国盟信息安全通报

2021 年 01 月 17 日第 232 期

全国售后服务中心

国盟信息安全通报

（第 232 期）

国际信息安全学习联盟

2021 年 1 月 17 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 268，其中高危漏洞 90 个、中危漏洞 140 个、低危漏洞 38 个。漏洞平均分值为 5.74。本周收录的漏洞中，涉及 0day 漏洞 136 个（占 51%），其中互联网上出现“Egavilan Media UnderOnstruction Page With Cpanel SQL 注入漏洞、Online Marriage Registration System SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3992 个，与上周（6932 个）环比减少 42%。

主要内容

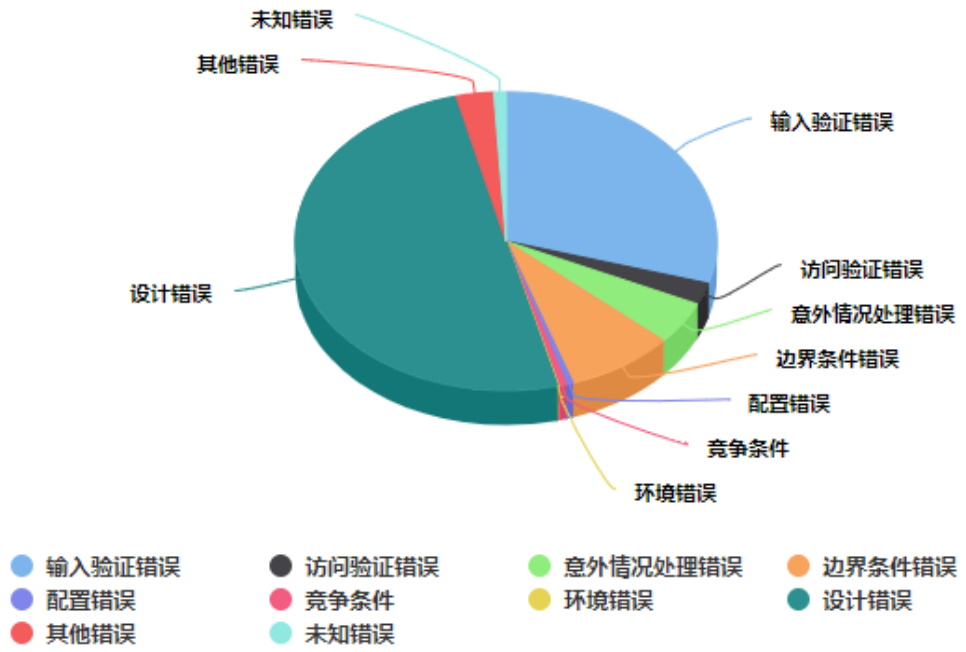
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

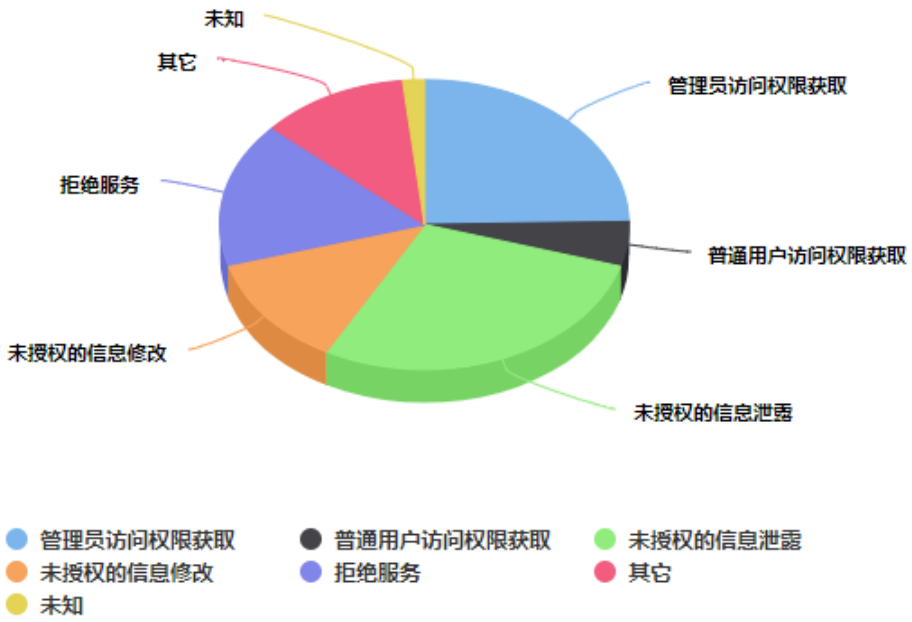
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 268，其中高危漏洞 90 个、中危漏洞 140 个、低危漏洞 38 个。漏洞平均分值为 5.74。本周收录的漏洞中，涉及 0day 漏洞 136 个（占 51%），其中互联网上出现“Egavilan Media UnderOnstruction Page With Cpanel SQL 注入漏洞、Online Marriage Registration System SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3992 个，与上周（6932 个）环比减少 42%。

二、安全漏洞增长数量及种类分布情况

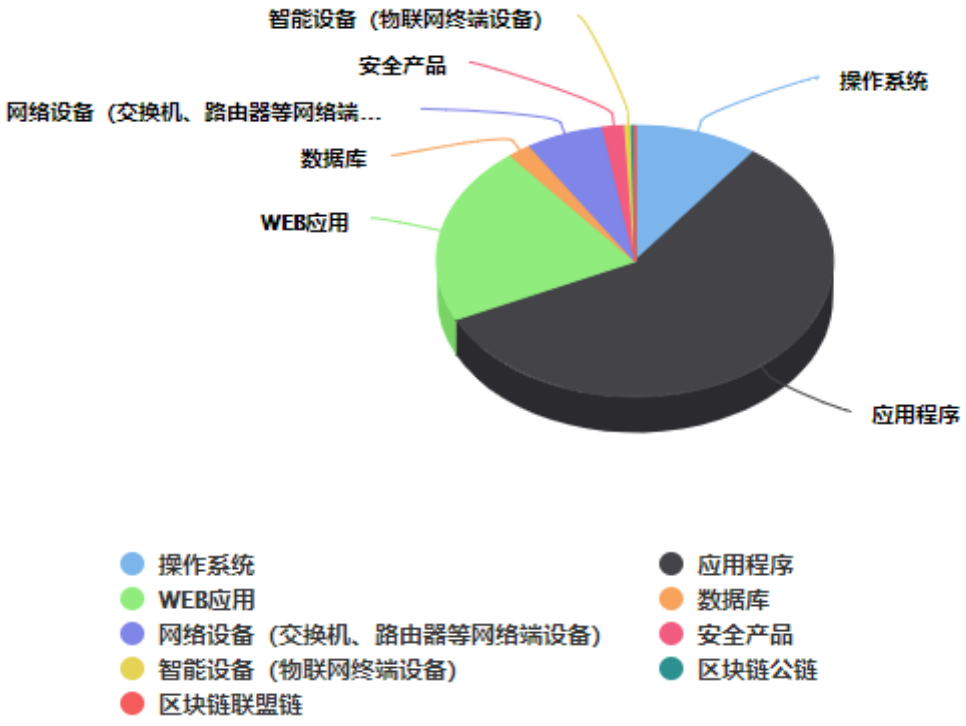
➢ 漏洞产生原因（2021 年 1 月 01 日—2021 年 1 月 17）



➢ 漏洞引发的威胁（2021 年 1 月 01 日—2021 年 1 月 17）



➢ 漏洞影响对象类型（2021 年 1 月 01 日—2021 年 1 月 17）



三、安全产业动态

➢ 统筹发展和安全 筑牢国家安全屏障

习近平总书记在中央政治局第二十六次集体学习时强调，做好新时代国家安全工作，要坚持总体国家安全观，抓住和用好我国发展的重要战略机遇期，把国家安全贯穿到党和国家工作各方面全过程，同经济社会发展一起谋划、一起部署。习近平总书记就贯彻总体国家安全观提出 10 点要求，其中一点就是坚持统筹发展和安全。这是继党的十九届五中全会把统筹发展和安全纳入“十四五”时期我国经济社会发展指导思想之后，以习近平同志为核心的党中央对统筹发展和安全再次作出重要部署。我们要深入学习领会习近平总书记关于统筹发展和安全的重要论述，推动相关重要战略部署落实落地，有效防范化解各类风险挑战，筑牢国家安全屏障，确保社会主义现代化事业顺利推进。

统筹发展和安全具有重大理论和现实意义

以习近平同志为核心的党中央高度重视统筹发展和安全。统筹发展和安全是对历史上大国兴衰经验的深刻总结，是对新中国成立 70 多年来推进社会主义现代化建设经验的深刻总结，是对发展和安全辩证统一关系的深刻认识和把握，是着眼于在不稳定不确定发展环境中更好推进中华民族伟大复兴的重要战略部署，具有深刻理论逻辑、历史逻辑和重大现实意义。

贯彻总体国家安全观的重要要求。2014 年，习近平总书记创造性地提出总体国家安全观。坚持总体国家安全观是习近平新时代中国特色社会主义思想的重要组成部分，是新时代

坚持和发展中国特色社会主义的基本方略之一。6 年多来，我们在维护国家安全、防范风险挑战方面的一系列成功实践，充分彰显了总体国家安全观的理论力量和实践品格。统筹发展和安全，是贯彻总体国家安全观的重要要求。习近平总书记强调，安全是发展的前提，发展是安全的保障，进一步阐明了两者的辩证统一关系。发展是我们党执政兴国的第一要务，是解决中国一切问题的关键。没有经济社会发展，就不可能实现国家长治久安、社会安定有序、人民安居乐业。国家安全是国家生存发展的基本前提，是安邦定国的重要基石。没有国家安全，就不可能实现经济社会可持续发展，已经取得的成果也会失去。事实证明，发展和安全相辅相成、不可偏废，统一于坚持和发展中国特色社会主义的伟大实践。

对历史经验的深刻总结。历史反复证明，能否统筹好发展和安全，关系国家兴衰、历史走向。纵览中国历代政治得失，封建王朝的衰亡大多与发展和安全摆布失据有关。纵览世界大国兴衰历史，大国兴起时，往往能够较好地统筹发展和安全，而衰落则与没有统筹好发展和安全密切相关。没有发展作为支撑的安全，必然难以长久；没有安全作为保障的发展，必然不可持续。发展和安全合则兴、离则弱、悖则亡，这是历史留给我们的深刻启示。

