

NEWSLETTER

数据合规

2019 第三期 /总第三期

## 数据合规时事速递

北京市环球律师事务所

2019年6月4日

## 目录

前 言 .....	3
一、新法速递 .....	4
1. App 违法违规认定方法草案发布，直击隐私保护痛点 .....	4
2. 等保 2.0 出台，网络安全将发生哪些变化 .....	7
3. 《数据安全管理办法》征求意见 监管部门亮剑 App 收集隐私 .....	9
4. 《网络安全审查办法》公开征求意见，网络审查要求渐严 .....	11
5. 日本拟修改《个人信息保护法》 新增企业停发广告义务 .....	13
二、监管动态 .....	14
1. 多款 App 收集个人敏感信息 广东通信管理局依法查处涉事企业 .....	14
三、相关案例 .....	15
1. 高通近 40 款芯片被曝出泄密漏洞！波及数十亿部手机 .....	15
2. 信托公司遭罚：违法查询个人信息和企业信贷信息 .....	16
3. 广东侦破一批涉个人信息网络违法犯罪案件 抓获万余名嫌疑人 .....	17
4. 大连警方破获侵犯公民个人信息案 查获个人信息近亿条 .....	18
四、环球解读 .....	19
1. 网信办送“儿童节礼物”：拟新规强化儿童信息保护 .....	19

## 前言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和网络安全监管。我国对个人信息保护和网络安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。据时代的机遇与挑战。



### 团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。



**孟洁**

合伙人律师

直线：86-10-6584-6768

总机：86-10-6584-6688

邮箱：mengjie@glo.com.cn

## 一、新法速递

### 1. App 违法违规认定方法草案发布，直击隐私保护痛点<sup>1</sup>

#### 草案概况

2019年5月5日，App专项治理工作组在其官方平台上发布通知，对《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“《App违法违规认定方法》（征求意见稿）”）公开征求意见。

此前，四部门联合发布的《App违法违规收集使用个人信息自评估指南》主要是要求App运营者对其收集使用个人信息的情况进行自查自纠。而本次发布的《App违法违规认定方法》（征求意见稿）不仅为App运营者自纠自查提供指引，还明确界定了App收集使用个人信息方面有哪些违法违规行为，帮助App经营者明确App评估和处置的标准和方法。全文的内容更加细化，针对App专项治理中的突出问题作出相应归纳。

草案采用列举方式呈现了三十余种App违法违规收集使用个人信息的类型。但值得注意的是，草案衔接了App个人信息保护违法违规类型与网络安全法、消费者权益保护法、广告法、电子商务法、民法典、刑法修正案等相关法律法规，即，草案回答了何种情形属于利用App违法违规行为的问题，而其他相关法律则回答的是违法违规或侵权者需要承担何种民事责任、行政责任或刑事责任的问题。

#### 起草背景

一、国际上，欧盟GDPR（《通用数据保护条例》）已经正式生效。其他国家如澳大利亚、新加坡、印度等国也出台对于个人信息保护的专门立法，个人信息保护立法在全球范围内均呈现趋严态势。

二、从国内立法来看，我国《网络安全法》已经实施一年有余。但该法中对于个人信息权利的规定仍过于抽象，难以落地，必须出台配套的法规规章帮助其实施。

三、移动互联网时代的到来一方面促进了算法科学、人工智能技术、云计算应用、人脸识别的发展，另一方面也带来精准诈骗、数据霸权、数据掠夺、网络攻击、数据安全等问题，保护个人信息与用户的合法权益迫在眉睫。

---

<sup>1</sup> app违法违规草案 直击隐私保护痛点，来源：光明日报。

## 草案重点

第一，强调收集和使用个人信息的**伦理责任**。该规定是为了回应 2012 年末全国人大常委会出台的《关于加强网络信息保护的決定》，将抽象的规定落实为类型化的实操规则。草案将个人信息保护伦理责任与具体网络实践相结合，规定了相应法律判断标准：如隐私政策的充分告知，收集信息类别、权限、目的、方式、范围的充分说明义务，敏感信息的特殊说明保护，隐私条款的文义简明要求等。

