全球数据安全观察

总第 96 期 2022 年第 24 期

(2022.07.04-2022.07.10)

大数据协同安全技术国家工程研究中心

目录

政策形势

1、《数据出境安全评估办法》发布

7 月 7 日，国家互联网信息办公室公布《数据出境安全评估办法》（简称《办法》），自 2022 年 9 月 1 日起施行。国家互联网信息办公室有关负责人表示，出台《办法》旨在落实《网络安全法》、《数据安全法》、《个人信息保护法》的规定，**规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，切实以安全保发展、以发展促安全。**

《办法》中规定了评估触发条件、评估内容、具体流程、评估主体等相关要求，对于评估活动不同阶段的重点事项、关注内容进行了明确，并提出了评估结果复评、评估结果有效期、重新申报评估等要求。

http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm

2、关于《个人信息出境标准合同规定（征求意见稿）》公开征求意见的通知

7 月 5 日，浙江省市场监管局发布全国首个互联网平台企业竞争合规的省级地方标《互联网平台企业竞争合规管理规范》（简称“规范”），8 月 5 日起在全省实施，旨在压实企

业的竞争合规主体责任，实现政府监管模式下的平台自治。

《规范》以互联网平台企业“自我优待”、“大数据杀熟”、算法滥用、强制“二选一”、资本无序扩张等破坏公平竞争的行为为研究对象，以发挥互联网平台企业竞争合规主体责任为出发点，从反垄断、反不正当竞争两个角度，全面梳理互联网平台企业竞争合规相关风险，明确互联网平台企业竞争合规管理活动要点。

https://mp.weixin.qq.com/s/rb9kdCxukAiKX5ph74ZSwg

3、深圳发布《企业合规管理体系（征求意见稿）》

7 月 7 日深圳市司法局发布公开征求《企业合规管理体系（征求意见稿）》意见的通告，以建立深圳企业合规地方标准，为深圳企业提供标准化指引，进一步加快合规示范区建设。

该征求意见稿规定了评价深圳企业（经营者）建立、运行、维护和改进合规管理体系的基本原则、合规评价体系，适用于深圳市任何类型、规模、性质和行业的企业（经营者）用于合规自评和第三方面向深圳企业（经营者）开展合规评价。此举旨在推动深圳企业（经营者）的治理机构、最高管理者运用普遍接受的良好治理方法、道德规范和社会准则来塑造企业（经营者）的合规之道，使合规文化成为企业（经

营者）文化的重要组成部分，将合规理念、合规管理融入到企业（经营者）的其他管理中，助力企业预防、发现和处理合规风险，并证明企业为实现上述目标已经实施了合理和适当的措施。

https://iiaf.org.cn/Item/213522.aspx

4、上海通管局启动网络和数据安全检查工作

7 月 7 日，上海市通信管理局发布通知，决定组织开展 2022 年上海市电信和互联网行业网络和数据安全检查工作。

通知中明确了此次检查工作的总体目标、检查对象、检查内容、工作安排以及工作要求，其中在检查内容部分明确了**检查企业落实《数据安全法》《电信和互联网企业数据安全合规性评估要点》的要求**，以及检查企业按照《个人信息保护法》《电信和互联网用户个人信息保护规定》《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》《关于开展信息通信服务感知提升行动的通知》要求，落实电信和互联网行业个人信息保护和用户权益保护专项治理工作情况。

https://mp.weixin.qq.com/s/qrxj6OLKeb1TD_Izn0B6ZA

5、欧洲议会通过了《数字服务法》和《数字市场法》

7 月 5 日，欧洲议会通过了《数字服务法》和《数字市场法》。这意味着欧美间的数字博弈正式迈入新阶段，而把控市场的美国科技巨头们即将迎来新的监管挑战。

《数字服务法》对 2000 年的《电子商务法》进行了更新和澄清，同时针对在线平台的透明度要求和问责机制给出了规范。《数字服务法》将引入一些重要的保护措施，尽管它没有全面禁止广告定向推送，但该法将禁止任何针对未成年人的定向广告等。在打击非法内容方面，该法案强调各大在线平台需要承担一定的社会义务。根据《数字服务法》，未能履行准则的公司将面临高达其全球营业额 6%的罚款。值得关注的是，每月拥有 4500 万户或更多用户的平台将接受独立审计，以防止其发布假新闻和非法内容。这些平台还必须向（经批准的）研究人员开放其算法和数据，使他们能够研究系统可能造成的影响和潜在危害。