实现中华民族伟大复兴的必然要求。新中国成立后，我们党对发展和安全高度重视，始终把维护国家安全工作紧紧抓在手上，在不同历史时期对统筹发展和安全作出正确战略决策，中华民族迎来了从站起来、富起来到强起来的伟大飞跃。新中国成立之初，国内形势与国际环境错综复杂。我们党以“打得一拳开，免得百拳来”的气魄作出抗美援朝、保家卫国的历史性决策，粉碎了侵略者将新中国扼杀在摇篮中的图谋。改革开放以来，我们党作出和平与发展是时代主题的科学判断，积极营造良好发展环境，抓住机遇加快发展，经济社会发展取得巨大成就。党的十八大以来，以习近平同志为核心的党中央加强对国家安全工作的集中统一领导，从全局和战略高度对国家安全作出一系列重大决策部署，强化国家安全工作顶层设计，完善各重要领域国家安全政策，健全国家安全法律法规，有效应对了一系列重大风险挑战，保持了我国国家安全大局稳定。当今世界正经历百年未有之大变局，我国正处于实现中华民族伟大复兴的关键时期。和平与发展仍是当今时代主题，但不稳定不确定因素增多，我们面临的风险挑战愈加复杂。这些风险挑战是我国由大向强发展进程中无法回避的，是实现中华民族伟大复兴绕不过的门槛。我们要认清我国发展所处的历史方位、国家安全面临的形势任务，更好统筹发展和安全各项工作。

牢牢掌握国家安全工作主动权

统筹发展和安全，既是重大理论问题，也是重要实践要求。要坚持总体国家安全观，维护和塑造国家安全，统筹传统安全和非传统安全，把国家安全贯穿到党和国家工作各领域全

过程，防范和化解影响我国现代化进程的各种风险。

在发展中保安全、在安全中促发展。发展和安全，犹如车之两轮、鸟之两翼，任何一方面有明显短板，都会影响中华民族伟大复兴进程。在全面建设社会主义现代化国家新征程上统筹发展和安全，既要求通过发展提升国家安全实力，又要求深入推进国家安全思路、体制、手段创新，营造有利于经济社会发展的安全环境，在发展中更多考虑安全因素，努力形成在发展中保安全、在安全中促发展的格局，实现更高质量、更有效率、更加公平、更可持续、更为安全的发展。我们要贯彻落实习近平总书记关于统筹发展和安全的重要论述，加强战略性、系统性、前瞻性研究谋划，深入思考今后一个时期我国经济社会发展存在哪些重大风险，深入思考防范化解重大安全风险的思路举措，深入思考如何把国家安全工作融入国家发展各领域全过程，牢牢掌握国家安全工作主动权。

维护和塑造国家安全。维护国家安全和塑造国家安全是统一的，塑造是更高层次、更具前瞻性的维护。随着我国日益走近世界舞台中央，我们要在变局中把握规律、在乱局中趋利避害、在斗争中争取主动，切实维护我国主权、安全、发展利益。塑造国家安全，不是要走国强必霸之路，而是坚定不移走和平发展道路，目的是为了实现中华民族伟大复兴；不是对现有国际秩序推倒重来、另起炉灶，而是在维护以联合国宪章宗旨和原则为核心的国际秩序基础上，与世界各国一起与时俱进完善全球治理体制机制；不是要零和博弈，而是要合作共赢、互惠互利，坚持多边主义和国际关系民主化，推动构建人类命运共同体。任何国家都没有包揽国际事务、主宰他国命运、垄断发展优势的权力，更不能在世界上搞霸权、霸凌、霸道。面对前进道路上的各种风险挑战，我们将以坚强决心、坚定意志、坚实国力为依托，统筹运用维护国家安全和塑造国家安全“两手”，不断增强塑造国家安全态势的能力。

统筹传统安全和非传统安全。当前，我国国家安全的内涵和外延比历史上任何时候都要丰富，时空领域比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂。总的看，政治、国土、军事安全仍然是国家安全的重中之重，任何时候都必须抓住不放。同时，在中国这样一个快速发展的国家，我们面临的非传统安全威胁越来越多，需要统筹兼顾、综合施策。突如其来的新冠肺炎疫情，是对我国应对非传统安全威胁能力的一次考验。在以习近平同志为核心的党中央坚强领导下，我们取得抗击新冠肺炎疫情斗争重大战略成果。当前和今后一个时期是我国各类矛盾和风险易发期，各种可以预见和难以预见的风险因素明显增多。党的十九届五中全会对应对经济、金融、网络、粮食、能源、生态、核、生物、海外利益等安全问题作出全面部署。我们要认真贯彻落实这些重要部署，深入掌握各类危害国家安全的新行为新动向，积极推进非传统安全领域国家安全立法，加强风险预警、防控机制和能力建

设，全面应对各领域安全风险和挑战。

汇聚维护国家安全的强大合力

维护好国家安全，是全党全社会的共同责任。我们要以习近平新时代中国特色社会主义思想特别是总体国家安全观为指导，充分发挥中国共产党领导的政治优势和中国特色社会主义的制度优势，汇聚起维护国家安全的强大合力。

坚持党对国家安全工作的绝对领导。“十三五”时期，党和国家走过了一段极不平凡的历程。以习近平同志为核心的党中央科学研判时与势，辩证把握机与危，坚持统筹发展和安全，打赢了一场又一场硬仗，抵御了一个又一个风险，不断取得新胜利。实践充分证明，办好中国的事情关键在党。新征程上，我们要办好发展安全两件大事，谱写经济快速发展、社会长期稳定“两大奇迹”新篇章，最根本的是要坚持党对发展和安全工作的全面领导，增强“四个意识”、坚定“四个自信”、做到“两个维护”。有以习近平同志为核心的党中央领航掌舵，有习近平新时代中国特色社会主义思想的科学指引，我们一定能够战胜各种风险挑战，将中国特色社会主义事业不断推向前进。

推进国家安全体系和能力现代化。党的十九届五中全会对“加强国家安全体系和能力建设”作出战略部署，为构建现代化国家安全体系和能力指明了方向。下一阶段，我们要进一步强化党对国家安全工作的领导，完善集中统一、高效权威的国家安全领导体制，健全国家安全法治体系、战略体系、政策体系、人才体系和运行机制，完善重要领域国家安全立法、制度、政策，健全国家安全审查和监管制度，加强国家安全执法，推动国家安全体系和能力同国家现代化进程相适应。

落实国家安全责任。坚持全国一盘棋，调动各方面积极性，集中力量办大事，是中国特色社会主义制度的显著优势之一，也是维护国家安全的重要基础。国家安全风险来自各个方面，化解风险要充分调动各方面积极性，打造人人有责、人人尽责的工作新局面。严格落实《党委（党组）国家安全责任制规定》，形成一级抓一级、层层抓落实的工作格局，确保党中央关于国家安全工作的决策部署落到实处。加强国家安全宣传教育，教育引导广大人民群众增强国家安全意识，巩固国家安全人民防线。

发挥专门机关作用。贯彻落实总体国家安全观，护航中华民族伟大复兴，是国家安全机关的重大政治责任。面对前进道路上的风险考验甚至惊涛骇浪，国家安全机关既要有敢于斗争的勇气，更要有善于斗争的本领。我们要充分发挥专门机关作用，依法防范、制止、打击危害我国国家安全的各类违法犯罪活动，加强国家安全干部队伍建设，打造坚不可摧的国家安全干部队伍，筑牢国家安全屏障。（来源：人民日报 作者：国家安全部党委书记、部长 陈文清）

➢ 以人民为中心 保护个人信息

个人信息直接关系人民群众隐私、财产和生命安全，也事关社会稳定、事关国家安全。加强个人信息保护，既是贯彻以人民为中心发展思想的具体体现，也是网络治理法治化的必然要求，还是实现人民美好网络生活的重要保障。加强个人信息保护，需要处理好三对关系。

保护个人信息要处理好安全与发展的辩证关系。从个人信息保护角度来看，安全是指个人隐私安全和数据安全，发展是指数据流通共享促进数字经济发展。个人信息包括个人隐私等敏感信息和非敏感个人信息。个人隐私等敏感信息需要严格保护。当然，部分信息经过数据脱敏等程序后，可与非敏感个人信息一起流通共享，这是发展数字经济的重要资源。一方面，安全是实现数字经济发展的前提和基础。保护个人隐私等敏感信息是释放数据红利的先决条件。“经济社会发展的每一个项目、每一个环节都要以安全为前提，不能有丝毫疏漏。”个人信息保护法草案进一步贯彻宪法和民法典的要求，保护公民的信息权利，平衡配置第三方收集和使用个人信息的权利与义务，有助于有效保护个人信息安全，同时也为数据的流通共享提供法理基础和法律边界，有助于为数字经济发展营造安全环境。另一方面，发展必须以维护安全为目的。数据是数字经济发展的源动力，是提升数字社会治理效能的基础要素。个人信息同时具有经济和社会属性，要坚持“在保护中利用、在利用时保护”。数据流通共享是为了推动经济和社会进步，进而更好地维护人民生命财产安全和个人隐私。在抗击新冠肺炎疫情中，中国依靠大数据溯源确诊病例的行动轨迹，让遏制疫情跑出“加速度”，有效维护了人民的生命安全。

保护个人信息要处理好多主体的关系，形成合力。习近平总书记指出：“要提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局”。一方面，要明确主体责任，各尽其责。必须坚持在党的领导下做好个人信息保护与利用的顶层设计，推动各方履行责任。政府要依法行政，加强管理，通过行政执法等方式化解冲突与矛盾。企业和社会组织等要贯彻有关的法律法规，进一步将法律法规的要求转化为本单位的内部规章制度，扎紧个人信息保护的藩篱，做好个人信息的储存、保密工作，合法合理使用数据信息推动数字化经济发展。网民也要发挥主体作用，加强个人信息保护意识，保护好自身的个人信息，防患于未然。另一方面，要形成以党政部门为核心的各主体协同合力。由于涉及主体过多，个人信息保护容易发生“九龙治水”的状况。因此，必须坚持党的领导，确保个人信息保护的正确方向，推动保障个人隐私、保障数据流通的社会效益和经济效益三方的统一。国家通过立法、执法、司法等活动加强对个人信息的管理，提高违法行为打击力度，依法严厉打击个人信息泄露、大数据杀熟等行为，推动各网络主体严格守法。在此基础上，各网络主体基于法治，形成以党政部门为核心，以法律法规为基础的协同治理格局，共同发力保护个人信息。

保护个人信息要处理好德治与法治的互补关系。德治和法治是个人信息保护的两种基本途径。法律是成文的道德，道德是内心的法律。一方面，德润人心，可以增强个人信息保护的道德底蕴。随着数字经济突飞猛进，个人信息保护领域新情况新问题层出不穷。但法律具有一定滞后性，在法律所不及的地方，需要道德发挥作用。心中的道德律，使人从内心认知到“应当怎么做”，使人们坚持道德底线，规范网络行为，增强个人信息保护的人文关怀，引领网络主体向上向善，使个人信息保护的关口前移。另一方面，法安天下，可以有力规范个人信息保护的行为。法律以既成的法条要求网络主体“必须怎么做”，是行为的戒度尺，设立了个人信息使用的界限、方式，震慑并纠正违法行为，强制而有力地维护着个人信息安全。除了国家层面的“硬法”，行业和企业制定的规章制度等“软法”，也是个人信息保护规范体系的重要组成部分。“没有规矩不成方圆”，通过严密的个人信息保护规范体系筑牢个人信息保护的法治屏障。（来源：广州日报）