第二，释明个人信息收集使用中的“**合法性、正当性和必要性**”三个基本原则。并且，草案以三个原则为基础，做出了具体判断标准：首先，草案将违法违规收集使用个人信息的合法与非法标准做出规定，回应了“合法性”原则；其次，草案规定了“未经同意收集使用”的具体情形，这是对“正当性”的细化。草案将算法也纳入这一部分法律规制，**首次将算法写入了个人信息的立法之中**。最后，草案第四大类八条规定基本涵盖了 App 超越必要性原则违法违规行为的所有类别，包括**游客模式、技术迭代问题、一揽子授权、采集频率**等问题在本次草案中均有回应。

第三，**对大数据与个人信息的差别的本质进行了区分**，目前学界内的通说为，个人信息属于隐私保护的领域，而大数据属于知识产权的领域，因为两者的本质有着很大的区别，因此如果对两者的使用出现混淆，会使得个人隐私保护与产业发展产生冲突。

在民法总则草案刚刚出台时，就有学者指出，数据本身由于概念的范围太大，不仅包括大数据还包括个人信息，不能简单的把其看作是知识产权的客体。对于大数据来说，其无疑属于知识产权；然而对于个人信息来说，其更多应属于隐私法律体系的范畴。在各网络平台收集的数据中，不能够直接或者间接的识别到的个人信息**属于大数据，其所有权应该属于数据的处理者**，即网络平台。如果这些数据能够通过直接或者间接的方式识别到个人信息，这些信息即**属于个人信息，所有权属于用户**。

我国的法律法规中，目前没有具体规定大数据的范围。而个人信息的概念早在《网络安全法》中就已经有了相应的规定。除了个人信息，其他不能直接或间接识别到自然人身份的数据，大部分是属于大数据的范畴，即属于知识产权的领域。对于这一部分数据的所有权应当属于另一个法律的框架。

在草案的第五部分，将是否对收集的数据进行“匿名化”处理，作为判断数据的处分是否合规的重要标准，这样的规定也契合了大数据发展的整体方向。目前对于数据的匿名化处理在我国法律法规中有所规定，但具体的落实有很多的不同。**且对于已经进行了脱敏处理的数据，在实践中存在“可逆性”技术将其恢复，这一部分需要进一步的立法对其规范。**

然而，**及时对数据进行了匿名化的处理，也并不代表其与用户就没有关系**。根据市场监督管理总局发布的《网络交易管理办法》（征求意见稿）以及《电子商务法》的相关规定，网络经营者利用大数据向用户进行**精准营销或推送**，也有一定的限制，如**必须以显著的方式标记不针对个人特征的选项**。由此可以看出，即使大数据的所有权问题已经明确，但其使用也有一定的限制。

第四，明确了用户对其个人信息的**绝对控制权**。这主要体现在如下几个方面：

首先，确立了被遗忘权。欧盟通过 GDPR 与判例加强了用户对数据的被遗忘权的保护。此次草案要求网络运营者必须尊重用户注销帐号的权利，尊重用户更改和删除个人信息权利。对于很多很久不再使用的帐号，出现了很多有关的数据泄露问题，因此给予用户注销自己帐号的权利是个人信息保护的重要环节。

其次，明确了用户在开放平台中对自我的个人信息的控制权。在“新浪诉脉脉”案中确立的两次同意原则，此次草案再次对此强调，平台不能用一揽子的协议让用户打包同意。

再次，此次草案强调了用户对个人信息的自我决定权。草案的整体构建了用户对个人信息的自我决定权利，包括帐号注销、更正信息、处分权限、二次同意模式等权限。考虑到民法典人格权编的草案中已经对个人信息权进行了确立，其范围已经可以适用到 App 领域。此次草案将法律基础与技术发展进行了很好的融合。

最后，草案突出了对未成年人个人信息的保护。在欧盟发布的 GDPR 中规定，网络平台在处理 16 周岁以下儿童的数据时，需要事先征求其监护人的同意或授权。同时，GDPR 又给予了成员国根据自身情况调整此年龄的权利，但最低不得低于 13 岁。在这次草案中，将需要获取监护人授权的年龄规定在了 14 周岁，比较符合互联网发展的整体趋势和实践。

