# 海问观察：网络安全及数据合规动态（2019 年 12 月）

傅鹏、赵卿梦

本动态涵盖 2019 年 12 月网络安全和数据合规领域的规定、规则及重大新闻。第一部分为我们理解值得关注的该领域的最新监管规则（部分监管规则，可能包含我们对其值得关注的要点或问题的简评）；第二部分为我们理解值得关注的该领域的重要事件或重大新闻（部分事件或新闻，可能包含我们对其值得关注的要点或问题的简评）。

本动态仅作为本所对网络安全及数据合规相关的近期话题的一般性探讨，不构成本所正式法律咨询意见。

## 一、 监管规则

### (一)《App 违法违规收集使用个人信息行为认定方法》

- 公布时间[1]：2019 年 12 月 30 日
- 发布单位：国家互联网信息办公室、工业和信息化部、公安部以及国家市场监督管理总局
- 数据合规看点：

#### 1. 明确了特别突出的 App 违法违规收集使用个人信息的情形

近期，App 专项治理工作组（以下简称“**App 治理工作组**”）发布了在其审查评估过程中发现的 57 款 App 违法违规收集个人信息的问题（详见本文第二部分第四节的评述），其中部分问题在 App 治理工作组的本次审查评估过程中出现在多款 App 上，本次《App 违法违规收集使用个人信息行为认定方法》（以下简称“**认定方法**”）也体现了该等突出的违法违规收集使用个人信息的问题：

##### (1) 接入第三方代码或插件收集或提供个人信息的情形

认定方法明确提出，App 利用第三方代码、插件收集个人信息，但是未明确说明运用前述方式收集个人信息的方式、目的或范围的，可被认定为“未明示收集使用个人信息的目的、方式和范围”；既未经用户同意，

也未做匿名化处理，App 通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息的，可被认定为“未经同意向他人提供个人信息”。

**(2) 隐私条款设置的常见问题**

针对 App 隐私条款设置的常见问题，例如用户首次运行时隐私条款未以弹窗等明显方式提示用户阅读、条款难以访问（需多于 4 次点击才可访问）、难以阅读或难以理解以及以默认选择同意方式出现隐私政策等，认定方法明确提出前述行为均可被认定为“未公开收集使用规则”或“未经用户同意收集使用个人信息”。

**(3) 捆绑收集个人信息行为**

针对 App 存在的要求用户一次性同意开启多个收集个人信息权限，用户不同意则无法使用以及因用户不同意收集非必要个人信息或打开非必要权限而拒绝提供业务功能等捆绑收集个人信息的行为，认定方法明确提出前述行为均可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”。

**2. 隐私保护规则的新变化**

正式发布的认定方法与此前于 2019 年 5 月 5 日发布的《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》（以下简称“**认定方法的征求意见稿**”）相比较，存在如下重要变化：

**(1) 调整隐私条款的设置要求**

认定方法放宽了隐私条款的形式要求，即 App 中具有隐私政策或者在其他 App 相关协议或规则中设置收集个人信息规则即可；同时，提出了隐私条款可读性要求，即隐私政策或收集个人信息规则不得出现文字过小过密、颜色过淡、模糊不清或者未提供简体中文版，亦或使用大量专业术语等情形。

**(2) 明确 App 的承诺响应期限**

对于用户在申请更正、删除个人信息及注销用户账号功能时以及用户在进行投诉和举报时，App 需要在多久时间内对上述需求有所响应这一问

题，认定方法的征求意见稿没有强制的时间要求，而认定方法要求 App 的响应期限不应超过 15 个工作日。

**(3) 个人信息收集使用规则变更后的用户同意**

认定方法规定收集使用个人信息的目的、方式、范围发生变化时，应以适当方式通知用户，包括更新隐私政策等收集使用规则并提醒用户阅读等，相较于认定方法的征求意见稿，删去了“重新授权”的表述。