➢ 《民法典》对公民个人信息全生命周期风险防范的意义

破解新时代公民个人信息保护难题，需要从根本上运用法治思维和法治方式，构建全生

命周期的法律法规体系和执法司法机制。2020 年颁布实施的《民法典》“人格权编”，专门设立第六章“隐私权和个人信息保护”，对公民个人信息保护做出总体性规定，为化解个人信息数据侵害风险提供了事前预防、事中控制、事后救济的系统性解决方案。

一、事前预防：保障数据安全降低个人信息泄露风险

隐私权是《中华人民共和国宪法》保护的重要人格权利。其第 38 条、第 40 条明确规定：“中华人民共和国公民的人格尊严不受侵犯”“公民的通信自由和通信秘密受法律的保护”。

大数据时代，公民个人信息安全风险显著增加。因此，《民法典》对隐私权进行了更详尽的规定和解释，第 1032 条明确规定“自然人享有隐私权”，且“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”。在网络空间，国家公权力领域、公共领域、私人领域高度叠加，“公共领域私人化”和“私人领域公共化”的公私领域相互融合，公民的私密空间、私密活动、私密信息被侵犯的风险显著增高。甚至有人戏称，在大数据时代，每个网民都在互联网上“裸奔”，公民的私人网络生活安宁和幸福感、安全感受到严重影响。

在风险社会，法益保护前置是有效应对网络犯罪和违法行为的方式。应当说明的是，法益保护前置不仅仅是刑事法益保护前置，通过刑事立法采用“抽象危险犯”的方式惩治犯罪，也包括民事法益保护前置和行政法益保护前置。特别是网络信息传播类违法违规现象，由于移动互联网的高传播速度和裂变式传播特征，一旦个人信息泄露，控制二次传播和消除负面影响的难度激增，因此，非常有必要在审慎稳妥的前提下将法律保护的关口前置。

《民法典》第 127 条规定：“法律对数据、网络虚拟财产的保护有规定的，依照其规定。”因此，建议将数据安全保护作为公民个人信息安全的前置环节，主要有三方面理由。

其一，数据是公民个人信息的主要载体。为防止对数据保护的专门性法律处于真空状态，2020 年 7 月，《中华人民共和国数据安全法（草案）》（以下简称“《数据安全法（草案）》”）发布，其中，第 3 条第 1 款明确规定“数据，是指任何以电子或者非电子形式对信息的记录”，以法律的形式明确了数据和信息的关系。从某种角度讲，对含有个人信息的数据进行有效保护，是个人信息保护的必要条件，有利于大幅降低公民个人信息泄露风险。

其二，数据安全是一种可持续的安全状态。数据安全并不是静态意义的安全，而是动态的全生命周期的安全。《数据安全法（草案）》第 3 条第 3 款规定：“数据安全，是指通过采取必要措施，保障数据得到有效保护和合法利用，并持续处于安全状态的能力。”如果承载公民个人信息的数据安全得到有效保护和合法利用，就可以将个人信息泄露规模从群体性泄露，控制并限制在个体性影响范围，最大程度减少信息泄露危害。

其三，数据安全更有利于压实网络服务商的责任。相比信息安全的个性化保护，数据安全提供了一种普遍性的法律约束。《数据安全法（草案）》第四章明确规定了“数据安全保护义务”，其中，第 25 条规定：“开展数据活动应当依照法律、行政法规的规定和国家标准的强制性要求，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。”对于重要数据的处理，更要“设立数据安全负责人和管理机构，落实数据安全保护责任”。

二、事中控制：个人信息处理应得到全方位保护

数据安全保护可以化解和降低大部分个人信息泄露风险，但是，数据的收集、存储、流转、加工是发展 IT 产业特别是大数据产业的必经环节，在此过程中，仍然无法避免个人信息不当使用。

《民法典》和《中华人民共和国个人信息保护法（草案）》进一步强化了个人信息保护的法律义务。《民法典》第 111 条和第 1035 条对个人信息保护进行总体规定，即“自然人的个人信息受法律保护”，而“处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理”。

所谓“合法”，就是要求信息收集应该具有合法目的、合法方式与合法内容，“不违反法律、行政法规的规定”。例如，《民法典》第 1033 条的禁止性规定：“除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施”侵扰他人的私人生活安宁的行为，以及“拍摄、窥视他人的私密空间、私密活动、私密部位，处理他人的私密信息”。

所谓“正当”，原则上要求“征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外”。需要强调的是，“同意”并非概括性同意，例如，公民同意下载安装手机应用 App，但并不等同于对该 App 的所有获取、处理公民个人信息的行为进行一次性授权，否则，“同意”规则就流于形式，实质上丧失了个人信息保护的“安全阀”作用，由公民“信息自决”的法律预期沦落为服务商“信息他决”的实务困境。“正当”原则要求个人信息获取方和个人信息提供方根据意思自治原则订立并遵守“双方的约定”，约定订立的便捷性应当服从于正当性。除非法律、行政法规规定（不包括部门规章和规范性文件），或经当事人同意，其他收集、使用、加工、传输他人个人信息行为，即为非法处理。

所谓“必要”，实际上是对“非必要不收集”“不得过度处理”的高度概括，或称之为公民个人信息处理的“最小比例原则”。在实务中，“过度处理”问题比较普遍，即部分国家机关、商业机构将获取数量更多、样本更全、数据颗粒度更细致的个人信息作为其“数据资产”，并通过数据加工等方式进一步提升数据价值，个别单位或个人还存在数据交易行为，导致公民对于授权提供后的个人信息保护，事实上无法有效监管，其知情权、监督权都无法得到有效保障。

个人信息安全并不仅仅专指违规收集个人信息，《民法典》特别规定了“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等”行为。《民法典》第 111 条又作出专门性规定，“任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”实际上，这为个人信息安全的全流程全周期保护奠定了良好的法律基础。个人信息安全的合法、正当、必要原则不仅仅需要应用于个人信息收集安全，也应当包括个人信息存储安全、个人信息使用安全、个人信息加工安全、个人信息传输安全、个人信息提供安全、个人信息公开安全，以及个人信息其他处理环节的安全。

三、事后救济：健全个人信息安全保护的多元机制

“无救济即无权利。”对个人信息保护救济，《民法典》主要通过三个方面进行保护。

一是明确网络侵权责任和救济方式。对侵犯公民个人信息的行为，《民法典》第 1194 条规定：“网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任。”《民法典》第 1197 条规定：“网络服务提供者知道或者应当知道网络用户利用其网络服务侵害他人民事权益，未采取必要措施的，与该网络用户承担连带责任。”对侵犯公民个人信息的行为，造成财产消极损害应对侵权导致的损害部分进行追偿，对非财产损害，应根据《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》，停止侵害、消除影响、赔礼

道歉，“造成严重后果的，受害人有权要求侵权人赔偿相应的精神损害抚慰金”。

二是沿用了网络信息传播权“避风港原则”的“通知—删除”义务。《民法典》第 1037 条第 2 款规定：“自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除”。相比《信息网络传播权保护条例》承担“删除”义务的“网络服务提供者”，《民法典》将个人信息保护的“删除”义务范围扩大到“信息处理者”，不再局限于互联网服务提供商（ISP）。

三是新增了向主管部门的报告义务，有利于重大信息安全事故的国家介入和行政处置。《民法典》第 1038 条增加了个人信息安全风险事件的报告义务，即“发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告”，以便主管部门能够及时有效采取应对手段。《民法典》与《网络安全法》相互衔接，根据《网络安全法》第 55 条规定，发生网络安全事件后，国家网信部门在监测到相关风险时，应协调有关部门“立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息”，从而形成公民个人信息大规模泄露在内的网络安全事件的国家、企业、公民保护合力。

个人信息安全保护是一个系统工程，保护公民个人信息，需要建立更加高效、便捷的救济和惩治途径，既需要明确规定个人信息安全保护的民事责任、行政责任和刑事责任，还需要明确并建立侵权后的救济途径。在《民法典》和即将颁布的《数据安全法》《个人信息保护法》等实体法做出重大变化后，立法机关也需要对诉讼法和有关配套法律法规及时做出必要调整和补充，更详尽规定救济途径。司法实务部门在“互联网法院”等试点基础上，亟待进一步建立健全侵犯公民个人信息等网络侵权行为的纠纷解决“绿色通道”。（来源：《中国信息安全》杂志 2020 年第 10 期）

➢ 2020 年中国网络与数据十大法治事件

信息通信技术的变革和创新给人类和社会的发展带来了新空间——网络空间。网络空间的载体是网络,核心是数据,依法加强国家网络空间和数据的治理是我国数字经济安全与发展的必要手段,也是数字经济时代国家治理体系和治理能力现代化的重要标志。2020 年的新冠肺炎疫情防控期间,我国网络与数据法治领域也面临了一场大考,但交出了满意的答卷,取得

了可喜的成绩。中国通信学会网络安全战略与法律委员会联合中国数字经济安全与发展 50 人论坛、中国信息通信研究院互联网法律研究中心、上海市法学会互联网司法研究会、浙江大学网络空间国际治理研究基地、南京邮电大学数字经济战略与法治研究中心、北京邮电大学互联网治理与法律研究中心、重庆邮电大学网络空间安全与信息法学院、西南政法大学中国信息法制研究所以及上海市光明律师事务所通过对全年网络与数据法治事件的跟踪、研究和评估,现发布“2020 年中国网络与数据十大法治事件”。

一、党的十九届五中全会《建议》强化数据治理机制

2020 年 10 月 29 日,党的第十九届中央委员会第五次全体会议审议通过的《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》(以下称:《建议》),《建议》提出：1.要建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范,推动数据资源开发利用；2.扩大基础公共信息数据有序开放,建设国家数据统一共享开放平台；3.保障国家数据安全,加强个人信息保护；4.提升全民数字技能,实现信息服务全覆盖；5.积极参与数字领域国际规则和标准制定。

党的十九届四中全会通过的《中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干重大问题的决定》提出了八项要求,为我国今后的网络与数据法治建设指明发展方向:

1.坚持法治建设为了人民、依靠人民,加强人权法治保障,保证人民依法享有广泛的权利和自由、承担应尽的义务,引导全体人民做社会主义法治的忠实崇尚者、自觉遵守者、坚定捍卫者;

2.建立健全运用互联网、大数据、人工智能等技术手段进行行政管理的制度规则。推进数字政府建设,加强数据有序共享,依法保护个人信息;

3.构建网上网下一体、内宣外宣联动的主流舆论格局,建立以内容建设为根本、先进技术为支撑、创新管理为保障的全媒体传播体系;

4.建立健全网络综合治理体系,加强和创新互联网内容建设,落实互联网企业信息管理主体责任,全面提高网络治理能力,营造清朗的网络空间;