《数字市场法》则是要求被称为“看门人”的大型平台公司不能滥用市场支配地位打压其他竞争企业，不能未经用户许可强行推送广告或安装应用软件。违反上述两项法律的企业都将被处以巨额罚款。所谓的“看门人”企业指那些提供社交网络、搜索引擎等“心平台服务”的大型企业，市值在 750 亿欧元以上或年营业额 75 亿欧元，且每月有 4500 万以上终

端用户，每年有 1 万户商业用户。

https://mp.weixin.qq.com/s/INZ9G2UmWX-pMYoFL33SVA

技术、产品与市场

1、NIST 发布新算法应对量子攻击，可支持下一代加密标准

7 月 5 日，美国国家标准与技术研究所（NIST）正式发布四种新的加密算法，用于保护联邦政府计算机和应用系统应对新型量子计算的网络攻击。据了解，这四种新加密算法包括一种用于通用加密用途的算法：CRYSTALS-Kyber，以及另外三种用于数字签名和身份验证的算法：CRYSTALS-Dilithium、Falcon 和 Sphincs+，它们将在 2024 年之前支持 NIST 未来的加密标准。

值得注意的是，本次推出的四种算法中，有三种算法：CRYSTALS-Kyber、Crystals-Dilithium 和 Falcon 是基于格（lattice）的算法。NIST 预计在后续应用中，大多数企业组织会使用 Crystals-Dilithium，原因是它性能良好、文档完备，而且更易于实施。不过，尽管 Falcon 算法需要相对复杂的实施过程，也无法适用于所有设备上，但它更小巧，会在使用较小数字签名的应用场合发挥作用。

https://mp.weixin.qq.com/s/jmMHEs1P0RKLutt8uj3UsQ

2、调查显示传统数据安全工具在 60%情况下无法抵御勒索软件攻击

据数据安全提供商 Titaniam Inc. 发布的《数据渗透和勒索状况报告》显示，虽然超过 70% 的企业拥有一套现有的预防、检测和回溯解决方案，但近 40% 的企业在过去一年中仍然受到了勒索软件攻击。

研究结果表明，**传统的数据安全工具，如安全备份和恢复工具、提供静态和传输中加密的解决方案、标记化和数据屏蔽等，在 60% 的时间里未能保护企业的数据免受勒索软件威胁**。传统数据安全工具的问题不在于它们没有强大的安全措施，而在于攻击者可以通过窃取凭证来实现对关键数据资产的特权访问，从而避开这些控制。

该研究强调，企业不能仅仅依靠传统的数据安全工具来抵御数据渗透和双重勒索勒索软件攻击，他们需要能够对使用中的数据进行加密，以阻止恶意行为者的行为。

https://www.cnbeta.com/articles/tech/1288629.htm

3、数据灾备需求正向全行业延伸，容灾将开启蓝海市场

频发的安全事件对数字经济发展带来巨大挑战，全行业从危机管理现实需求出发，正促进灾备体系向全行业广泛延伸应用。威胁加剧、灾备云化、云化应用是灾备向全行业延

伸应用的关键。

伴随着云容灾市场的成熟，其带来的广泛应用终将推动其驶入蓝海市场。全行业对业务连续性、数据保护工作持续增量，以及对不同云提供迁移的便利支持，由第三方技术支撑的云容灾解决方案对业务、数据再生速度快，多云异构对多云环境的完美支持等，已经逐渐成为各级企业的刚性需求。而备份和归档相对而言则是红海市场，其应用仅限于特定行业的合规需求。

企业以业务、经营、生产为中心的，基于业务连续性，数据资产保护为核心视角的灾难应急恢复，容灾技术才是最佳选择，时代也正推动着云容灾解决方案向更广泛的行业应用一路前行。

https://mp.weixin.qq.com/s/j0i8AN-vwilH9ZqTsQGyoQ

4、业界首发《 数字城市网络安全评价指数白皮书（2022）》

白皮书首次提出“数字城市网络安全评价指标”这一概念及评价标准，从安全的维度，为数字城市发展评价指标体系的建立，提供重要参考。

据了解，“数字城市网络安全评价指标”围绕城市数字化网络安全管理保障、城市数字化网络安全技术保障、城市数字化网络安全运营保障 3 个方面形成城市数字化网络安全评

价指标体系，包含 11 个二级指标，48 个三级指标，涵盖城市数字化网络安全顶层设计、管理机制、基础设施安全、业务系统安全、监测预警、响应处置与应急保障等多方面内容。期待借助这本报告的全方位评估，为我国各城市数字化转型过程中的网络安全建设提供方向指引。