## 2. 等保 2.0 出台，网络安全将发生哪些变化<sup>2</sup>

### 出台背景

2019 年 5 月 13 日，网络安全等级保护制度 2.0 标准（以下简称“等保 2.0”）正式发布，2019 年 12 月 1 日开始实施。从 2008 年起，等保 1.0 标准发布，标志着我国进入“等保 1.0”时代。为适应新技术的发展，解决云计算、物联网、移动互联和工控领域信息系统的等级保护工作的需要，公安部牵头组织开展了信息技术新领域等级保护重点标准申报国家标准的工作，等级保护即将进入 2.0 时代。

### 主要变化

从 1.0 到 2.0，我国等级保护制度走过了十几年。等级保护 2.0 针对网络安全进行了一次重大升级。对于保护对象的范围，等保 2.0 在传统系统的基础上扩大了云计算、移动互联、物联网、大数据等对象，对等级保护制度提出了新的要求。其中，主要的变化体现在以下几个方面：

一、内涵更加丰富。与 1.0 相比，等保 2.0 标准内涵更加丰富，除进行 1.0 时代网络定级及备案审核、等级测评、安全建设整改、自查等规定动作外，还增加了测评活动安全管理、网络服务管理、产品服务采购使用管理、技术维护管理、监测预警和信息通报管理、数据和信息安全保护要求、应急处置要求等内容。

二、增加对场景的保护要求。相对 1.0，等保 2.0 标准有一个很大的变化，就是加入了对各种新场景的保护要求。例如，针对云计算的场景，提供防火墙服务的某公司就专门研发了安全 XSec 资源池的方案，目前资源池方案已经应用到十几个省市，通过把用户需要的各种功能进行细化，从而做到能够适应云计算环境下弹性扩展的要求。再通过和云平台厂商合作，或者使用某公司自身云计算产品，做到各个安全组件都能够统一编排，从而实现了安全服务化交互，而不是产品化交互。这是对于等保 2.0 要求的回应。

三、确立可信计算的重要技术地位。可信验证一级可基于可信根对设备的系统引导程序、系统程序等进行验证，并在检测到其可信性受到破坏后进行报警；可信验证四级可基于可信根对设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

四、明确态势感知要求。在等级保护 2.0 的安全框架当中，明确提出了要态势感知，而且

---

<sup>2</sup> 等保 2.0 出台，网络安全将发生哪些变化，来源：新华网。

在等保 2.0 标准当中也提出要具备对新型攻击分析的能力，要能够检测对重点节点及其入侵的行为，对各类安全事件进行识别报警和分析。

## 专家意见

近日，在网络安全等级保护制度 2.0 国家标准宣贯会上，公安部网络安全保卫局党委书记王璞玮认为，“网络安全等级保护制度 2.0 国家标准的发布，是具有里程碑意义的一件大事，标志着国家网络安全等级保护工作步入新时代。”

### 3. 《数据安全管理办法》征求意见 监管部门亮剑 App 收集隐私<sup>3</sup>

#### 出台背景

5月28日，国家互联网信息办公室会同相关部门研究起草了《数据安全管理办法（征求意见稿）》（以下简称《管理办法》），对网络运营者在数据收集、处理使用、安全监督管理三方面做出了具体要求。如今，大数据的发展让设备更智能化，但双刃剑的另一面则是个人隐私失去保护伞，《管理办法》的执行或许可以让用户获得部分选择权，但具体如何对非法收集数据的企业监督定责，则会是另一个实施难点。

#### 主要亮点

一、**严控收集**。“网络运营者通过网站、应用程序等产品收集使用个人信息，应当分别制定并公开收集使用规则。收集使用规则**应当明确具体、简单通俗、易于访问，突出网络运营者基本信息**等。”在《管理办法》中，公开是数据收集的主要关键词。

而在数据安全监督管理方面，《管理办法》则指出，发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，网络运营者应当立即采取补救措施，及时以电话、短信、邮件或信函等方式告知**个人信息主体**，并按要求**向行业主管监管部门和网信部门报告**。

二、**用户选择**。《管理办法》第二十三条拟规定，网络运营者利用用户数据和算法推送新闻信息、商业广告等（以下简称“定向推送”），应当以明显方式标明“**定推**”字样，为用户提供停止接收定向推送信息的功能；用户**选择停止**接收定向推送信息时，**应当停止推送，并删除**已经收集的设备识别码等用户数据和个人信息。