5.发挥网络教育和人工智能优势,创新教育和学习方式,加快发展面向每个人、适合每个人、更加开放灵活的教育体系,建设学习型社会;

6.构建基层社会治理新格局。推动社会治理和服务重心向基层下移,把更多资源下沉到基层,更好提供精准化、精细化服务;

7.坚持总体国家安全观,统筹发展和安全,坚持人民安全、政治安全、国家利益至上有机统一。以人民安全为宗旨,以政治安全为根本,以经济安全为基础,以军事、科技、文化、社会安全为保障,健全国家安全体系,增强国家安全能力。

8.健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制。

二、中共中央 国务院《意见》加快培育数据要素市场

党的十九届四中全会首次提出,把数据作为生产要素按贡献参与分配,这是的一项重大产权制度,为加速数据生产要素市场的培育提出了方向,具有重大战略意义。2020 年 3 月 30 日,中共中央、国务院发布了《关于构建更加完善的要素市场化配置体制机制的意见于构建更加完善的要素市场化配置体制机制的意见》(以下称:《意见》),《意见》明确提出在以下三个方面加快培育数据要素市场。

1.推进政府数据开放共享。优化经济治理基础数据库,加快推动各地区各部门间数据共享交换,制定出台新一批数据共享责任清单。研究建立促进企业登记、交通运输、气象等公共数据开放和数据资源有效流动的制度规范;

2.提升社会数据资源价值。培育数字经济新产业、新业态和新模式,支持构建农业、工业、交通、教育、安防、城市管理、公共资源交易等领域规范化数据开发利用的场景。发挥行业协会商会作用,推动人工智能、可穿戴设备、车联网、物联网等领域数据采集标准化。

3.加强数据资源整合和安全保护。探索建立统一规范的数据管理制度,提高数据质量和规范性,丰富数据产品。研究根据数据性质完善产权性质。制定数据隐私保护制度和安全审查制度。推动完善适用于大数据环境下的数据分类分级安全保护制度,加强对政务数据、企业

商业秘密和个人数据的保护。

三、中共中央《法治社会建设实施纲要》确立依法治理网络空间

2020 年 12 月 7 日,中共中央印发了《法治社会建设实施纲要(2020-2025 年)》(以下称:《纲要》)。《纲要》提出,法治社会是构筑法治国家的基础,法治社会建设是实现国家治理体系和治理能力现代化的重要组成部分。建设信仰法治、公平正义、保障权利、守法诚信、充满活力、和谐有序的社会主义法治社会,是增强人民群众获得感、幸福感、安全感的重要举措。

《纲要》强调,要推动社会治理从现实社会向网络空间覆盖,建立健全网络综合治理体系,加强依法管网、依法办网、依法上网,全面推进网络空间法治化,营造清朗的网络空间。《纲要》对依法治理网络空间提出了三大举措,涉及二十四项内容:

(一)完善网络法律制度

1.通过立改废释并举等方式,推动现有法律法规延伸适用到网络空间；2.完善网络信息服务方面的法律法规,修订互联网信息服务管理办法,研究制定互联网信息服务严重失信主体信用信息管理办法,制定完善对网络直播、自媒体、知识社区问答等新媒体业态和算法推荐、深度伪造等新技术应用的规范管理办法；3.完善网络安全法配套规定和标准体系,建立健全关键信息基础设施安全保护、数据安全管理和网络安全审查等网络安全管理制度,加强对大数据、云计算和人工智能等新技术研发应用的规范引导；4.研究制定个人信息保护法；5.健全互联网技术、商业模式、大数据等创新成果的知识产权保护方面的法律法规；6.修订预防未成年人犯罪法,制定未成年人网络保护条例；7.完善跨境电商制度,规范跨境电子商务经营者行为；8.积极参与数字经济、电子商务、信息技术、网络安全等领域国际规则和标准制定。

(二)培育良好网络法治意识

1.坚持依法治网和以德润网相结合,弘扬时代主旋律和社会正能量；2.加强和创新互联网内容建设,实施社会主义核心价值观、中华文化新媒体传播等工程；3.提升网络媒介素养,推动互联网信息服务领域严重失信“黑名单”制度和惩戒机制,推动网络诚信制度化建设；4.坚决依法打击谣言、淫秽、暴力、迷信、邪教等有害信息在网络空间传播蔓延,建立健全互联网违法和不良信息举报一体化受理处置体系；5.加强全社会网络法治和网络素养教育,制定网络素养教育指南；6.加强青少年网络安全教育,引导青少年理性上网；7.深入实施中国好网民工程和网络公益工程,引导网民文明上网、理性表达,营造风清气正的网络环境。

(三)保障公民依法安全用网

1.要牢固树立正确的网络安全观,依法防范网络安全风险；2.落实网络安全责任制,明确

管理部门和网信企业的网络安全责任；3.建立完善统一高效的网络安全风险报告机制、研判处置机制,健全网络安全检查制度；4.加强对网络空间通信秘密、商业秘密、个人隐私以及名誉权、财产权等合法权益的保护；5.严格规范收集使用用户身份、通信内容等个人信息行为,加大对非法获取、泄露、出售、提供公民个人信息的违法犯罪行为的惩处力度；6 督促网信企业落实主体责任,履行法律规定的安全管理责任；7.健全网络与信息突发安全事件应急机制,完善网络安全和信息化执法联动机制；8.加强网络违法犯罪监控和查处能力建设,依法查处网络金融犯罪、网络诽谤、网络诈骗、网络色情、攻击窃密等违法犯罪行为；9.建立健全信息共享机制,积极参与国际打击互联网违法犯罪活动。

四、强化疫情期间个人信息保护和利用大数据支撑疫情联防联控工作

为了做好个人信息保护和利用大数据支撑疫情联防联控工作,2020 年 2 月 4 日,中央网络安全和信息化委员会办公室发布了《关于做好个人信息保护利用大数据支撑联防联控工作的通知》(以下称:《通知》),《通知》明确了疫情期间个人信息保护的六大要点:

1.各地方各部门要高度重视个人信息保护工作,除国务院卫生健康部门依据《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外,其他任何单位和个人不得以疫情防控、疾病防治为由,未经被收集者同意收集使用个人信息。法律、行政法规另有规定的,按其规定执行。

2.收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》,坚持最小范围原则,收集对象原则上限于确诊者、疑似者、密切接触者等重点人群,一般不针对特定地区的所有人群,防止形成对特定地域人群的事实上歧视。

3.为疫情防控、疾病防治收集的个人信息,不得用于其他用途。任何单位和个人未经被收集者同意,不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息,因联防联控工作需要,且经过脱敏处理的除外。

4.收集或掌握个人信息的机构要对个人信息的安全保护负责,采取严格的管理和技术防护措施,防止被窃取、被泄露。

5.鼓励有能力的企业在有关部门的指导下,积极利用大数据,分析预测确诊者、疑似者、密切接触者等重点人群的流动情况,为联防联控工作提供大数据支持。

6.任何组织和个人发现违规违法收集、使用、公开个人信息的行为,可以及时向网信、公安部门举报。网信部门要依据《网络安全法》和相关规定,及时处置违规违法收集、使用、公开个人信息的行为,以及造成个人信息大量泄露的事件;涉及犯罪的公安机关要依法严厉打击。

《通知》依法对疫情期间的数据安全和个人信息保护做出全面的指导,切实加强了数据

安全和个人信息安全,严防疫情数据泄露,保护确诊者、疑似者、密切接触者等重点人群的信息和隐私安全,严禁单位和个人对疫情数据和个人信息的滥用等违法违规行为。

2020 年 3 月 2 日,民政部办公厅、中央网信办秘书局、工业和信息化部办公厅、国家卫生健康委办公厅发布《新冠肺炎疫情社区防控工作信息化建设和应用指引》(以下称:《指引》),《指引》提出了疫情社区防控工作信息化建设和应用目标,按照疫情防控总体部署和社区防控工作要求,坚持适用性、便捷性、安全性和前瞻性相统一,发挥互联网、大数据、人工智能等信息技术优势,依托各类现有信息平台特别是社区信息平台,开发适用于社区防控工作全流程和各环节的功能应用,有效支撑社区疫情监测、信息报送、宣传教育、环境整治、困难帮扶等防控任务,统筹发挥城乡社区组织、社区工作者的动员优势和信息化、智能化手段的技术优势,有效支撑省、市、县、乡四级数据联通,构筑起人防、物防、技防、智防相结合的社区防线,形成立体式社区防控数据链路和闭环,提升城乡社区疫情防控工作成效。

五、《民法典》强化对公民隐私权和个人信息的保护力度

2020 年,新中国第一部以法典命名的法律——《中华人民共和国民法典》(以下简称:《民法典》)正式颁布,开创了我国法典编纂立法的先河。在《民法典》的七编中,唯独有一编名称中有一个格外醒目的字——“人”,即第四编“人格权编”,人格权独立成编恪守了“以人民为中心”的理念,以人格尊严的至高无上为其根本出发点,这是我国民法典编纂最大的创新和亮点。

《民法典》第四编在对传统人格权保护的基础上,有针对性的对网络时代公民隐私权做出了新规定,尤其是强化了对个人信息保护的力度,完善了“个人信息”的定义和保护范围。《民法典》第一千零三十四条规定:“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息,包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。”从以上“个人信息”的定义中可以看出,《民法典》与《网络安全法》最大的不同在于,前者只强调“识别特定自然人的各种信息”,而后者范围扩大至“识别自然人个人身份的各种信息”。

《民法典》对于个人信息的处理,在《网络安全法》遵循“合法、正当、必要”原则的基础上,增加了“不得过度处理”,并须符合四个条件:一是征得该自然人或者其监护人同意,但是法律、行政法规另有规定的除外;二是公开处理信息的规则;三是明示处理信息的目的、方式和范围;四是不违反法律、行政法规的规定和双方的约定。

六、《数据安全法(草案)》进入立法程序

第十三届全国人大常委会第二十次会议对《中华人民共和国数据安全法(草案)》(以下称:

《数据安全法(草案)》)进行了审议,我国数据安全法正式进入立法程序。《数据安全法(草案)》)是数字安全领域一部基础性的法律,共七章,五十一条,分别为总则、数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任及附则。整体上看,数据安全法(草案)》)体现了总体国家安全观的立法目标,突出了“数据安全与发展”并重原则。关于“数据安全与发展”的关系,《数据安全法(草案)》确定为:“以数据开发利用和产业发展促进数据安全,以数据安全保障数据开发利用和产业发展”,主要有以下亮点:

首先,按照总体国家安全观的要求,确立数据安全保护管理各项基本制度,提升国家数据安全保障能力,有效应对数据这一非传统领域的国家安全风险与挑战,切实维护国家主权、安全和发展利益。