https://mp.weixin.qq.com/s/ZLU9Cvwf0rvUZCPw6jxUfw

5、人为错误依然是最重大的安全威胁

根据 SANS 最新发布的 2022 年安全意识报告，人为错误仍然是网络攻击和数据泄露的最主要和最有效媒介。举一个浅显易懂的例子：迄今为止后果最为严重的几次超大规模（影响用户数超过 1 亿）数据泄露事件大多与 ElasticSearch 数据库配置错误有关。

研究发现，在企业面临的最大威胁中，网络钓鱼攻击位居榜首，商业电子邮件泄露(BEC)攻击位居第二，勒索软件位居前三。前三名中有两个依赖于社会工程策略，虽然勒索软件攻击可以通过脚本漏洞利用实现自动化，但也经常会利用社会工程策略或勾结内部人员。

此外，该报告还指出，绝大多数勒索软件攻击也都是从网络钓鱼电子邮件或利用弱密码开始的。

https://www.secrss.com/articles/44343

业界观点

1、姚期智：只有数据要素流通起来才能产生大规模的经济价值

“数据正在成为数字经济的关键生产要素，充分释放数据要素价值，迫切需要加快推进数据要素市场化建设。”图灵奖获得者、中科院院士、清华大学交叉信息研究院院长姚期智近日接受记者专访时表示，数字经济的发展需要核心技术为基础，应该进一步增加数据交易类技术、数据流通审计技术、数据建模与模型治理等底层技术的投入，并以这些底层技术“新基建”为引领，加快实现数据要素市场化配置、合理分配数据要素收益等。

在姚期智看来，数据产权、流通交易、收益分配、安全治理等都与数据要素市场化建设密切相关，需要四大类关键技术的支撑。

第一，数据交易类技术，包括高效实现数据撮合、数据价值分配的技术，以及记录数据交易过程的技术。

第二，数据流通过程中的安全审计、合规审计类技术。

第三，数据加工分析的技术，包括辅助数据科学家建模，或自动化建模的技术。

第四，数据模型治理的技术。

https://mp.weixin.qq.com/s/bJ1h6eSCUm3TRgXMWvH82w

2、方滨兴：广州发展数据安全产业应抓住两个机遇

在 7 月 8 日举行的“2022 · 云山论剑”广州数据安全峰会上，中国工程院院士方滨兴接受采访时建议，广州发展数据安全产业应抓住两个机遇：一方面通过发展网络安全保险，转移数据安全风险；另一方面，建立交易数据使用权的可信计算平台，保留数据所有权，释放数据使用权。

方滨兴说，网络安全风险最有效的解决方案是，一种是风险缓解，一种是风险转移。他认为，网络安全保险作为风险转移的重要手段，在网络安全领域引入保险机制，是解决我国网络安全风险问题，提高网络安全风险治理能力的新途径。网络安全保险有助于构建新型网络安全生态，赋能企业的网络安全整体防灾水平。

如何平衡数据要素流动与个人信息保护的冲突，如何在确保数据安全的前提下，最大限度地挖掘大数据价值，是当前面临的一大难题。“我个人推崇数据不动、程序动。眼下对于广州而言，数据使用权交易会是一个机会”，方滨兴说，数据使用权交易强调可用不可见，有利于保障数据安全。

他建议政府层面构建可信计算平台，数据共享汇聚到这个平台后，通过平台进行数据交易。与过去数据交易不一样

的是，平台“交易数据使用权，而不是所有权。因为交易所有权走不动的，而交易使用权，买方用一次就付你一次钱”，他说，这样数据交易就活跃起来了，“我觉得这是个机会”。https://www.sohu.com/a/565374739_161795

3、沈昌祥：主动免疫可信计算让黑客进不去、拿不走、赖不掉

在 7 月 8 日举行的“2022·云山论剑”广州数据安全峰会上，中国工程院院士、中央网信办专家咨询委员会顾问、国家集成电路产业发展咨询委员会委员、国家三网融合专家组成员沈昌祥应邀通过远程直播做了《开创安全可信数字经济新生态》主题演讲。他认为，筑牢网络安全防线，需要构建主动免疫防护新体系。