从该等规定的文义来看，个人信息收集使用规则变更后，App 应更新收集使用规则并提醒用户阅读，不强制要求再度取得用户的“同意”。但是，结合认定方法的其他条款来看，在特定场景下，App 变更个人信息收集使用规则仍然需要取得用户的同意。例如，认定方法的第三部分第 1 条以及第 3 条规定：“征得用户同意前就开始收集个人信息或打开可收集个人信息的权限”以及“实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围”均可被认定为“未经用户同意收集使用个人信息”，因此，如果 App 扩大了收集用户个人信息的范围和权限，那么就该等扩大部分仍然需要取得用户的同意和授权，此时 App 仅做到提醒用户阅读修改后的规则无法满足“征得用户同意”和“用户授权”的要求。

**(4) 定向推送信息规定有待明确**

对于目前市场上 App 中广泛存在的“定向推送”信息的功能，在此前的认定方法的征求意见稿中要求 App 应当提供终止定向推送的选项，本次正式发布的认定方法修改为：利用用户个人信息和算法定向推送信息，应当提供非定向推送信息的选项。

认定方法的征求意见稿中的要求较为明晰，即 App 应提供终止定向推送的选项，用户可以选择关闭 App 中的定向推送功能；但正式发布的认定方法中提及的“提供非定向推送信息的选项”可能有两种理解的角度：一方面，可以解读为用户可以选择开启 App 中非定向推送信息的选项，实现的效果是 App 不可再定向推送任何信息；另一方面，可以解读为 App 可以向用户提供定向推送的信息，但同时需要保证其 App 不能仅有定向推送的内容，应当也含有非定向推送的信息。

就第一种角度而言，在认定方法修改前后实现的效果是一致的，即用户可以通过选择关闭或开启特定选项后，实现 App 不能够再利用个人信息

和算法定向推送信息给用户；而第二种角度，会存在一定差异，正式发布的认定方法仅要求 App 能够做到其平台上提供非定向推送的信息。

通过与其他个人信息保护规范进行横向比较，发现对于定向推送的规则也有所不同：(i) 在《数据安全管理办法（征求意见稿）》中规定应当向用户提供终止定向推动功能的选项；(ii)在《信息安全技术 个人信息安全规范（征求意见稿）》（2019 年 10 月 22 日版）中按照服务类型的不同，进行了区分规定：如果提供电子商务服务，应保证在提供定向推送信息时，也提供不针对个人特征的选项；如果提供新闻信息服务，应提供关闭个性化展示模式的选项；如果在提供业务功能的过程中使用个性化展示，应提供用户的“自主控制机制”。

目前监管规则中对于“定向推送”的实施要求尚不明晰，有待监管机关在实际执法中进一步澄清。但是，对“定向推送”的相关要求被放置于“未经用户同意收集使用个人信息”大框架下，其本质应当是为了实现收集或使用用户个人信息的行为均应得到用户的同意，意味着需要赋予用户自主选择的权利。前文中第一种理解，即赋予用户能够终止 App 利用个人信息进行推送可能更贴合这一本质要求；第二种理解则赋予了 App 更大的自由度和发展空间。

**(5) 删去了未成年人个人信息权益保护的规定**

认定方法删去了认定方法的征求意见稿中对侵犯未成年人在网络空间合法权益的情形进行认定的章节，因此未成年人个人信息权益的特殊保护仍有待具体监管细则的出台。

**简评**：总体而言《App 违法违规收集使用个人信息行为认定方法》的规定具有较高的可操作性，能够给 App 运营者在个人信息收集和使用的实践中提供较为明确的指引，App 运营者应当用认定方法中的情形比照其现有业务流程进行逐一确认，避免出现认定方法中列举的违规行为。

## (二)《中国人民银行金融消费者权益保护实施办法（征求意见稿）》

- 发布时间： 2019 年 12 月 27 日
- 发布单位：中国人民银行

- 数据合规看点：

1. **法规涵盖的主体范围：**《中国人民银行金融消费者权益保护实施办法（征求意见稿）》适用于在境内设立的银行业金融机构、非银行支付机构，商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及征信机构、特许货币兑换经营机构可以参照适用。其中,相较于 2016 年实施的《中国人民银行金融消费者权益保护实施办法》，商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及特许货币兑换经营机构为本次征求意见稿新增的主体范围。