其次,坚持安全与发展并重,规定支持、促进数据安全与发展的措施,提升数据安全治理和数据开发利用水平,促进以数据为关键要素的数字经济发展。

再次,立足数据安全工作实际,着力解决数据安全领域突出问题,落实数据活动主体的安全保护义务与责任,切实维护公民、组织的合法权益。

第四,适应电子政务发展的需要,建立政务数据安全管理制度和开放利用规则,大力推进政务数据资源开放和开发利用。

七、《个人信息保护法(草案)》公开征求意见

第十三届全国人大常委会第二十二次会议对《中华人民共和国个人信息保护法(草案)》(以下简称:《个人信息保护法(草案)》)进行了审议,2020 年 10 月 21 日,全国人大法工委公开就《草案》公开征求意见。《草案》全文共八章七十条,总则(总则);个人信息处理规则(第二章,本章分为三节,即一般规定、敏感个人信息的处理规则和国家机关处理个人信息的特别规定;个人信息跨境提供的规则(第三章);个人在个人信息处理活动中的权利(第四章);个人信息处理者的义务(第五章);履行个人信息保护职责的部门(第六章);法律责任(第七章);附则(第八章)。

《个人信息保护法(草案)》把以人民为中心理念贯穿立法工作始终,坚持了问题导向和立法前瞻性相结合,借鉴了国外立法的先进经验和做法,尤其是聚焦了广大人民群众对个人信息保护领域突出问题的重大关切,构建了比较完善可行的个人信息保护制度规范。《个人信息保护法》、《网络安全法》和《数据安全法》将构成我国网络与数据保护法治领域的三驾马车。《个人信息保护法(草案)》的起草工作主要把握了以下三点重要内容:

一是坚持立足国情与借鉴国际经验相结合。从我国实际出发,深入总结网络安全法等法律、法规、标准的实施经验,将行之有效的做法和措施上升为法律规范。从上世纪 70 年代开始,经济合作与发展组织、亚太经济合作组织和欧盟等先后出台了个人信息保护相关准则、

指导原则和法规,有 140 多个国家和地区制定了个人信息保护方面的法律。草案充分借鉴有关国际组织和国家、地区的有益做法,建立健全适应我国个人信息保护和数字经济发展需要的法律制度;

二是坚持问题导向和立法前瞻性相结合。既立足于个人信息保护领域存在的突出问题和人民群众的重大关切,建立完善可行的制度规范。同时,对一些尚存争议的理论问题,在本法中留下必要空间,对新技术新应用带来的新问题,在充分研究论证的基础上作出了必要规定,体现法律的包容性、前瞻性;

三是处理好与有关法律的关系。把握权益保护的立法定位,与民法典等有关法律规定相衔接,细化、充实个人信息保护制度规则。同时,与网络安全法和已提请全国人大常委会审议的数据安全法草案相衔接,对于网络安全法、数据安全法草案确立的网络和数据安全监管相关制度措施,《个人信息保护法(草案)》不再作规定。

八、《未成年人保护法(修订案)》时隔 14 年再次修订,增设网络保护专章

2019 年 10 月 21 日,《中华人民共和国未成年人保护法(修订案)》(以下称:《未成年人保护法(修订案)》)提请十三届全国人大常委会第十四次会议审议,其中最大的亮点是专门增设了“网络保护”一章。2020 年 10 月 17 日,《未成年人保护法(修订案)》经十三届全国人大常委会第二十二次会议表决通过,自 2021 年 6 月 1 日起施行,这是《未成年人保护法(修订案)》时隔 14 年再次修订。

随着信息技术的快速发展,网络空间作为家庭、学校、社会等现实世界的延展,已经成为未成年人成长的新环境。修订草案适应客观形势的需要,增设“网络保护”专章,对网络保护的理念、网络环境管理、相关企业责任、网络信息管理、个人网络信息保护、网络沉迷防治等作出全面规范。

《未成年人保护法(修订案)》第五章“网络保护”共有十七条,主要涉及的内容:加强未成年人网络素养宣传教育,创作与传播利于未成年人健康成长的网络内容,加强对未成年人网络保护工作的监督检查,定期开展预防未成年人沉迷网络的宣传教育,为未成年人提供的互联网上网服务设施,未成年学生不得将手机等智能终端产品带入课堂,未成年人的父母或者其他监护人应当提高网络素养,处理未成年人个人信息应当遵循合法、正当和必要原则,不得向未成年人提供诱导其沉迷的产品和服务,国家建立统一的未成年人网络游戏电子身份认证系统,网络直播服务提供者不得为未满十六周岁的未成年人提供网络直播发布者账号注册服务,网络产品和服务提供者应当建立便捷、合理、有效的投诉和举报渠道等。

九、中央经济工作会议明确提出“强化反垄断”

2020 年 12 月 11 日,中共中央政治局召开会议,要求强化反垄断和防止资本无序扩张。12 月 16 日至 18 日在北京举行的中央经济工作会议重申,要强化反垄断和防止资本无序扩张。中央经济工作会议明确指出,反垄断、反不正当竞争,是完善社会主义市场经济体制、推动高质量发展的内在要求。要加强规制,提升监管能力,坚决反对垄断和不正当竞争行为。

中央政治局会议和中央经济工作会议均明确提出,要强化反垄断和防止资本无序扩张,得到社会热烈反响和广泛支持。平台企业,尤其是超级平台企业的反垄断已成为关系全局的紧迫议题。

目前,超级平台已经成为互联网领域的市场寡头,超级平台之所以能够成为市场寡头,是因为其通过自身营造的网络生态系统吸引千万流量、汇聚海量信息,进而形成网络的交叉效应。因此,超级平台最重要的是对数据的垄断,对数据的控制提高了超级平台的市场进入壁垒及转换成本,带来了超级平台通吃的局面,而且超平台本还有一项重要的职能,就是对平台的监管和治理。因此,反垄断法必须有所作为,不能任由平台集中和垄断数据影响整个行业的正常竞争秩序和良性发展。

为预防和制止平台经济领域垄断行为,引导平台经济领域经营者依法合规经营,促进线上经济持续健康发展,市场监管总局起草了《关于平台经济领域的反垄断指南(征求意见稿)》,于 2020 年 11 月 10 日向社会公开征求意见。

《征求意见稿》共六章二十四条,对平台经济领域开展反垄断监管坚持以下五项原则:

一是营造公平竞争秩序。着力预防和制止排除、限制竞争的垄断行为,维护平台经济领域公平竞争、开放包容的发展环境,降低市场进入壁垒,促进更多主体进入市场,公平有序参与竞争,激发市场活力。

二是加强科学有效监管。《反垄断法》的基本制度、规制原则和分析框架适用于平台经济领域所有市场主体。反垄断执法机构将根据平台经济的发展状况、发展规律和自身特点,强化竞争分析和法律论证,不断加强和改进反垄断监管,增强反垄断执法的针对性、科学性。

三是激发创新创造活力。维护平台经济领域公平竞争,引导和激励平台经营者将更多资源用于技术革新、质量改进、服务提升和模式创新,防止和制止排除、限制竞争行为抑制平台经济创新发展和经济活力,有效激发全社会创新创造动力,构筑经济社会发展新优势和新动能。

四是促进行业健康发展。通过反垄断监管维护平台经济领域公平有序竞争,充分发挥平台经济高效匹配供需、降低交易成本、发展潜在市场的作用,推动资源配置优化、技术进步、效率提升,支持和促进实体经济发展。

五是维护各方合法利益。平台经济发展涉及多方主体。反垄断监管在保护市场公平竞争、

保障和促进平台发展的同时,着力维护平台内经营者和消费者等各方主体的合法权益,使全社会能够共享平台技术进步和经济发展成果,实现平台经济整体生态和谐共生和健康发展。

《征求意见稿》对平台进行了明确的定义,即平台为互联网平台,是指通过网络信息技术,使相互依赖的多边主体在特定载体提供的规则和撮合下交互,以此共同创造价值的商业组织形态。《征求意见稿》对相关市场界定,要求在遵循《反垄断法》和《国务院反垄断委员会关于相关市场界定的指南》所确定的一般原则的基础上,要考虑平台经济的特点,结合个案进行具体分析。

《征求意见稿》还就平台经济领域垄断协议,滥用市场支配地位行为,经营者集中以及滥用行政权力排除、限制竞争做出了详细的认定标准。

十、国家对互联网平台企业开展反垄断调查

2020 年 12 月,国家市场监管总局根据举报,依法对阿里巴巴集团控股有限公司实施“二选一”等涉嫌垄断行为开展立案调查。2020 年 12 月 24 日,国家市场监管总局调查组执法人员进驻阿里巴巴集团控股有限公司开展调查。调查人员对阿里巴巴集团控股有限公司及部门相关负责人进行了调查询问,并提取相关证据资料。阿里巴巴集团控股有限公司积极配合,认真接受调查组询问,及时提供相关资料,自觉接受调查。

近年来,我国平台经济蓬勃发展,新业态、新模式层出不穷,对推动经济高质量发展、满足人民日益增长的美好生活需要发挥了重要作用。但与此同时,平台经济凭借数据、技术、资本优势也呈现市场集中度越来越高的趋势,市场资源加速向头部平台集中,关于平台垄断问题的反映和举报日益增加,显示平台经济发展中存在一些风险和隐患。

纵观全球,谷歌、苹果、Facebook、亚马逊四大科技巨头在全球范围内被多次提起反垄断调查。据南都个人信息保护研究中心统计,这些反垄断调查中,谷歌面临 27 起、亚马逊和苹果面临 22 起、Facebook 面临 13 起,其中欧盟对谷歌进行反垄断处罚的金额已经累计超过 600 亿元。

我国互联网业态的飞速发展直接得益于我国采取的包容与审慎并重的监管原则,针对互联网巨头的反垄断调查,视乎要来得迟一些。尽管我国《反垄断法》在 2008 年 8 月 1 日就已经生效,但时至今日没有一家中国互联网公司因为违反《反垄断法》而被公开查处。应当指出,互联网行业从来不是,也不应该成为反垄断的法外之地。2020 年初公布的《〈反垄断法〉修订草案(公开征求意见稿)》首次增设互联网经营者市场支配地位认定依据的规定。这次国家市场监管总局依法对阿里巴巴集团控股有限公司实施“二选一”等涉嫌垄断行为开展立案调查,可谓是中国互联网反垄断调查的“第一案”。（来源：法制日报）