“利用缺陷挖掘漏洞进行攻击是网络安全永远的命题”，沈昌祥在演讲中指出，传统的“封堵查杀”（即杀病毒、防火墙、入侵检测“老三样”）难以应对未知恶意攻击，且容易被攻击者利用，找漏洞、打补丁的传统思路也不利于整体安全。

那么，在数字化转型的新形势下，如何保障网络安全、数据安全？沈昌祥指出，根据我国《网络安全法》《国家网络空间安全战略》《关键信息基础设施安全保护条例》以及网络安全等级保护制度 2.0 标准等要求，夯实网络安全基础，需

要全面使用安全可信的产品和服务，以构建关键基础设施安全保障体系。

如何构建网络安全主动免疫保障体系呢？沈昌祥提出，第一是利用一种新模式计算，即主动免疫可信计算。主动免疫可信计算在实施运算的同时进行免疫的安全防护，能及时识别“自己”和“非己”成分，从而使攻击者无法利用缺陷和漏洞对系统进行非法操作，达到预期的计算目标；二是建立计算部件+防护部件“二重”体系结构；三是建立可信安全管理中心支持下的主动免疫三重防护框架。加上可信动态访问控制，全程管控，技管并重，最终达到让攻击者“进不去、拿不到、看不懂、改不了、瘫不成、赖不掉”的防护效果。

https://www.toutiao.com/article/7117985451641668129/

4、严宏伟：以新思维破解政务数据有序共享难题

建设数字政府，已经成为加强党的执政能力建设，增强政府治理效能，提高政府服务效率，推进国家治理体系和治理能力现代化的重要举措。建设数字政府的着力点是实现数据资源有序共享。随着全国电子政务一体化的持续建设和应用，数据资源共享在数字政府建设过程中起着越来越重要的作用。

树立新思维，破解政务数据有序共享难题，中共中央党

校（国家行政学院）电子政务研究中心副主任严宏伟提出以下四点认识:

（1）树立系统思维，保证政务共享数据资源的质量;

（2）树立产权思维，明晰政务数据共享的各方权益;

（3）树立创新思维，发挥政务数据支持决策咨询的潜能;

（4）树立底线思维，保护动态政务数据的安全。

https://mp.weixin.qq.com/s/fX6741PpytUgWD6aGKK6Rg

5、解读：《个人信息出境标准合同规定（征求意见稿）》

6 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规定（征求意见稿）》（“标准合同规定”）。《个人信息保护法》第三十八条明确列举了三种向中国境外提供个人信息的路径，包括:（1）通过国家网信部门组织的安全评估;（2）通过专业机构进行的个人信息保护认证;（3）与境外接收方订立国家网信部门制定的标准合同。由于订立标准合同兼具成本优势和可操作性，因此出境标准合同也一直是企业关注的重点。作为跨境提供个人信息的选择路径之一，理解标准合同文本的适用及内容有重要意义。

标准合同规定提供了中国版跨境传输个人信息的标准合同文本，在使用该标准合同文本时可以进一步关注下述事项:

（1）与其他出境相关的合同的关系。中国版标准合同文本规定了跨境传输个人信息的法定责任义务，个人信息处理者与境外接收方签订与个人信息出境活动相关的其他合同，均不得与标准合同相冲突。而在实践中，其他法域的监管机构也通过相应的标准合同文本管理跨境个人信息传输（例如欧盟 SCCs 等），因此跨国企业将会面临着协调不同法域标准合同文本的问题。

（2）关于适用委托处理的场景。中国《个人信息保护法》规定个人信息处理者和受托人的角色。个人信息处理者在个人信息处理活动中可以自主决定个人信息处理目的、处理方式，而受托人则是接受个人信息处理者委托而处理个人信息。中国版标准合同文本规定了个人信息处理者向境外接收方提供个人信息的模式，并不适用受托人向境外提供个人信息的场景。不过，中国版标准合同在境外接收方义务中，规定了“受个人信息处理者委托处理个人信息”的义务，说明境外接收方可以是受托人的角色，接受委托处理个人信息。