三、**数据安全责任人法定化**。此次意见稿中明确了设立数据安全责任人的要求及其职责范围。第二章第八条中规定，在收集使用规则中，应当提供网络运营者主要负责人、数据安全责任人的姓名及联系方式。第二章第十七条和第十八条提到，网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人。

四、首次对**爬虫**进行规定。意见稿第二章第十六条规定，网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量**超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止**。这是对爬虫技术的使用规范进行了首次规定。

---

<sup>3</sup> 《数据安全管理办法》征求意见 监管部门亮剑 App 收集隐私，来源：人民网。

## 专家意见

对于《管理办法》实施的难点，有关专家<sup>4</sup>认为，“在于监督和定责。在对网络运营者的监督中，全面和细致地监督到网络运营者在数据收集、处理使用的方方面面，在用户这端，若不建立统一的投诉平台，也很难解决用户举报难、投诉难、立案难的问题。在定责方面，网络运营者在数据安全方面若违反规定，如何视情况为其定责，关系到惩罚措施和力度的问题”。

---

<sup>4</sup> 艾媒咨询分析师李松霖

## 4. 《网络安全审查办法》公开征求意见，网络审查要求渐严<sup>5</sup>

### 出台背景

为提高关键信息基础设施安全可控水平，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同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、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合起草了《网络安全审查办法（征求意见稿）》，于2019年5月24日公开向社会征求意见。

### 审查对象

此次发布的征求意见稿重点强调了关键基础设施，要求运营者**采购网络产品和服务时预判风险，形成安全风险报告**。凡是会影响或可能影响国家安全的，都应当依照《网络安全审查办法》进行审查。

征求意见稿中，提出了四种需要申报并进行安全审查的情况：（一）关键信息基础设施整体停止运转或主要功能不能正常运行；（二）大量个人信息和重要数据泄露、丢失、毁损或出境；（三）关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁；（四）其他严重危害关键信息基础设施安全的风险隐患。

与2017年《网络产品和服务安全审查办法》中的规定相比，新办法的规定更偏向实务层面，操作性有所提升。

### 审查主体

根据征求意见稿，中央网络安全和信息化委员会统一领导网络安全审查工作。国家网信办会同其他11个联合起草单位，建立国家网络安全审查工作机制。

网络安全审查相关制度规定和工作程序的制定、网络安全审查的实施，则由网络安全审查办公室来具体执行。该办公室设在国家网信办。

根据《办法》，全部审查程序完成可能需要近两个月的时间。有专家指出，网络安全审查办公室与成员单位共同审查，体现了网络安全审查工作要引入各方专业意见，形成合力。不过，

---

<sup>5</sup> 国家网信办《网络安全审查办法》公开征求意见 增加特别审查程序，来源：南方都市报。

由于实际市场环境的复杂性，较长的审查周期会面临操作上的困难。

## 评估因素

与 2017 年的试行办法相比，征求意见稿还介绍了评估安全风险时主要的考虑因素。在“产品和服务的可控性、透明性以及供应链安全”这一条，征求意见稿明确，因为政治、外交、贸易等**非技术因素**导致产品和服务供应中断的可能性也将被纳入考虑。这意味着，今后的网络安全审查工作，将**不只是技术层面**的审查。

并且，征求意见稿第三条也出现新增表述，即“网络安全审查坚持防范网络安全风险与促进先进技术应用、增强公正透明与保护知识产权相统一”。意味着在当前贸易冲突背景下，我国依然坚持开放、公正的原则立场。

## 5. 日本拟修改《个人信息保护法》 新增企业停发广告义务<sup>6</sup>

### 修改情况

日本政府的个人信息保护委员会于4月25日发布了可能明年向国会提交的《个人信息保护法》**修正案的中期汇总**。从此次汇总的内容看，主要针对企业收集的地址和姓名等个人信息，对个人停止在广告中使用其个人信息的要求，企业有义务做出同意。在欧盟，为了保护处于弱势地位的普通用户，对**巨型IT企业**在个人数据的收集和使用上进行严格监管。日本政府也参照国际发展的整体趋势，对个人信息的保护展开了很多行动。