四、政府之声

➢ 工信部印发《电信和互联网行业数据安全标准体系建设指南》通知

2020 年 12 月 25 日，工业和信息化部办公厅关于印发《电信和互联网行业数据安全标准体系建设指南》的通知 [工信厅科〔2020〕58 号]。

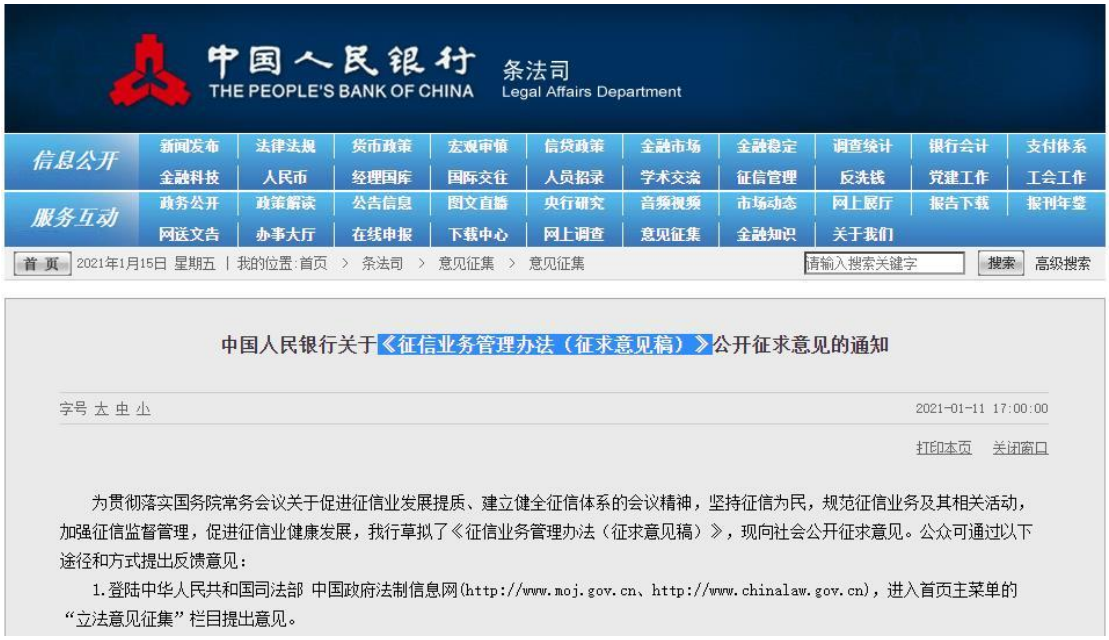
通知要求：为发挥标准对电信和互联网行业数据安全的规范和保障作用，加快制造强国和网络强国建设步伐，现将《电信和互联网行业数据安全标准体系建设指南》印发给你们，请结合本行业(领域)、本地区实际，在标准化工作中贯彻执行。（来源：工业和信息化部办公厅）

- **《电信和互联网行业数据安全标准体系建设指南》全文：**
- https://www.miit.gov.cn/jgsj/kjs/jscx/bzgf/art/2020/art_05443293fbb3406bb70be70f660faddf.html

➢ 中国人民银行就《征信业务管理办法（征求意见稿）》公开征求意见

2021 年 1 月 11 日，中国人民银行发布《征信业务管理办法（征求意见稿）》（以下简称“《办法》”），《办法》分七章 46 条，主要对信用信息和征信业务做了明确规定；从保护个人和企业合法权益角度对信用信息采集、整理、保存和加工进行了规定；规范信用信息的使用，保障用于合法目的；对信用信息安全和跨境流动进行了规定。

《征求意见稿》明确指出，以“信用信息服务、信用服务、信用评分、信用评级、信用修复”等名义对外提供征信功能服务，适用本办法。



征求意见稿指出，个人征信机构、保存或处理 50 万户以上企业信用信息的企业征信机构，应当符合以下要求：1）系统测评为国家信用信息安全等级保护三级或三级以上；2）设立信息安全负责人，由公司章程规定的高级管理人员担任；3）设立专职部门，负责管理信息安全工作，定期检查有关业务及征信系统的安全管理制度及措施执行情况。

征求意见稿指出，征信机构在中国境内开展征信业务及相关活动，生产数据库、备份数据库应设在中国境内。征信机构向境外提供企业信用信息查询服务，应当审查信息使用者的身份、用途，确保信用信息用于跨境贸易、融资等合理的用途，并采取单笔查询的方式提供。征信机构向境外提供企业信用信息的，应当向中国人民银行备案。征信机构与境外征信机构合作的，应当在合作协议签署后向中国人民银行备案。（来源：中国人民银行）

- **《征信业务管理办法（征求意见稿）》**
- **全文：**http://www.pbc.gov.cn/tiaofasi/144941/144979/3941920/4160598/index.html

➢ 中共中央印发《法治中国建设规划（2020－2025 年）》

2021 年 1 月 10 日，中共中央印发了《法治中国建设规划（2020－2025 年）》，并发出通知，要求各地区各部门结合实际认真贯彻落实。

规划提出，深化行政执法体制改革，统筹配置行政执法职能和执法资源，最大限度减少不必要的行政执法事项。健全事前事中事后监管有效衔接、信息互联互通共享、协同配合工作机制。完善行政执法权限协调机制。健全行政执法和刑事司法衔接机制，全面推进“两法

衔接”信息平台建设和应用。完善行政强制执行体制机制。

规划提出，加强科技和信息化保障。充分运用大数据、云计算、人工智能等现代科技手段，全面建设“智慧法治”，推进法治中国建设的数据化、网络化、智能化。优化整合法治领域各类信息、数据、网络平台，推进全国法治信息化工程建设。

规划提出，加快推进我国法域外适用的法律体系建设。强化涉外法律服务，维护我国公民、法人在海外及外国公民、法人在我国的正当权益。建立涉外工作法务制度。引导对外经贸合作企业加强合规管理，提高法律风险防范意识。建立健全域外法律查明机制。（来源：新华社）

- **中共中央印发《法治中国建设规划(2020－2025 年)》**
- **全文：**http://www.gov.cn/xinwen/2021-01/10/content_5578659.htm

➢ 中国银保监会印发《保险中介机构信息化工作监管办法》

2021 年 1 月 5 日，为加强保险中介监管，提高保险中介机构信息化工作与经营管理水平，构建新型保险中介市场体系，推动保险中介行业高质量发展，银保监会近日印发了《保险中介机构信息化工作监管办法》（以下简称《办法》）。

《办法》起草工作坚决贯彻落实中央精神，注意把握以下工作原则：一是坚持问题导向，切实防范风险；二是规范信息交互，提升监管效能；三是科学合理适度，避免过高要求。《办法》起草过程中，坚持开门立法，通过市场调研、监管座谈、书面征求意见等形式广泛征求意见，银保监会对反馈意见逐条研究论证，绝大多数意见已采纳。各相关单位普遍认为《办

法》有助于规范保险中介机构信息化工作、提高保险中介机构经营管理水平，能够为保险中介监管提供有效抓手，更好地促进保险中介行业高质量发展。

《办法》共 6 章 36 条，对保险中介机构信息化工作提出全面要求。一是在总则中明确《办法》的制定目的、适用范围、基本原则、责任主体和监管部门。二是在基本要求中规定保险中介机构的信息化工作机构职责、关联企业隔离要求、高管负责制度、信息化岗位要求、业务申请条件、分支机构管理、监管报送要求、突发事件报告等内容。三是提出信息系统建设要求，明确保险中介机构信息系统的基本功能、建设方式、外包管理、权限管理、数据录入、系统变更等要求。四是明确信息安全要求，对保险中介机构信息化工作的安全体系、等级保护、数据安全、个人信息保护、终端安全、教育培训等提出要求。五是规定保险中介机构信息化工作监督管理的有关内容，包括监管理念、监管分工、审查、现场检查、责任追究等，明确提出：不符合《办法》要求的视为不满足《保险代理人监管规定》《保险经纪人监管规定》《保险公估人监管规定》对于信息化建设和管理的相关规定，不得经营保险中介业务。六是在附则中明确《办法》的实施时间、过渡期整改要求、解释权和此前发布的相关规范性文件的废止，要求保险中介机构在《办法》实施之日起一年内完成整改并向监管部门报送报告。（来源：中国银行保险监督管理委员会）

- **《保险中介机构信息化工作监管办法》全文：**
- http://www.cbirc.gov.cn/cn/view/pages/govermentDetail.html?docId=958343&itemId=&generaltype=1

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 1 月安全更新

发布日期：2021-1-12

更新日期：2021-1-12

2021 年 1 月 12 日，微软发布了 2021 年 1 月份的月度例行安全公告，修复了其多款产品存在的 83 个安全漏洞。受影响的产品包括：Windows 10 20H2 & WindowsServer v20H2（62 个）、Windows 10 2004 & WindowsServer v2004（62 个）、Windows 10 1909 & WindowsServer v1909（59 个）、Windows 8.1 & Server 2012 R2（42 个）、Windows Server 2012（38 个）、Microsoft Edge (HTML based)（1 个）、Microsoft Office-related software（10 个）。利用上述漏洞，攻击者可进行欺骗，绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2021-1673	**Windows RPC Runtime 远程代码执行漏洞**	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2021-1648	**Microsoft splwow64 权限提升漏洞**	重要 特权提升	Windows 10 Server 2016 Server 2019 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2021-1674	**Windows Remote Desktop Protocol Core 安全功能绕过漏洞**	重要 安全功能绕过	Windows 10 Server 2016 Server 2019 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2021-1665	**GDI+远程代码执行漏洞**	严重 远程代码执行	Windows 10 Server 2016

			Server 2019 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2021-1643	**HEVC Video Extensions 远程代码执行漏洞**	严重 远程代码执行	HEVC Video Extensions
CVE-2021-1705	**Microsoft Edge (HTML-based) 内存破坏漏洞**	严重 远程代码执行	Microsoft Edge(EdgeHTML-based)
CVE-2021-1714	**Microsoft Excel 远程代码执行漏洞**	重要 远程代码执行	Office 2010/2013/2016/2019 365 Apps Enterprise Excel 2010/2013/2016 Office Web Apps 2013 Office Online Server Office 2019 for Mac SharePoint Ent. 2013
CVE-2021-1715	**Microsoft Word 远程代码执行漏洞**	重要 远程代码执行	Office 2010/2016/2019 365 Apps Enterprise Word 2010/2013/2016 Office Web Apps 2010/2013 Office Online Server Office 2019 for Mac SharePoint 2010 SharePoint Ent. 2013 SharePoint 2016 SharePoint 2019
CVE-2021-1707	**Microsoft SharePoint Server 远程代码执行漏洞**	重要 远程代码执行	SharePoint 2010 SharePoint 2013 SharePoint Ent 2016 SharePoint 2019

来源： https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan

➢ Adobe Illustrator 存在 dll 劫持漏洞

发布日期： 2021-1-7
更新日期： 2021-1-7
受影响系统：

Adobe Illustrator v25.0

描述：

CVE(CAN) ID: CNVD-2020-69411

Adobe 是美国一家跨国电脑软件公司，总部位于加州的圣何塞。主要从事多媒体制作类软件的开发。

Adobe Illustrator 存在 dll 劫持漏洞，攻击者可利用该漏洞可以加载恶意 dll，执行恶意代码。

建议：

厂商补丁：

adobe

目前厂商尚未提供相关漏洞补丁链接，请关注厂商主页随时更新：

https://www.adobe.com/

➢ Oracle Database Server Scheduler component 未授权访问漏洞

发布日期：2021-1-5

更新日期：2021-1-5

受影响系统：

Oracle Oracle Database Server 11.2.0.4

Oracle Oracle Database Server 12.1.0.2

Oracle Oracle Database Server 12.2.0.1

Oracle Oracle Database Server 18c

Oracle Oracle Database Server 19c

描述：

CVE(CAN) ID: CVE-2020-14735

Oracle Database Server 是美国甲骨文（Oracle）公司的一套关系数据库管理系统。该数据库管理系统提供数据管理、分布式处理等功能。

Oracle Database Server Scheduler component 存在未授权访问漏洞，攻击者可利用该漏洞拥有本地登录特权，登录到调度程序执行的基础设施，从而危及调度程序，导致 Scheduler 被接管。