2. **金融信息出境的要求：**在境内收集的消费者金融信息的存储、处理和分析应当在中国境内进行。但是因业务需要，确需向境外提供消费者金融信息的，且满足以下条件可以向境外提供：(i) 为处理跨境业务所必需；(ii) 经金融消费者书面授权；(iii) 信息接收方为完成该业务所必需的关联机构（含总公司、母公司或者分公司、子公司等）；(iv) 通过签订协议、现场核查等有效措施，要求境外机构为所获得的消费者金融信息保密；(v) 符合法律法规和其他相关监管部门的规定。

   其中，就第(iii)条所列的条件，实务过程中可能出现向非关联机构传输金融信息的需求，例如跨境汇款业务等跨境金融服务，境内金融机构如果需要向境外非关联机构传输金融信息，如何处理该等情形下金融信息的跨境需求，有待实践的检验。

3. **金融信息安全事件应对的期限要求：**在确认信息发生泄漏、毁损、丢失时，金融机构应当在 72 小时以内采取补救措施并告知金融消费者。

4. **鼓励金融机构协助消费者金融信息的转移：**鼓励金融机构在技术可行的前提下，基于金融消费者的请求，将其金融信息转移至金融消费者指定的其他金融机构。

**简评：**消费者的金融信息作为特殊类别的个人信息，涉及个人的身份、财产以及征信的多重方面，因此，监管机关在规范金融机构对消费者金融信息的收集和使用上，除兼顾一般性个人信息的保护规则外，还提出了更加严格的要求。

### (三) 《网络信息内容生态治理规定》

- 发布时间： 2019 年 12 月 15 日（2020 年 3 月 1 日起施行）

- 发布单位： 国家互联网信息办公室

- 数据合规看点：

1. **网络信息内容的分类规定：**根据网络信息内容生产者制作、复制和发布信息内容的不同，将网络信息内容划分为三类，即鼓励类信息、禁止类信息和限制类信息。其中：(i) 鼓励类信息指包含宣扬中国特色社会主义、弘扬社会主义核心价值观及宣扬优秀道德文化和时代精神等内容的信息，鼓励制作、复制和发布该等信息；(ii) 禁止类信息指包含违反宪法原则、危害国家安全和利益、侵犯他人合法权益等内容的信息，不得制作、复制和发布该等信息；(iii) 限制类信息指包含内容与标题不符、炒作绯闻、丑闻或劣迹、煽动人群或地域歧视等内容的信息，防范和抵制该等信息。

2. **网络信息内容服务平台应当建立网络信息内容生态治理机制，健全用户管理和信息审查处置制度：**网络信息内容服务平台应当健全用户管理和平台信息管理等制度。同时，网络信息内容服务平台应当设立网络信息内容生态治理负责人，配备与业务范围和服务规模相适应的专业人员。

3. **网络信息内容服务平台对三类信息的传播管理：**(i) 不得传播禁止类信息；(ii) 不得在平台的“重点环节”呈现限制类信息。其中，“重点环节”指首页、弹窗、热门、热搜、精选、榜单、推荐、热搜词、默认搜索、联想词、预置内容等处于产品或服务醒目位置、易引起使用者关注的环节；(iii) 鼓励在“重点环节”呈现鼓励类信息。

4. **网络信息内容服务平台应加强对个性化算法推荐信息的管理：**网络信息内容服务平台采用个性化算法推荐技术推送信息的，不得推送禁止类信息或限制类信息，鼓励推送鼓励类信息；同时，应当建立健全人工干预和用户自主选择机制。

5. **热点问题的规范治理：**网络信息内容生产者、网络信息内容服务使用者和网络信息内容服务平台：(i) 不得通过发布、删除信息以及其他干预信息呈现的手段侵害他人合法权益或者谋取非法利益；(ii) 不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动；(iii) 不得通过人工方式或者技术手段实施流量造假、流量劫持以及虚假注册账号、非法交易账号、操纵用户账号等行为，破坏网络生态秩序。