### 新法要点

在此次中期汇总的内容中，对IT企业收集个人信息规定，“关于停止利用，有必要探讨拓展个人权利范围的方法”。

对有关**删除在网上发布的以前的照片和犯罪历史的网络搜索结果**等的“被忘却的权利”，将继续讨论是否将其写入修正案。这个权利在欧洲已被确立。

对于企业将合法收集的用户个人信息用于发送广告和市场调查，当用户提出删除这部分数据请求时，**目前的实践中是由运营商自己决定的，而修正案中则规定企业应对其进行妥善应对**。

未来受到该法律监管的对象不仅是日本的企业，**对于像亚马逊和谷歌这样的巨型跨境IT企业也可能被包括在内**。目前日本政府还在对此机制进行讨论，将据点在海外的企业也纳入日本法律的监管体系。

---

<sup>6</sup> 日本拟修改〈个人信息保护法〉新增企业停发广告义务，来源：商务部官网。

## 二、监管动态

### 1. 多款 App 收集个人敏感信息 广东通信管理局依法查处涉事企业<sup>7</sup>

#### 行动概述

“3·15”前夕，广东省通信管理局（“广东省管局”）抽查了辖区内各大应用商店，重点排查收集用户信息的违规行为，发现违规 App20 个。广东省管局对涉事应用商店所属企业进行了约谈，包括广州优视网络科技有限公司（PP 助手）、广东太平洋互联网信息服务有限公司（太平洋电脑）等公司，并责令其下架违规 App。违规 App 目前已全部下架。同时，广东省管局对北京钰诚科技有限公司、陕西艺唐新文化传播有限公司、北京享宇金融服务外包有限公司、鼎盛鑫金融服务（深圳）有限公司等 App 运营企业给予了警告。

#### 抽查情况

本次发现的违规 App 多为贷款类，存在的主要问题有：一是注册时没有公示用户服务协议和隐私协议；二是隐私协议未明确收集哪些用户个人信息；三是隐私协议包含获取“用户的手机通讯运营商的服务密码、验证码”等；四是未提供注销功能；五是存在静默下载的问题，使用过程中在用户不知情时下载其他应用软件并消耗用户流量；六是存在积分墙的限制，即在安装运行后无法使用并要求下载其他应用软件。

#### 监管方向

下一步，广东省管局将严格落实《网络安全法》、《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号）中关于用户信息保护的规定，依法依规严厉查处涉事企业，并将违规企业纳入电信业务经营不良名单。

---

<sup>7</sup> 多款 App 收集个人敏感信息 广东通信管理局依法查处涉事企业，来源：工信部官网。

## 三、相关案例

### 1. 高通近 40 款芯片被曝出泄密漏洞！波及数十亿部手机<sup>8</sup>

#### 事件情况

据 EETOP 论坛 27 日报道，英国安全业者 NCC Group 公布了藏匿在超过 40 款高通芯片的旁路漏洞，可用来窃取芯片内所储存的机密信息，该漏洞还涉及采用相关芯片的 Android 装置。NCC Group 早在去年就发现了这一漏洞，并于去年 3 月通知高通，高通则一直到今年 4 月才开始正式修补。

该漏洞编号为 CVE-2018-11976，涉及高通芯片安全执行环境（Qualcomm Secure Execution Environment, QSEE）的椭圆曲线数码签章算法（Elliptic Curve Digital Signature Algorithm, ECDSA），将允许黑客推测出存放在 QSEE 中、以 ECDSA 加密的 224 位与 256 位的金钥。

根据高通所张贴的安全公告，CVE-2018-11976 属于 ECDSA 签章代码的加密问题，将会让存放在安全区域的私钥外泄至一般区域。它被高通列为重大漏洞，而且影响超过 40 款的高通芯片，可能波及数十亿台的 Android 手机及设备。

#### 专家意见

NCC Group 资深安全顾问 Keegan Ryan 指出，诸如 TrustZone 或 QSEE 等安全执行环境设计，受到许多行动装置与嵌入式装置的广泛采用。虽然安全区域与一般区域使用的是不同的硬件资源、软件或资料，但它们依然以同样的微架构为基础。于是他们打造了一些工具来监控 QSEE 的资料流与程序流，并找出高通导入 ECDSA 的安全漏洞，成功地在高通芯片上恢复了 256 位的加密私钥。

