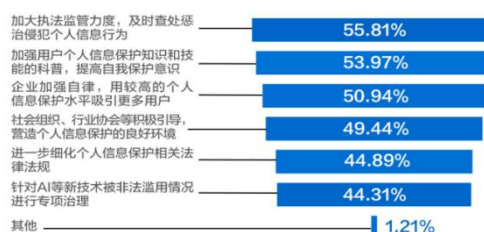
调研显示，64.64%受访者认为仍需要加强监管——因为个人信息保护问题层出不穷；25.61%的人则持相反意见，认为目前监管力度已足够，需发挥个人信息的使用价值；另有接近一成受访者态度中立，表示应当视情况而定，建议对用户体量不同的企业进行分级分类监管。

为提高个人信息保护力度，受访者也纷纷给出了建议。按选择数量占比情况，靠在前三位的分别是，建议加大执法监管力度，及时查处惩治侵犯个人信息行为，其次为加强公众个保知识和技能科普，提高自我保护意识，还有建议企业加强自律，用较高的个人信息保护水平吸引更多用户。

对于个人信息保护的监管，你的态度是？



为提高个人信息的保护力度，你认为需要怎么做？



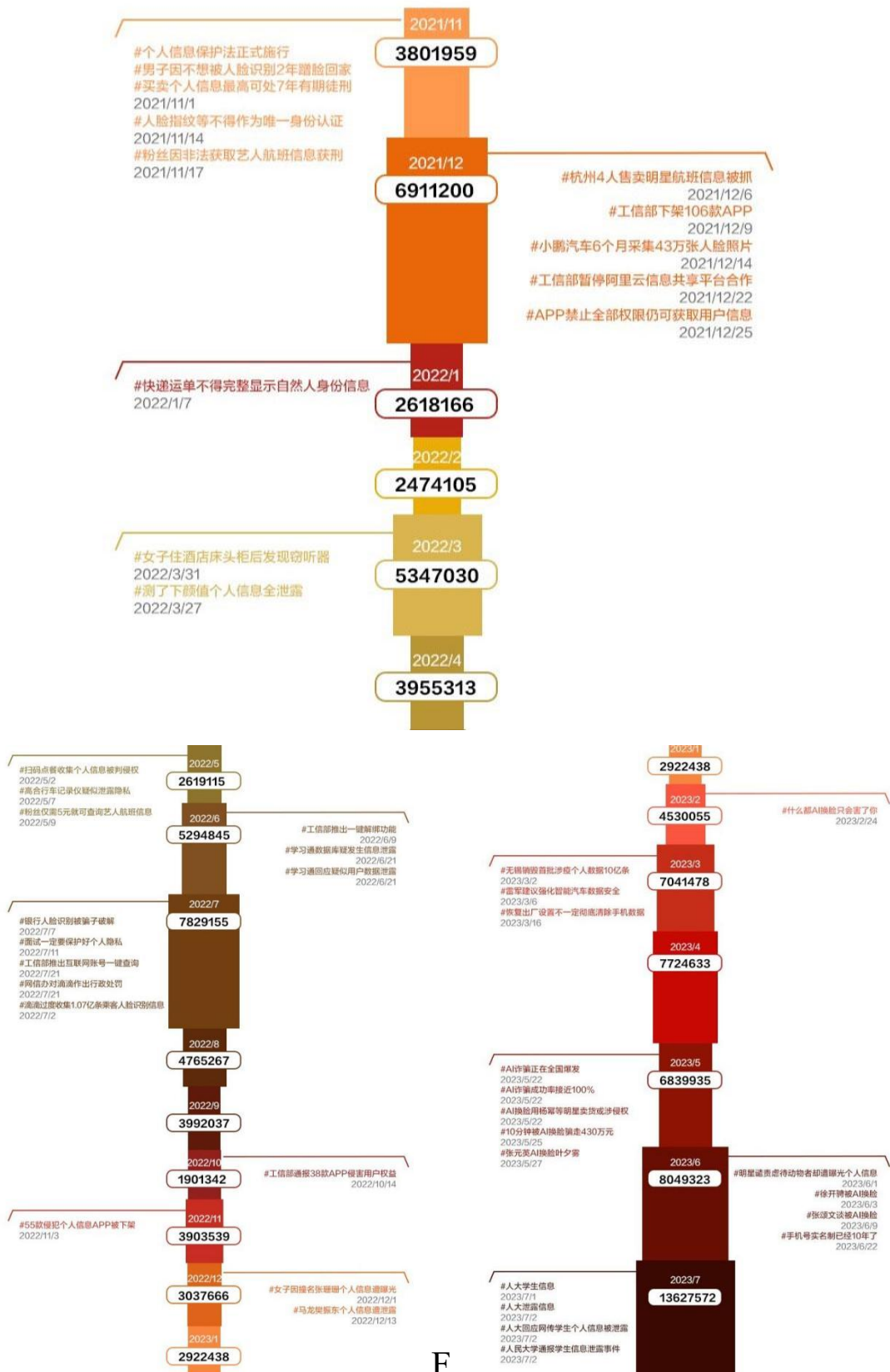
（二）个人信息保护数据统计分析

社交媒体平台是社情民意的一面镜子，为充分了解公众态度，本部分以隐私保护、隐私泄露、个人信息保护、个人信息权益、数据安全、网络安全、个人信息安全等作为关键词，对发布于2021年11月1日至2023年8月1日期间，热度最高的一千条新浪微博博文进行统计分析。