6. **法规的部分规则和罚则仍有待进一步细化和明确：**就规则层面而言，例如法规要求平台建立用户账号信用管理制度，根据用户账号的信用情况提供相应服务，但是，对信用划分和管理的规则均有待明确；又如法规要求平台编制信息内容治理工作年度报告，但未明确该等报告的进一步处理；就罚则层面

而言，对于网络信息内容服务平台的处罚形式主要是约谈、警告、责令改正以及责令暂停信息更新，同时，罚则部分又设置了兜底性质的条款，即“按照有关法律、行政法规的规定予以处理”，使处罚的形式不局限于本法规。

**简评：**《网络信息内容生态治理规定》提出了对网络信息内容服务平台管理责任的具体化要求，并且对目前网络信息服务的热点问题予以了回应；但是，法规的部分规则和罚则仍有待进一步细化和明确。

**(四)《工业互联网企业网络安全分类分级指南（试行）（征求意见稿）》**

- 发布时间：2019 年 12 月 17 日
- 发布单位：工业和信息化部
- 数据合规看点：

1. **工业互联网企业分类：**依据企业属性，工业互联网企业划分为应用工业互联网的工业企业（“**联网工业企业**”）、工业互联网平台企业以及工业互联网基础设施运营企业。本指南旨在对联网工业企业网络安全分级进行规范；工业互联网平台企业以及工业互联网基础设施运营企业应当按照《通信网络安全防护管理办法》的分级方式进行规范。

2. **行业指导与地方监管相结合：**工业和信息化部对主管行业领域的工业互联网企业网络安全工作开展指导管理。地方主管部门对本行政区域工业互联网企业的网络安全工作开展指导监管。

3. **联网工业企业分级：**根据企业所属行业网络安全影响程度、企业规模、企业应用工业互联网的程度、企业发生网络安全事件的影响程度等要素将企业分为三个等级。

4. **联网工业企业评级流程：**联网工业企业通过工业互联网企业网络安全分类分级管理服务平台在线填报问卷，形成自评报告；地方主管部门可自行或组织第三方专业服务机构对企业提交的自评报告进行核查确认企业的最终等级并有权要求企业予以补正后再予以确认等级；当联网工业企业网络安全风险程度发生重大变化时，应主动重新定级。

5. **工业互联网企业的安全管理规定：**根据工业互联网企业等级的不同，指南中体现了不同的监管力度，详见下述表格：

| 企业等级及其安全管理要求 | |
|---|---|
| 二级工业互联网企业 | 三级工业互联网企业 |
| 逐步建立健全网络安全责任制 | 应当建立健全网络安全责任制，并且应设置专门网络安全机构，加强网络安全考核以及确保安全投入 |
| 积极建设企业级工业互联网安全监测平台，并与省级工业互联网安全监测平台对接 | 应当建立完善企业级工业互联网安全监测平台，并接入省级工业互联网安全监测平台。同时，省级以上工业互联网安全监测平台应定期向三级企业通报安全风险 |
| 每两年进行一次网络安全风险评估与审计 | 每年进行一次网络安全风险评估与审计。 |

**简评：**《工业互联网企业网络安全分类分级指南（试行）（征求意见稿）》中制定了适用于应用工业互联网的工业企业的等级分类评定的具体规则，依据该规则，可以将应用工业互联网的工业企业划分为一级企业、二级企业和三级企业，并且，根据企业级别的不同，指南中进一步规定了不同程度的规范事项，为工业互联网企业的网络安全管理提供了较为详细的指引。

## 二、 案例事件

### (一)工业和信息化部网络安全管理局 2019 年一系列检查结果公示

2019 年，工业和信息化部网络安全管理局（“**网络安全管理局**”）按照《国务院办公厅关于推广随机抽查规范事中事后监管的通知》、《工业和信息化部**“双随机一公开”**监管实施办法》、《工业和信息化部随机抽查事项清单（2018 年版）》等相关要求，组织对部分电信和互联网企业、域名机构的网络安全防护工作情况、网络与信息安全责任落实情况、网络数据安全保护责任及管理措施落实情况等开展随机抽查。