Ryan 解释，大多数的 ECDSA 签章都在处理随机数值的乘法回圈，假设黑客能够恢复这个随机数值的少数位，就能利用既有的技术来恢复完整的私钥。虽然这两个区域都含有对抗旁路攻击的机制，但他们发现有两个区域可外泄该随机数值的资讯，并绕过了这些限制，找出了该数值的部份位，最终成功恢复了 Nexus 5X 手机上所存放的 256 位私钥。

---

<sup>8</sup> 贸易战促使中国押后宣布限制数据出境的规定，来源公众号：享法互联网 JoyLegal。

## 2. 信托公司遭罚：违法查询个人信息和企业信贷信息<sup>9</sup>

### 处罚情况

某信托公司近日遭中国人民银行处罚，处罚原因是**违法查询个人信息和企业信贷信息等**。4月22日，中国人民银行武汉分行网站公布了行政处罚信息公示表（武银罚字〔2019〕第14号），该信托公司未经同意查询个人信息和企业的信贷信息，被中国人民银行武汉分行处罚款人民币29万元。

### 公示信息

#### 行政处罚信息公示表

报送单位：（盖章）中国人民银行武汉分行      报送时间：2019-4-19

序号	企业名称	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期
1	信托有限公司	武银罚字〔2019〕第14号	未经同意查询个人信息和企业的信贷信息	处罚款人民币29万元	中国人民银行武汉分行	2019年4月10日

图片来源于网络，图片来源于网络

<sup>9</sup> 某国际信托遭罚：违法查询个人信息和企业信贷信息，来源：上海信托网。

### 3. 广东侦破一批涉个人信息网络违法犯罪案件 抓获万余名嫌疑人<sup>10</sup>

#### 行动概况

广东省公安厅发布消息称，今年1至4月，“净网2019”专项行动中，广东警方共侦破各类涉网案件6300余宗，抓获犯罪嫌疑人1.5万余名，摧毁多个侵犯公民个人信息、网络诈骗等网络违法犯罪团伙窝点。公安机关先后破获佛山特大网络交友诈骗案、梅州张某丰等人侵犯公民个人信息案、惠州“2·19”投资诈骗案等涉网案件，一举摧毁上述网络违法犯罪团伙。

#### 侦查案例

广东梅州警方1月份查获一个出售公民个人信息的犯罪团伙，该团伙从2018年开始，通过淘宝店铺、QQ空间、微信朋友圈等多个平台发布售卖微信号、QQ号、身份证、银行卡的推广信息，并进行交易。办案民警称，一套身份证和银行卡信息价值900元，一个旧微信号价值65元。期间，该团伙共卖出微信号500余个，QQ号100余个，身份证银行卡10余套。

今年2月，惠州警方查处一个犯罪团伙。其利用社交软件广泛交友，以投资证券软件形式实施网络诈骗。该团伙从网络上购买大量股民QQ号，并添加好友，冒充资深炒股专家进行接触，一旦认定属于“优质”对象，就拉其进诈骗群，诱导其下载非法第三方软件进行投资，通过操控软件骗取受害人巨额财富。

#### 专家意见

广东省公安厅网警总队总队长李正祥表示，当前网络违法犯罪总体呈现出两种特点。其一，侵犯公民个人信息仍处于高度活跃期。其二，依托公民个人信息实施的网络诈骗层出不穷，主要类型有网络交友诈骗、网络投资诈骗等方面。

李正祥表示，下一步，广东警方将继续加大对各类网络违法犯罪的打击力度，进一步督促各行业部门加强安全管理，防止内部人员泄露公民个人信息。同时，进一步加强防范宣传，提高群众网络反诈骗意识，营造清朗干净的网络空间。

---

<sup>10</sup> 广东侦破一批涉个人信息网络违法犯罪案件 抓获万余名嫌疑人，来源：国家互联网信息办公室官网。

## 4. 大连警方破获侵犯公民个人信息案 查获个人信息近亿条<sup>11</sup>

### 侦查情况

5月8日，大连市公安局金州分局网安大队公布消息称，近日通过网络巡查发现，一名男子有侵犯公民个人信息的嫌疑。通过进一步工作发现，该男子有网络攻防能力，并具有非法获取公民信息的重大嫌疑。经缜密部署，该分局网安大队联合属地派出所在其藏匿的某小区家中将嫌疑人肖某成功抓获。