（3）单独同意。中国版标准合同在“个人信息处理者的义务”及境外接收方再转移的义务中，均规定了“单独同意”的要求，与《个人信息保护法》的要求保持一致。值得注意的是，中国版标准合同在“单独同意”的部分也提到了“相关法律法规规定无需取得个人单独同意的除外”，进一步表

示单独同意应该是同意的子集，如有其他个人信息处理的合法基础，并不必须取得跨境提供个人信息的单独同意。

（4）责任承担。中国版标准合同文本明确规定了“个人信息处理者”的义务、“境外接收方”的义务。在责任承担上，个人信息处理者和境外接收方对因违反标准合同而共同对个人信息主体造成的任何物质或非物质损害承担连带责任。

同时，为了充分保障个人信息主体可以获得赔偿，中国标准合同文本以境内的“个人信息处理者”为抓手，明确个人信息处理者应就境外接收方因违反标准合同而对个人信息主体造成的任何物质和非物质损失向个人信息主体负责，之后再向境外接收方追偿。

https://mp.weixin.qq.com/s/DIb4dc3F-noUwLQ0trnDIg

数据安全事件

1、AMD 被黑客窃取 450GB 机密数据原因曝光: 用 123456 当密码

2022 年 7 月 5 日报道，上月底 RansomHouse 表示，黑客从 AMD 服务器上盗取了 450GB 的数据。RansomHouse 自称是一个专业调解社区，旨在帮助黑客和被勒索的公司之间进行谈判付款。

早在 2022 年 1 月 5 日，AMD 服务器就被黑客组织入侵。RansomHouse 目前公布了被窃取的部分数据作为证据，其中包括一些 AMD 员工的密码和一些系统文件。据 RansomHouse 称，AMD 几乎没有安全系统，许多员工使用简单的密码，如 “password”、“123456” 或 “amd123”。AMD 的安全部门也使用了这些密码，正是因为这个原因黑客才窃取了上述大量数据。

https://www.ithome.com/0/627/976.htm

2、HackerOne 员工从漏洞赏金报告中窃取数据以获取经济利益

2022 年 7 月 5 日报道，HackerOne 披露了涉及一名前雇员的事件的详细信息，据称该雇员访问了内部数据以获取个

人经济利益。未具名的个人从提交给漏洞赏金平台的安全报告中获取信息，并试图在平台之外披露相同的漏洞。据HackerOne 称，他可以访问 2022 年 4 月 4 日至 6 月 23 日的数据。

https://portswigger.net/daily-swig/hackerone-employee-stole-data-from-bug-bounty-reports-for-financial-gain

3、连锁酒店巨头万豪证实其又发生一起数据泄露事件

2022 年 7 月 7 日报道，酒店集团万豪国际集团已经证实了另一起数据泄露事件，黑客们声称窃取了 20GB 的敏感数据，包括客人的信用卡信息。该事件首先由 Databreaches.net 报道，据说发生在 6 月，一个不知名的黑客组织宣称他们利用社会工程欺骗马里兰州一家万豪酒店的员工，以让他访问了该员工的电脑。提供给 Databreaches.net 的数据样本显示了从 2022 年 1 月开始的航空公司机组成员的预订记录和客人的姓名和其他细节以及用于预订的信用卡信息。

万豪表示，在威胁者联系公司进行敲诈之前，连锁酒店已经发现并正在调查这一事件，万豪表示它没有支付这笔钱，被访问的数据主要包含有关酒店运营的非敏感内部业务文件。

https://www.cnbeta.com/articles/tech/1289421.htm

4、美国婚姻部承认因不安全的亚马逊存储桶导致数据泄露

2022 年 7 月 6 日，据外媒报道，美国婚姻部（AMM）表示，在今年早些时候向 FBI 报告了敏感数据泄露事件后，它正在处理另一个数据安全问题。

WebsitePlanet 的安全研究人员本周发布了一份报告，称他们发现了一个不安全的亚马逊存储桶，其中包含来自教堂的大量数据，没有任何密码保护或加密控制。暴露的信息包含 630 GB 的数据，涉及约 185,000 名主礼人员和大约 15,000 对已婚夫妇以及婚礼宾客的个人信息。

https://therecord.media/american-marriage-ministries-acknowledges-data-exposure-after-earlier-incident-reported-to-fbi/?web_view=true