建议：

厂商补丁：

oracle

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.oracle.com/security-alerts/cpuoct2020.html

➢ Jiransecurity Spamsniper 缓冲区溢出漏洞

发布日期：2021-1-9
更新日期：2021-1-9
受影响系统：
jiransecurity Jiransecurity Spamsniper >=5.0，<=5.2.7
描述：

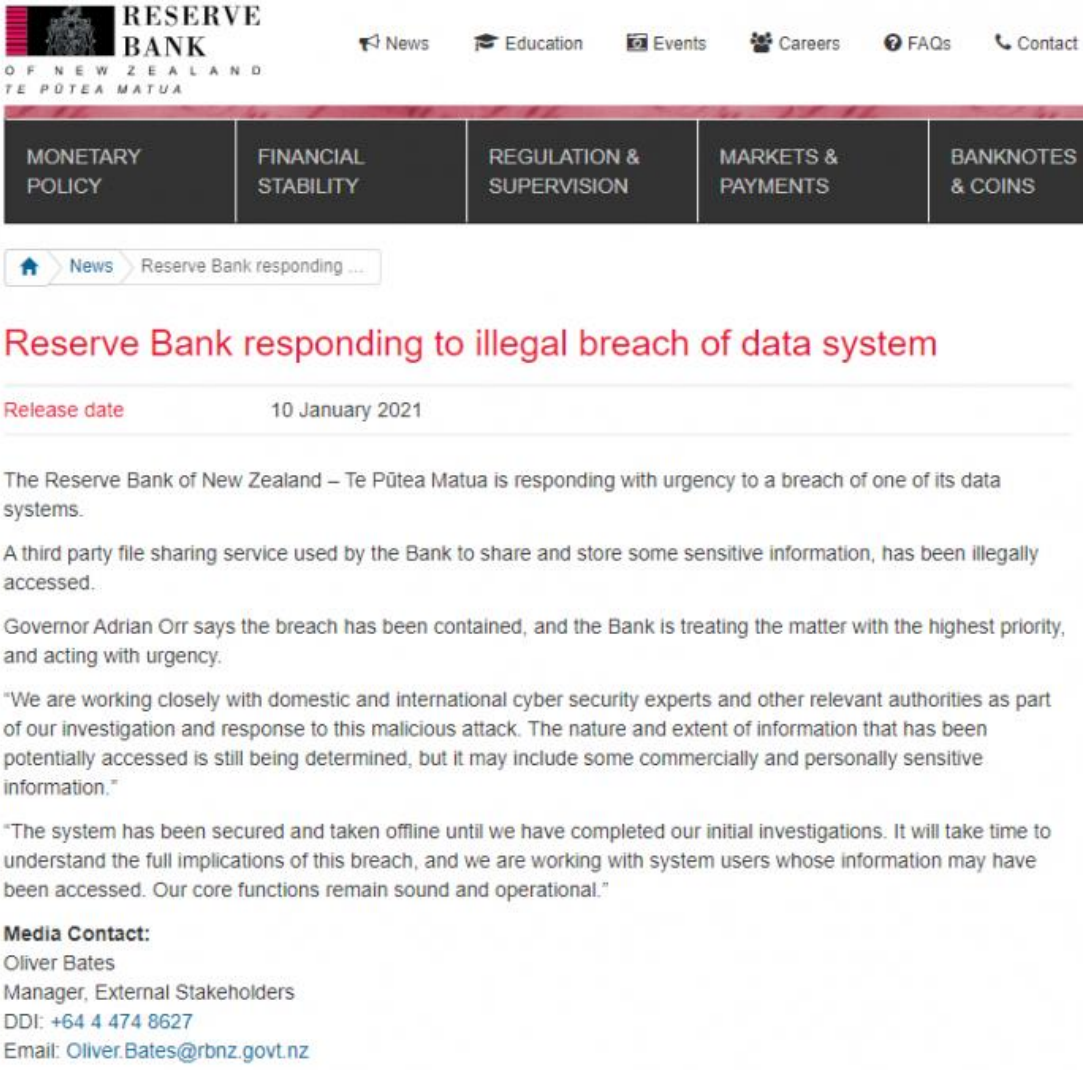
CVE(CAN) ID: CVE-2020-7845
Jiransecurity Spamsniper 是韩国 Jiransecurity 公司的一款集成多功能的电子邮件安全软件。该软件具备阻止垃圾邮件，病毒邮件、防骗、邮件服务器保护、管理、归档等功能。
Spamsniper 5.0 版本至 5.2.7 版本存在缓冲区溢出漏洞，该漏洞源于命令解析邮件时边界检查不当导致的基于堆栈的缓冲区溢出漏洞。它导致远程攻击者可利用该漏洞通过精心制作的数据包执行任意代码。
建议：

厂商补丁：
Jiransecurity
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.jiransecurity.com/

六、本期网络安全事件

➢ 新西兰央行称其数据系统遭黑客攻击 或已获取商业和个人敏感信息

2021 年 1 月 11 日据外媒报道，新西兰央行周日表示，该行的一个数据系统已被一名身份不明的黑客入侵，该黑客有可能已经获取商业和个人敏感信息。这家总部位于惠灵顿的银行在一份声明中说，新西兰储备银行用于共享和存储敏感信息的第三方文件共享服务已被非法访问。



RESERVE BANK OF NEW ZEALAND TE PŪTEA MATUA

News Education Events Careers FAQs Contact

MONETARY POLICY | FINANCIAL STABILITY | REGULATION & SUPERVISION | MARKETS & PAYMENTS | BANKNOTES & COINS

News > Reserve Bank responding ...

Reserve Bank responding to illegal breach of data system

Release date 10 January 2021

The Reserve Bank of New Zealand – Te Pūtea Matua is responding with urgency to a breach of one of its data systems.

A third party file sharing service used by the Bank to share and store some sensitive information, has been illegally accessed.

Governor Adrian Orr says the breach has been contained, and the Bank is treating the matter with the highest priority, and acting with urgency.

"We are working closely with domestic and international cyber security experts and other relevant authorities as part of our investigation and response to this malicious attack. The nature and extent of information that has been potentially accessed is still being determined, but it may include some commercially and personally sensitive information."

"The system has been secured and taken offline until we have completed our initial investigations. It will take time to understand the full implications of this breach, and we are working with system users whose information may have been accessed. Our core functions remain sound and operational."

Media Contact:
Oliver Bates
Manager, External Stakeholders
DDI: +64 4 474 8627
Email: Oliver.Bates@rbnz.govt.nz

行长 Adrian Orr 表示：漏洞已经得到控制。该银行的核心功能 “仍然健全和运作。”Orr 表示：“我们正在与国内和国际网络安全专家和其他相关部门密切合作，作为我们调查和应对这次恶意攻击的一部分。”

“潜在被访问的信息的性质和范围仍在确定中，但可能包括一些商业和个人敏感信息，”

Orr 补充道。在银行完成初步调查之前，该系统已经被保护并下线。“了解此次数据泄露事件的全部影响需要时间，我们正在与信息可能被访问的系统用户合作，”Orr 说。

该银行拒绝回答寻求更多细节的电子邮件问题。目前还不清楚黑客入侵事件发生的时间，也不清楚是否有任何迹象表明谁是责任人，以及文件共享服务是在哪个国家。

在过去的一年里，新西兰的几个主要机构都成为了网络干扰的目标，其中包括新西兰证券交易所，该交易所的服务器在 8 月份遭网络黑客攻击，连续崩溃近一周时间。

奥克兰大学计算机科学教授 Dave Parry 告诉新西兰电台，银行数据泄露事件背后的“罪魁祸首”很可能是另一个政府。“最终如果你是从一种类似于犯罪的角度来的，政府机构是不会支付你的赎金或其他什么的，所以你更感兴趣的可能是从政府对政府的层面来的，”Parry 说。（来源：cnBeta）

➢ 央视曝光窃听黑色产业链：设备可伪装成充电宝 可远程定位和录音

2020 年 12 月 28 日，近日，江苏省南京警方摧毁了一条包括生产厂家、销售代理在内的生产销售定位、窃听、偷拍设备的网络黑色产业链条，抓获犯罪嫌疑人 28 名，缴获相关设备 2000 多个。警方调查发现，这些设备被生产者伪装成充电宝，可以在使用者不知情的情况下，被人远程定位、轨迹查询、远程录音等，涉嫌侵犯公民个人信息。

GPS 定位器变身窃听器 有公司因此损失上千万

一提起窃听，很多人可能最先想到的都是谍战剧的剧情。然而，这些我们在电影电视里

看到的情节很有可能就发生在我们身边。今年 8 月，央视网曾报道，北京一家安防公司就因为商业机密被窃听，企业竞标失败，蒙受了重大损失，而窃听器竟然是我们常见的 GPS 定位器。

在北京一家安防公司，记者见到了这样一个小黑盒。工作人员告诉记者，企业讨论营销方案的会议是高度保密的，但没人想到，座椅下却藏着这个小黑盒。由于商业机密泄露，企业竞标失败，从而蒙受了上千万元的损失。这种小黑盒子，叫做 GPS 定位器，它广泛用于汽车防盗和企业运营车辆管理。

而这样的产品是如何用来非法窃听的呢?