### 案件事实

办案民警在嫌疑人的笔记本电脑、网盘中发现了大量公民信息，这些信息包括某交友网站数据 2500 万条、某知名论坛数据 4000 万条、某手机网站信息 26 万条，还含有 225 万条的某航空公司信息和 6400 条的某地人口信息。这些数据中包含用户姓名、住址、账号和密码等信息。同时，肖某还利用搜索引擎从网上搜索并下载了数千万条公民个人信息。

警方经审讯得知，嫌疑人肖某使用计算机技术发现网站漏洞并攻入多个企业网络以及社交平台的服务器，非法获取公民个人信息近亿条。这些信息一旦公开，将会对公民人身财产安全造成巨大威胁。此案的破获，及时制止了信息泄露，保护了人民财产安全。

### 案件动态

目前，犯罪嫌疑人已被警方依法刑事拘留。

---

<sup>11</sup> 大连警方破获一起侵犯公民个人信息案 查获个人信息近亿条，来源：新华社。

## 四、环球解读

### 1. 网信办送“儿童节礼物”：拟新规强化儿童信息保护

#### 草案概况<sup>12</sup>

2019年5月31日，国家互联网信息办公室发布关于《儿童个人信息网络保护规定（征求意见稿）》公开征求意见的通知。通知称，为了规范收集使用儿童个人信息等行为，保护儿童合法权益，为儿童健康成长创造良好的网上环境，起草了《儿童个人信息网络保护规定（征求意见稿）》（简称“《征求意见稿》”），5月31日起向社会公开征求意见，为期1个月。

意见稿拟要求，网络运营者不得收集与其提供的服务无关的儿童个人信息，不得违反法律、行政法规的规定和用户协议的约定收集儿童个人信息。网络运营者收集、使用儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的明示同意。明示同意应当具体、清楚、明确，基于自愿。网络运营者使用儿童个人信息，不得超出约定的目的和范围。

意见稿拟要求，网络运营者对其工作人员应以最小授权为原则，严格设定信息访问权限，控制儿童个人信息知悉范围。工作人员访问儿童个人信息的，应当经过个人信息保护专员或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载儿童个人信息。网络运营者不得披露儿童个人信息。儿童或者其监护人要求网络运营者删除其收集、存储、使用的儿童个人信息的，网络运营者应当及时采取措施予以删除。

意见稿还提出，网络运营者发现儿童个人信息发生或者可能发生泄露、毁损、丢失的，应立即启动应急预案，采取补救措施；造成或者可能造成严重后果的，应立即向有关主管部门报告，并将事件相关情况告知受影响的儿童及其监护人，难以逐一告知的，应当采取合理、有效的方式发布相关警示信息。

意见稿拟规定，网络运营者收集、使用、转移、披露儿童个人信息，为维护国家安全或者公共利益；为消除儿童人身或者财产上的紧急危险；法律、行政法规规定的其他情形，可以不经儿童监护人的明示同意。

违反本规定的，根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

违反本规定被追究法律责任的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

---

<sup>12</sup> 网信办拟规定 保护儿童信息，来源：新京报

## 环球解读<sup>13</sup>

### 1. 保护对象的年龄线设置

我国法律法规及国标对处于不同年龄阶段的未成年人规定了不同的权利，可以分为以下两个角度讨论：

第一，从民事主体的角度，根据《中华人民共和国民法总则》第十七条“十八周岁以下的自然人均为未成年人，除特殊情况<sup>14</sup>外，均属于限制民事行为能力人，只能实施与其智力、精神状况相适应的民事法律行为。否则，需要由其法定代理人代理或者经其法定代理人同意、追认”。

第二，从个人信息主体的角度，根据《国标》第 5.5 条第 c) 款“收集年满 14 的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意。”本次《征求意见稿》所保护的主体仅为儿童，根据征求意见稿第二十七条的规定，儿童指不满十四周岁的未成年人。《数据安全管理办法（征求意见稿）》第 12 条也规定“收集 14 周岁以下未成年人个人信息的，应当征得其监护人同意”，将保护的个人信息主体也定为 14 周岁以下的儿童。