5、云配置错误暴露了 Amazon S3 存储桶中的 3TB 敏感机场数据

2022 年 7 月 7 日，据外媒报道，错误配置的 Amazon S3 存储桶导致 3TB 的机场数据（超过 150 万个文件）可公开且无需身份验证的访问，凸显了旅游行业中不安全的云基础设施所带来的危险。

Skyhigh Security 发现的泄露信息包括员工个人身份信息 (PII) 和其他敏感的公司数据，影响哥伦比亚和秘鲁的至

少四个机场。PII 的范围从航空公司员工、身份证的照片（如果被恐怖组织或犯罪组织利用可能会造成严重威胁）到有关飞机、燃料管线和 GPS 地图坐标的信息。报告称，该存储桶（现已安全）包含可追溯到 2018 年的信息。

https://www.darkreading.com/application-security/cloud-misconfig-exposes-3tb-sensitive-airport-data-amazon-s3-bucket?&web_view=true

6、黑客公布伊朗钢铁制造企业近 20G 绝密文件，疑似以色列幕后支持

2022 年 7 月 7 日，攻击三家伊朗钢铁制造企业的黑客组织 Predatory Sparrow 发布了所谓的近 20GB 绝密数据，其中包含公司文件，这些文件揭示了这些设施与伊朗强大的伊斯兰革命卫队的隶属关系。在一系列英语和波斯语的推文中，这个自称为 Gonjeshke Darande 或 Predatory Sparrow 的组织表示，19.76GB 的文件只是即将发布的“第一部分”。该组织还发布了一张似乎是钢铁设施内部的图像。

https://www.secrss.com/articles/44473

7、美国眼科诊所遭遇数据泄露，影响 92,000 名患者

2022 年 7 月 4 日报道，位于密苏里州的一家医疗诊所已

向美国监管机构通报了一起数据泄露事件。Mattax Neu Prater 眼科中心于 6 月底宣布了违规行为，但该事件发生在 2021 年 12 月。据 HIPAA 称，有 92,361 人受到了违规行为的影响。提供手术和非手术护理的 Mattax Neu Prater 表示，“第三方数据安全事件”可能导致未经授权访问某些患者的敏感个人信息。

https://portswigger.net/daily-swig/us-eye-clinic-suffers-data-breach-impacting-92-000-patients

8、Mangatoon 数据泄露暴露了 2300 万个账户的数据

2022 年 7 月 9 日报道，漫画阅读平台 Mangatoon 遭遇数据泄露，黑客从不安全的 Elasticsearch 数据库中窃取了属于 2300 万用户帐户的信息。泄露事件暴露了姓名、电子邮件地址、性别、社交媒体账户身份、来自社交登录的身份验证令牌和加盐的 MD5 密码哈希。数据泄露是由一位名叫“pompompurin”的知名黑客实施的，他说他们从使用弱凭据的 Elasticsearch 服务器上窃取了数据库。

https://www.bleepingcomputer.com/news/security/mangatoon-data-breach-exposes-data-from-23-million-accounts/

9、Quantum 勒索软件攻击已经影响 657 个医疗保健机构

2022 年 7 月 7 日，应收账款管理公司 Professional Finance Company Inc. (PFC) 表示，2 月下旬的勒索软件攻击导致数据泄露，影响了 600 多家医疗机构。该公司于 5 月 5 日开始通知受影响的医疗保健提供者的患者，称正在进行的调查发现攻击者在加密 PFC 的某些系统之前访问了包含其个人信息的文件。攻击期间暴露的敏感信息包括患者的姓名、地址、应收账款余额以及有关向账户付款的信息。

https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-affects-657-healthcare-orgs/

10、国家计算机病毒应急处理中心披露 15 款 App 存在隐私不合规行为

国家计算机病毒应急处理中心近期通过互联网监测发现 15 款移动 App 存在隐私不合规行为，违反网络安全法、个人信息保护法相关规定，涉嫌超范围采集个人隐私信息。

包括未向用户告知个人信息处理者的名称或者姓名和联系方式，或处理的个人信息种类、保存期限等等行为。

针对上述情况，国家计算机病毒应急处理中心提醒广大手机用户首先谨慎下载使用以上违法、违规移动 App，同时要注意认真阅读其用户协议和隐私政策说明，不随意开放和

同意不必要的隐私权限，不随意输入个人隐私信息，定期维护和清理相关数据，避免个人隐私信息被泄露。

https://mp.weixin.qq.com/s/eDI5Na6eWVpsMypoSqN_YQ