2019 年 12 月 10 日，网络安全管理局发布工作动态并对上述检查结果进行公示[2]。工作动态显示，抽查中共发现 68 家电信和互联网企业、域名机构不同程度存在违规情况。经过归纳总结，本次抽查反映的主要问题及对应的存在该问题的企业数量统计如下表所示：

| 问题类型 | 存在此问题的企业数量 | | | |
|---|---|---|---|---|
| | 基础电信企业[3]（共 23 | 互联网企业（共 37 家） | 虚拟运营商（共 7 家） | 域名注册和管理服务 |

| | | | | |
|---|---|---|---|---|
| | 家） | | | 机构（共1家） |
| 业务系统部分配置不符合网络安全防护标准有关要求 | 14 | 4 | / | / |
| 业务系统未开展定级备案、符合性评测和/或安全风险评估工作 | 1 | 5 | / | 1 |
| 未严格落实物联网卡安全管理相关规定 | 6 | / | 4 | / |
| 未严格落实电话用户真实身份信息登记相关规定 | 6 | / | 5 | / |
| 未及时整改前期已发现的网络安全隐患 | 2 | 2 | / | / |
| 未开展网络安全事件应急演练 | 1 | 1 | / | / |
| 未有效采取数据分类和/或敏感信息加密等保护措施 | / | 17 | / | / |
| 互联网信息安全管理系统部分功能和/或性能指标不符合电信主管部门以及相关标准要求 | / | 16 | / | / |
| 未有效建立用户信息安全保护制度 | / | 12 | / | / |
| 未有效建立企业新业务安全评估制度 | / | 10 | / | / |
| 未建立恶意程序处置的技术手段 | / | 1 | / | / |
| 未对批量导出、复制、销毁信息实行审查，并采取防泄密措施 | / | 1 | / | / |

**简评**：从上述统计可以看出，就普通用户及大量互联网服务提供企业最关注的“互联网企业”这一统计项目来看，最核心、高发的问题仍然集中在数据保护、安全管理、信息安全保护、安全评估方面，这些问题在抽查的37家互联网企业当中出现的概率都较高，从一定程度上也反映出对于没有被抽查到的更广泛的互联网服务提供企业来说，这些问题或者类似的问题也可能普遍存在，值得依据法规及时自查，并在被主管机关抽查之前及时整改。

## (二) 中国人民银行、公安部对买卖银行卡或账户的个人实施联合惩戒

2019年12月16日，中国人民银行（“**人民银行**”）与公安部联合发布通知，为有效遏制买卖银行卡、账户的行为，强化源头治理的方式，决定依法对买卖银行卡或账户的个人实施惩戒。通知表明，人民银行已将“3.26”特大贩卖银行卡和企业对公账户案中602名涉案个人的信息移送金融信用信息基础数据库，银行业金融机构（“**银行**”）和非银行支付机构（“**支付机构**”）将对相关个人实施5年内暂停其银行账户非柜面业务、支付账户所有业务，并不得为其开立账户的惩戒措施。

惩戒期满后，对上述个人办理新开立账户业务的，银行和支付机构应加大审核力度。通知提出“异议制度”，若个人对惩戒措施提出异议的，银行和支付机构应当做好解释说明，若个人不认同公安机关对其认定的，银行和支付机构应当及时告知个人认定涉案事实的公安机关名称，个人可以向相关公安机关进行申诉。

**简评**：本通知为跨部门联合下发，提出的惩戒措施是对个人信息犯罪刑事罚则体系的完善和补充。中国人民银行与公安部联合实施惩戒工作，一方面公安机关利用极强的侦查能力发现了一批涉嫌违法犯罪的个人；另一方面该等个人当中如有尚不涉及刑事犯罪的个体，则人民银行可通过类似本次惩戒的手段打击违法行为。