1. 个人信息保护“热搜”情况

对微博“实时热点榜”进行统计后发现，近两年来与个人信息保护相关的热搜共有113个，其中热度较高、值得关注的重点词条有45个。

哪些隐私保护事件“霸榜”微博热搜？



F

2021 年 11 月 1 日，“个人信息保护法正式施行”登上微博热搜榜，排名第 2 位。《个人信息保护法》的施行意味着个人信息保护“征程”进入新阶段，自然备受瞩目。不仅如此，当日共有 6 个相关词条登上热搜榜，包括快递信息被倒卖、强制“刷脸”进小区事件等，后者还登上热搜第一位。当月共有 17 个相关热搜，整体热度约 380 万。

2022 年整体热度值呈现“w”走势，波峰的出现主要取决于当月是否发生关注度较高的个人信息安全事件。在关注度较高的热搜话题中，监管动态、执法案例也是不可忽视的重要部分。此外，经历了个人信息被无条件攫取的“野蛮期”、多家中央部委开展专项治理的“强监管期”，如今广大网友的个人信息保护意识明显提升。越来越多人在面对个人信息被侵害时能及时察觉和拒绝，同时在社交平台上曝光事实，交流经验，共寻解决办法。比如，“女子住酒店床头柜后发现窃听器”、“面试一定要保护好个人隐私”、“测了下颜值个人信息全泄露”等从日常生活中发掘的话题频频登上热搜榜。

2023 年无疑是 AI 技术“井喷”发展的一年，其中“AI 换脸”技术带来的便利和风险备受关注。从年初开始，不少网友热衷于对明星的影视形象进行 AI 换脸，并收获了较高流量，进而“什么都 AI 换脸只会害了你”等讨论该技术法律及伦理风险的词条出现在热搜上。重要的是，“AI 换脸”

更大的风险体现在网络诈骗方面。5月至7月，5条AI诈骗相关词条登上热搜榜，涉及相关案例、建议、统计数据等。5月22日，“AI诈骗正在全国爆发”词条登上热搜榜首，阅读量高达约2.3亿。

疫情宣告结束后，涉疫数据如何处理一直是各方关注焦点。3月，江苏无锡举行涉疫个人数据销毁仪式，首批销毁数据10亿条，门铃码、疫查通、货运通行证等40多项“数字防疫”应用也于当天陆续下线。无锡市成为“身先士卒”对涉疫数据进行销毁的地级市，此举备受瞩目——相关消息登上热搜榜第2位。

值得注意的是，今年7月相关博文总热度达到统计期限内最高水平，近1400万——这与当月发生的人大毕业生盗取学生信息一事密切相关。有网友爆料称，中国人民大学某毕业生在校期间盗取学校内网数据，在网站上发布全校学生照片、姓名、学号等个人信息并进行颜值打分。不久，嫌疑人马某某被刑事拘留。

2. 个人信息保护热点话题情况

通过对相关博文进行统计，筛选出词频在十万以上的百余个热词，了解民众在讨论个人信息保护相关话题时最关注的内容，并大致归为个人信息保护客体、主体、安全事件关联词三类。

在个人信息保护客体关联词板块，“信息”“视频”两

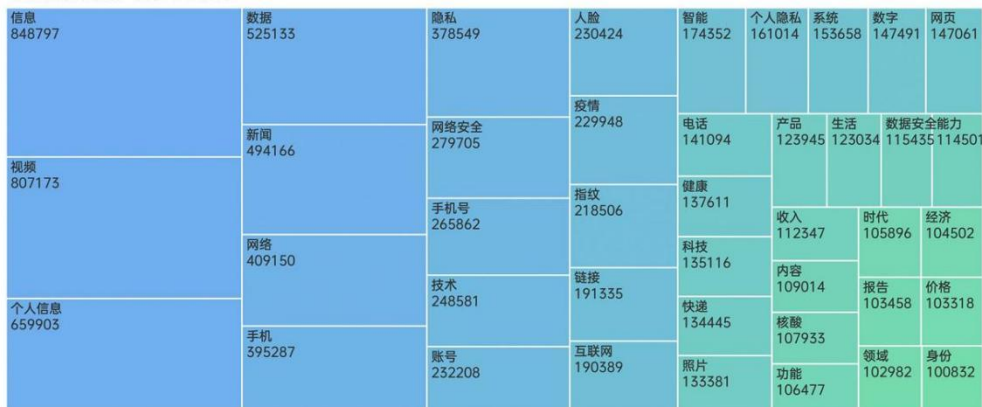
词以 80 万以上的词频数高居榜首，“个人信息”“数据”紧随其后。其他热词则囊括了大部分常见类型个人信息，比如手机号、人脸、指纹、账号、照片等，此外网络安全、互联网、智能、数据安全、科技、产品、链接等也备受关注。