### 2. 保护儿童个人信息的全生命周期

此次《征求意见稿》沿用了《国标》的基本框架，参考了保护个人信息全生命周期的思路，对儿童个人信息的收集、存储、使用、转移、披露均有完整的覆盖（第三条）。并且，在收集信息前要求获得监护人的明示同意，在收集后监护人有权要求删除或更正。

第一，在信息收集、使用方面，《征求意见稿》明确了需要得到儿童监护人的明示同意，并且要求明示同意应当具体、清楚、明确和基于自愿（第七条）。此外，第十一条、第十四条和第十五条中，全方位详细规定了需要征得明示同意的各种情形，比如收集信息的目的、范围、方式、期限等发生变化，和第三方共用、向第三方转移时均需要获得监护人的明示同意。第八条还进一步要求在提供同意选项的同时，还需要向儿童监护人提供拒绝选项（第八条），这些都与《国标》是一脉相承的。需要注意的是，根据《征求意见稿》，收集、使用儿童个人信息，需要得到的是监护人的“明示”同意。但《数据安全管理办法（征求意见稿）》第十二条，收集 14 周岁以下未成年人个人信息的，应当征得其监护人同意，可能包括明示和默示同意两种情形。根据《国标》，明示同意是指个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”、主动填写或提供等。因此，有待于不同法规之间的相互统一与协调适用。

第二，在信息存储、委托处理方面，与《国标》的相关规定没有实质性区别，同样要求不得超过实现收集、使用目的所必须的期限（第九条）。同时，明确要求采取加密措施存储（第

---

<sup>13</sup> 作者：孟洁

<sup>14</sup> 第十八条 十六周岁以上的未成年人，以自己的劳动收入为主要生活来源的，视为完全民事行为能力人。

十条)，这条是对儿童信息的增强性保护措施的特殊规定。涉及儿童信息委托处理时，网络运营者需要进行安全评估。受托方的义务基本与《国标》规定保持一致，不得进行受托范围以外的处理（第十三条）。相较于《国标》，《征求意见稿》严格要求网络运营者与受托方应当签署委托协议来明确双方责任、处理事项、处理期限、处理性质和目的。并且在受委托方的义务中，增加了其协助网络运营者回应儿童监护人提出的申请，以及不得转委托的规定。

第三，个人信息主体权利实现方面，明确要求网络运营者对错误的儿童信息进行更正（第十七条）；对于删除儿童个人信息，相较于《国标》，《征求意见稿》增加了当出现儿童监护人撤回同意，以及儿童或者其监护人通过注销等方式终止使用产品或者服务两种情形时，网络运营者应当及时采取措施予以删除。

### 3. 保护儿童个人信息的行业规则

《征求意见稿》强调了网络运营者的行业规范，比如要求网络运营者应当设置专门的儿童个人信息保护规则和用户协议，设立专人负责儿童信息保护（第五条）；工作人员访问儿童个人信息的，应当以“最小授权”为原则，设定严格的访问权限，需要经过个人信息保护专员或者其授权的管理人员审批（第十二条）。

网络运营者是否需要单独写一个针对儿童信息保护的隐私政策，还是用户协议里包含儿童信息保护的规则，目前在《征求意见稿》阶段还没有统一答案。但可能一般认为，专注于儿童内容和产品的运营者，需要设有专门针对儿童的隐私政策。但老少兼宜的产品或者服务，专门设计单独的儿童隐私政策成本较高也会造成用户多套版本查看的混乱，可以在总的用户协议中特别列出针对儿童规则这种方式来解决。

根据《国标》，儿童个人信息也是个人敏感信息的一类，一般企业要求敏感信息的审批也应当经过个人信息保护专员或者其授权的管理人员，记录访问情况，并采取技术措施，避免违法复制和下载。

### 4. 违法处理儿童个人信息的处罚

此次《征求意见稿》对侵犯儿童个人信息安全规定了惩罚措施，可以算作是一大亮点。

根据《征求意见稿》，违反相关规定，网信办会根据情节轻重，采取约谈或者根据《中华人民共和国网络安全法》第六十四条根据情节单对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

《征求意见稿》的惩罚措施是对《国标》推荐性标准没有强制执行力的有利补充，对企业有很强的震慑力。

中国首家律师事务所

中国首家律师事务所