### (三)工信部通报第一批侵害用户权益行为 App

根据《工业和信息化部关于开展 App 侵害用户权益专项整治工作的通知》的要求，App 侵害用户权益专项整治行动已按计划、分阶段推进。工业和信息化部（“**工信部**”）于 2019 年 12 月 19 日发布“关于侵害用户权益行为的 App（第一批）通报”[4]，通报显示，专项行动中，自查自纠阶段共有八千多款 App 完成整改。监督检查阶段，工信部组织第三方检测机构对各大应用商店 App 进行检查，并进行督促整改。截至该通报发布时，尚有 41 款 App 存在问题。经过归纳总结，本次专项行动中反映的主要问题及对应的存在该问题的 App 数量统计如下表所示：

| 问题类型 | 存在此问题的 App 数量 | 占比 |
|---|---|---|
| 私自收集个人信息 | 21 | 51% |
| 过度索取权限 | 19 | 46% |
| 账号注销难 | 15 | 37% |
| 不给权限不让用 | 11 | 27% |
| 私自共享给第三方 | 11 | 27% |
| 强制用户使用定向推送功能 | 7 | 17% |
| 超范围收集个人信息 | 3 | 7% |
| 频繁申请权限 | 1 | 2% |

工信部针对上述通报展开了后续行动，并于 2020 年 1 月 3 日发布通报，通报表明，依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》等法律和规范性文件要求，针对经第三方检测机构核查复检、尚未按要求完成整改的 3 款 APP，进行下架处理。

### (四)App 治理工作组关于 61 款 App 存在收集使用个人信息问题的通告

2019 年 12 月 20 日，App 治理工作组发布“关于 61 款 App 存在收集使用个人信息问题的通告”[5]，列明了近期在评估中发现的 57 款 App 存在收集使用个人信息问题的具体名单和具体问题。此外，该通告也提到，针对 7 月至 10 月期间经发送整改通知并建议一个月内整改而至今仍未完成整改的 4 款 App，已将核验结果提交相关部门，将建议依法予以处置。经归纳总结，本次评估发现的 App 存在的主要问题及占比如下表所示：

| 问题方面 | 被整改 App 数量 | 占比 | 简评 |
|---|---|---|---|
| 未明示收集使用个人信息的目的、方式和范围 | 55 | 96% | 本次监管中涉及“未逐一列出嵌入的第三方 SDK 收集使用个人信息的目的、类型”问题的 App 有 34 款，强调了委托的第三方或嵌入的第三方代码、插件收集使用个人信息时也应当符合相关规定。 |
| 未经同意向他人提供个人信息 | 47 | 82% | 此方面涉及的监管要点为：转让个人信息时，应满足两个条件之一：（1）告知个人信息主体转让目的、数据接收方类型及可能产生的后果，并事先征得个人信息主体的授权同意；或（2）去标识化，且确保数据接收方无法识别或者关联个人信息主体。 |
| 未经同意收集使用个人信息 | 39 | 68% | 该方面具体包括“违规收集”、“私自收集”、“超范围收集”等类型。 |
| 未建立并公布安全投诉、举报渠道或未按法律规定提供删除或更正个人信息功能 | 39 | 68% | 在“注销功能”方面，本次监管关注点与《信息安全技术 个人信息安全规范》（10 月 22 日最新修订稿）的修改相对应，针对注销难问题，提出更细致的要求，包括注销步骤不应设置不合理的条件或额外增加信息主体义务。 |
| 未公开收集使用规则 | 34 | 60% | 此方面主要针对隐私政策的合法合规性，本次评估除强调 App 应当制定隐私政策并明示外，还提出了更细致的要求，包括隐私政策文字显示不宜过小、过密，链接应当易于访问等。 |
| 违反必要性原则，收集与其提供的服务无关的个人信息 | 31 | 54% | 该方面具体包括“不给权限不让用”、“频繁申请权限”、“过度索取权限”等类型。 |