在个人信息保护主体关联词板块，可以进一步细分为个人、企业平台以及监管部门。个人包括孩子、未成年人、消费者、未成年、演员、老人、公民、投资人等关联词，其中有关未成年人群体的关联词多次出现，词频位居前列，未成年人个保话题十分突出。微博、苹果、微信、企业、平台、机构等或个别或统称的各类企业机构关联词也“榜上有名”。另外，近年来，个人信息保护领域监管不断加强，作为主要监管部门的工信部、网信办均出现在热词榜单中，此外还包括官方、警方、部门等词语。

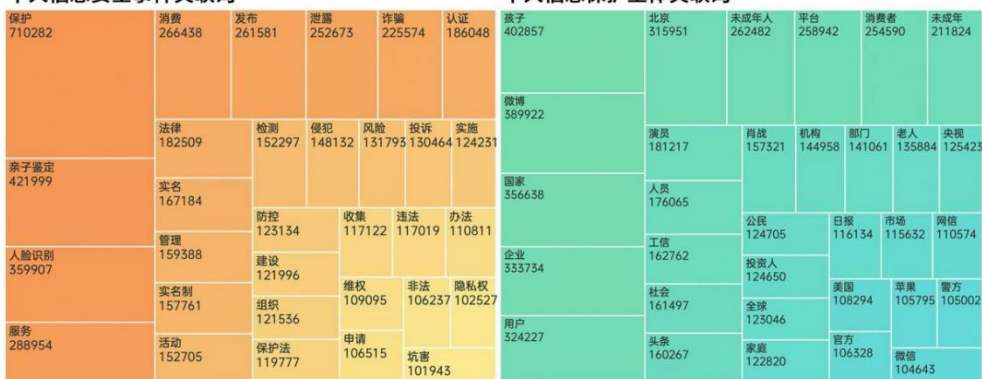
在个人信息安全事件关联词中，亲子鉴定、人脸识别两项技术排在前列，词频数分别约为 42 万和 36 万。泄露、诈骗、侵犯、投诉、违法、非法、坑害、维权等与个人信息安全事件紧密相关的词语都包含在内，同时，法律、保护法、隐私权、实名、管理、检测、认证等法律监管相关词语也被网友广泛提及。

隐私保护话题下，网友最关心什么？ 未成年人隐私保护备受关注，人脸识别频被提及

个人信息保护客体关联词



个人信息安全事件关联词



个人信息保护主体关联词

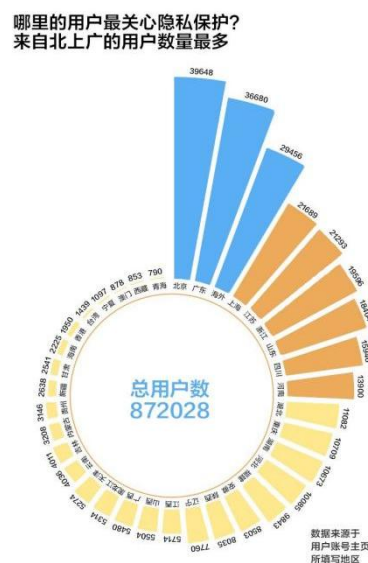
3. 用户特征情况

通过提取所有相关发博用户的公开账号信息,包括性别、地区、粉丝数等,试图了解微博上关注此类话题的用户特征。

统计显示,两年来约有 87 万网友在微博上讨论个人信息保护相关话题。从性别来看,女性对此类话题的关注度远远高于男性,有 70.93% 的相关博文由显示为女性的账号所发,男性仅占 29.07%。

从地域分布来看，根据已填写所在地区的账号情况，来自经济发达城市的用户对个人信息保护话题更为关注。北京、

广州用户最活跃，分别有近 4 万和 3.7 万用户参与讨论，其次是上海、江苏，参与用户在 2 万人以上。浙江、山东紧随其后，人数分别为近 2 万和 1.8 万，四川、河南、湖北、重庆等参与人数在 1 万以上。此外，来自海外的用户群体也很庞大，数量接近第一梯队。统计显示，有近 2.9 万海外用户参与了相关讨论，人数高于上海。



在用户类型方面，参与相关话题的普通用户占比 78.26%，名人则占 14.9%。同时，72.7%参与讨论的用户粉丝数在 500 人以下。这意味着，微博上相关话题的主要发声者是普通公众，在个人信息保护监管趋严，公众意识加强的大背景下，广大网友发声的意愿和能力较强。另外，标签为“政府”的相关用户约有 1.4 万，主要是政法系统的官方宣传账号，包括来自全国各地的各级公安局、检察院、法院等。这些账号通常是个人信息保护相关警情通报、案例发布、法律解析、

宣传引导的重要阵地，是面向广大网友的重要消息来源和宣传窗口。

在微博讨论隐私保护的都是谁？
普通用户占比近八成，检察院、法院积极科普