该通告体现的若干具体问题如下表所示：

| 问题方面 | 具体问题 |
| --- | --- |
| 未明示收集使用个人信息的目的、方式和范围 | 在申请打开可收集个人信息的权限时，和/或收集用户身份证号等个人敏感信息时，未同步告知用户其目的 |
| | 未明示收集的个人信息的目的、方式和范围 |
| | 未逐一列出嵌入的第三方 SDK 收集使用个人信息和目的、类型 |
| | 收集使用个人信息的目的、方式和范围发生变化时，未以更新隐私政策等方式通知用户 |
| | 有关个人信息收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解 |
| 未经同意向他人提供个人信息 | 既未经用户同意，也未做匿名化处理，通过客户端嵌入的 SDK 向第三方提供个人信息或将个人信息传输到境外云服务器；或通过客户端向第三方传输个人信息 |
| 未公开收集使用规则 | 在首次运行时未经过弹窗等明显方式提示用户阅读隐私政策 |
| | 隐私政策难以访问、难以阅读或未提供简体中文版 |
| | 在 App 中无法找到隐私政策 |
| 违反必要性原则，收集与其提供的服务无关的个人信息 | 申请打开的权限或收集的个人信息与现有业务功能无关 |
| | 收集个人信息的频度超出业务功能实际需要 |
| | 将 targetSDKversion 值设置小于 23，要求用户一次性同意开启多个可收集个人信息的权限，用户不同意则无法使用 |
| | 因用户不同意打开非必要的权限，拒绝提供所有业务功能或其中一项业务服务 |
| | 首次打开 App 时，强制要求用户输入非必要个人信息 |
| 未经同意收集使用个人信息 | 以默认选择同意隐私政策的非明示方式征求用户同意 |
| | 征得用户同意前就收集个人信息 |
| | 用户撤销权限授权，明确表示不同意收集该类个人信息后，仍通过其他途径收集设备个人信息 |
| | 用户明确表示不同意打开电话、存储、位置等权限后，仍频繁征求用户同意，干扰用户正常使用 |
| 未建立并公布安全投诉、举报渠道或未按法律规定提供删除或更正个人信息功能 | 未建立并公布个人信息安全投诉、举报渠道 |
| | 未提供有效的注销用户账号功能 |
| | 为注销用户账号设置不合理条件 |

**(五)2020 年将制定个人信息保护法**

2019 年 12 月 20 日，全国人大常委会法工委在其第三次记者会中介绍[6]，2020 年的立法工作计划已经全国人大常委会第四十四次委员长会议原则通过，备受关注的《个人信息保护法》将于 2020 年制定。

**后记：**

海问在网络安全、数据合规领域积累丰富的经验，亦持续关注不断更新的法律法规及与数据合规有关的时事热点。您可通过如下链接浏览此前的《海问观察：网络安全及数据合规动态》：

《海问观察：网络安全及数据合规动态》（2019 年 9 月上半月）
《海问观察：网络安全及数据合规动态》（2019年9月下半月-10月上半月）
《海问观察：网络安全及数据合规动态》（2019年10月下半月-11月）

实习生朱安琪对本文亦有贡献。

---

[1] 该法规于 2019 年 11 月 28 日由国家互联网信息办公室、工业和信息化部、公安部以及市场监管总局联合发布，但于 2019 年 12 月 30 日在国家互联网信息办公室官方网站正式对外公开，详见：http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm?scene=2&clicktime=1577667572&enterid=1577667572&from=singlemessage&isappinstalled=0。

2 来源见工信部官网，网址：http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057728/c7565082/content.html。

[3] 基础电信企业，指四个基础电信运营商（即中国电信、中国移动、中国联通和中国广电）的各省级分公司，本次抽查的统计口径以基础电信运营商省级分公司为基础。

4 来源见工信微报，网址：https://mp.weixin.qq.com/s/4aLKXLtFKM1vLBiFReLsxA。

5 来源见 App 治理工作组，网址：https://mp.weixin.qq.com/s?src=11&timestamp=1577781488&ver=2067&signature=ufk1SRMn4fifamVrF0X2z9Asnui00VBTktJDfWl8kKryXAANoIO0sAnik9itSC6U4s0gz9FAtXVzP*ptC4O4Lmb1OcDdXFa5Qc15He1wy9rirNpZZ2eOIIP0mVC5wZ5v&new=1。

6 来源见中国人大网，网址：http://www.npc.gov.cn/npc/c30834/201912/885be3e9128247518bfb25242f56aec4.shtml。