记者尝试买了一个产品进行测试，拆开产品的包装，是一个火柴盒大小的塑料盒，记者按使用说明书在手机上安装好 APP，打开 APP，果然在上面就能实时观察车辆的行驶轨迹。接下来要尝试的是远程监听。两位记者约定，一位和定位器一起留在车内，另一位记者回到办公室准备听音。结果证实，不管被窃听者的声音是大还是小，监听到的声音就像跟对方打电话那么清楚。此外，在 APP 的界面中，还有一个“远程录音”的按钮，启动后，这段对话就被存到了手机里。

也就是说，只要在被窃听者身边放置这样一个 GPS 定位器，就相当于放了一个保持通话的手机。一切声音会被传到窃听者的手机上，甚至被录音，被而窃听者对发生的这一切却浑然不知。

GPS 定位器广泛用于私家车的防盗和企业进行车辆管理。但是，当 GPS 定位器被设计成小巧易于隐蔽、能远程听音的时候，就让产品变了味。而且一些生产厂家和销售商家也正是利用监管盲区，在一些电子产品销售推广广告中进行或多或少的明示暗示其隐藏功能。

这种能够远程收音的 GPS 定位器，内部结构非常简单：一块物联网芯片，还有一块为它供电的电池。芯片接收卫星数据，将数据传输至信号塔，再经信号塔将定位数据传至服务器，使用者向服务器发送请求，就能获取芯片的精准位置。相比一般的物联网芯片，这块芯片上多加了一个微型的麦克风。

目前，GPS 定位器这类产品尚未列入国家强制性产品认证目录。但在此基础上增加麦克风收音等功能却没有相关管理规定，形成监管的盲区。而生产厂家和销售商家也正是利用这种监管盲区，在这类产品销售推广广告中，进行或多或少的明示暗示其隐藏功能。

专家：保护个人信息，应从生产源头开始堵截

2015 年起实施的《禁止非法生产销售使用窃听窃照专用器材和“伪基站”设备的规定》明确禁止自然人、法人及其他组织非法生产、销售、使用窃听窃照专用器材。我国《最高人

民法院关于行政诉讼证据若干问题的规定》第五十七条也明确规定，以窃听手段获取的材料不但不能作为定案依据，行为人很可能还要承担相关的法律责任。对此，专家指出，随着科技的发展，法律应该同步跟进，对利用新技术手段实施的各类违法行为进行规范。

中国政法大学传播法研究中心副主任朱巍：“对个人信息实际上在各个国家，包括中国在内都是一个最高位阶的保护。不能靠企业自律，也不能通过个案来处理，应该是一个常态化的过程。必须是线上线下结合起来，从它的生产源头开始堵截才可以。”（来源：央视网）

➢ 4 万多个人信息被出售 《民法典》实施首例个人信息保护诉讼案宣判

2021 年 1 月 8 日，卖了 4 万余条个人信息，获利 3.4 万元，孙某不仅要被追究刑事责任，还要承担相应的民事责任。近日，由浙江省杭州市下城区检察院提起的民法典实施后全国首例个人信息民事公益诉讼案件，杭州互联网法院通过网络开庭审理并当庭作出判决，支持检察机关的全部诉讼请求，判决孙某赔偿损失 3.4 万元，并在省级新闻媒体公开赔礼道歉，相关赔偿款项将专门用于个人信息保护或信息安全保护等公益事项。

2020 年 8 月，下城区检察院在审查孙某涉嫌侵犯公民个人信息犯罪刑事案件中发现，

2019 年 2 月至 9 月，孙某先后 8 次将从网络购买、互换获得的 4.5 万余条含姓名、电话号码、电子邮箱的公民个人信息，通过微信、QQ 等方式，出售给他人用于虚假外汇业务推广，获利 3.4 万元。上述信息被多次非法倒卖，众多不特定人员的个人信息长期遭受侵害，致使社会公共利益受损。在依法追究孙某刑事责任的同时，该院依法向杭州互联网法院提起民事公益诉讼。

检察机关认为，孙某的行为虽然发生在民法典实施前，但民法典对个人信息保护有更为详尽的规定。案件适用民法典更能体现法律对不特定民事主体人格尊严和人格自由的保护和尊重。案件适用民法典也不存在会“减损当事人的合法权益、增加当事人的法定义务或者背离当事人的合理预期”的情形。同时，民法典规定，侵害他人人身权益造成财产损失的，按照被侵权人因此受到的损失或者侵权人因此获得的利益赔偿。该案中，被告孙某应按照其获利赔偿损失 3.4 万元，并在省级新闻媒体公开赔礼道歉。据此，该院请求法院适用民法典的规定依法判决。

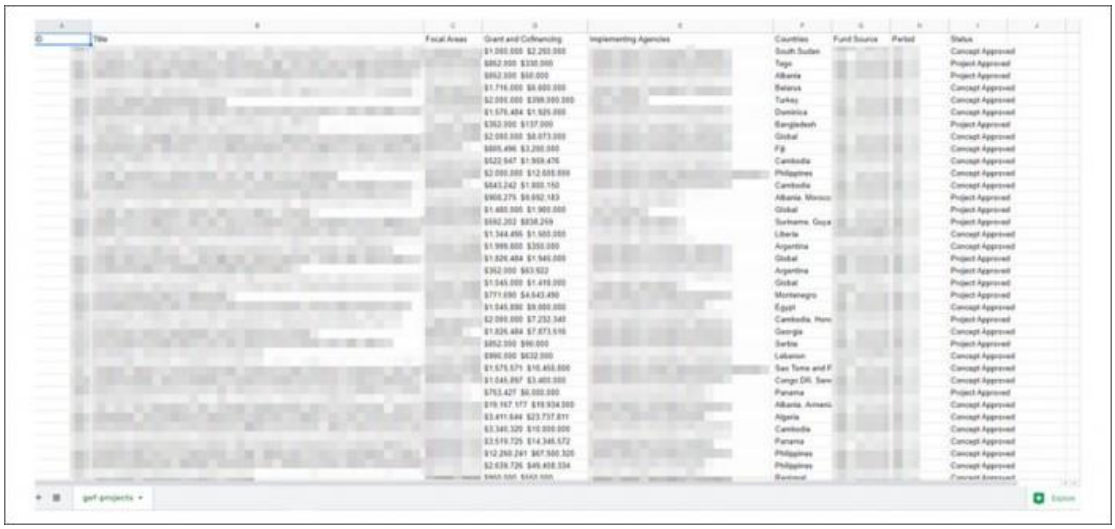
庭审中，检察机关结合危害后果、法律责任与民法典相关法条精神对被告进行了深刻的法庭教育，被告孙某充分认识到其行为给社会公众带来的不良影响，通过其代理律师表示真诚认错悔过，当庭表示服判认罚。法院当庭宣判支持检察机关全部诉讼请求。（来源：杭州日报）

➢ 环境署数据库的一个漏洞暴露联合国雇员数据

2021 年 1 月 14 日报道，据一组独立安全研究人员称，联合国环境规划署（简称“环境署”）所属 GitHub 库的一个漏洞暴露了超过 10 万条员工记录，包括个人身份信息、联系方式和其他敏感数据。环境署负责协调联合国的环境活动。一个新的道德黑客组织 Sakura Samurai 在其报告中指出，这些漏洞源于一个暴露 GitHub 存储库凭证的终端。

“这些凭证让我们有能力下载 GitHub 库，识别出大量的用户凭证和个人身份信息。我们总共识别了超过 10 万条私人员工记录。”该小组的安全研究人员之一 John Jackson 说。

分析还显示，在联合国拥有的名为 ilo.org 的网络服务器上有多个.Git 目录。Jackson 在报告中写道：“这些.Git 内容就可以用各种工具（如'git-dumper'）进行外泄。”



据 Sakura Samurai 报道，在研究人员将他们的发现通知给联合国后，该国际组织修复了该漏洞，GitHub 库已无法访问。目前无法立即联系到联合国发言人发表评论。研究人员还指出，虽然没有证据表明有威胁行为者访问了这些数据，但这样做相对容易。

研究人员首先接管了属于联合国国际劳工组织的一个 MySQL 数据库和一个调查管理平台，开始了他们的行动。然后，该小组分析了 MySQL 数据库中的域，找到了 UNEP 的子域，这让他们找到了 GitHub 的凭证。“最终，一旦我们发现了 GitHub 凭证，我们就能够下载很多受密码保护的私人 GitHub 项目，在这些项目中，我们发现了 UNEP 生产环境的多套数据库和应用凭证，”Jackson 指出。

暴露的数据包括超过 102000 条联合国员工的记录，包括员工的身份证号码、姓名和其他敏感数据。报告称，还可以访问 7000 多条员工国籍记录、1000 多条普通员工记录、项目和资金数据以及环境署项目的评估记录。

研究人员还指出，他们能够找到更多 U.N.GitHub 库的凭证，这可能导致更多未经授权的访问多个 U.N.数据库。“我们决定停止并报告这个漏洞，一旦我们能够访问通过数据库备份暴露的私人项目中的（个人身份信息），”Jackson 写道。

GitHub 存储库中暴露的员工数据可能会给联合国带来重大的网络威胁。“对员工数据泄露的主要担忧是，在对员工本身以及与他们互动的任何商业伙伴进行高度针对性的后续社会工程攻击时有用，”安全公司 Cerberus Sentinel 的解决方案架构副总裁 Chris Clements 说。

“所披露的管理凭证很可能已经足以损害脆弱的应用程序以及共享相同基础设施或重用相同密码的其他应用程序。拥有这种访问权限的攻击者可以将恶意软件插入生产应用程序中，试图感染用户。”

安全公司 KnowBe4 的安全意识倡导者 Javvad Malik 表示，攻击者可能会使用这些暴露的数据。“获得对员工潜在敏感信息的访问权限，可以通过网络钓鱼、密码重置或身份窃取来利用对组织、同事或个人本身的攻击，”Malik 说。

其他攻击

随着 COVID-19 的到来，攻击者一直在欺骗联合国和其他机构，作为他们利用流行病主题的运动的一部分。2 月，安全公司 Kaspersky 和 Sophos 报告说，黑客利用设计成美国疾病控制和预防中心和联合国世界卫生组织的域名进行网络钓鱼活动。根据谷歌威胁分析小组的报告，5 月份，在印度活动的"hack-for-hire" 组织发出欺骗世界卫生组织的电子邮件，以窃取世界各地金融服务、咨询和医疗保健公司员工的证书。（来源：互联网综合整理）

➢ 巨量客户信息被售卖？交行紧急发声明

2021 年 1 月 11 日，交通银行发布公告，回应近期流传的“交通银行客户信息被售卖”一事。交通银行方面表示，近日，有不法分子在暗网发帖贩卖所谓交通银行客户信息，并有部分自媒体转发相关信息。经系统核查比对，确认与交通银行真实客户信息不符。

此前，有公众号发帖称，2021 年 1 月交行遭遇黑客攻击，导致大量信息被泄露贩卖，并以“8.8 枚比特币”的价格被发帖贩卖。对此，交行郑重声明：不存在黑客入侵，不存在客户信息泄漏，并已就相关违法行为向公安部门报案。

三个抓手形成合力保护个人金融信息安全

商业银行作为金融服务行业的关键部门，拥有海量的账户信息和交易信息。实际上，随着个人对信息安全和隐私的保护意识愈加强烈，个人金融信息安全正牵动着消费者的神经。目前，制度约束、监管惩戒与行业自律三个抓手正在形成合力，有力保护个人金融信息安全。

2018 年 5 月，中国银保监会发布《银行业金融机构数据治理指引》，要求银行业金融机

构建立数据安全策略与标准，并进一步提出银行要划分数据安全等级，明确访问和拷贝等权限，监控访问和拷贝等行为，完善数据安全技术，定期审计数据安全。这是从监管层面引导银行建立客户信息安全保护机制。

目前，商业银行在构建信息安全防御体系、加强隐私保护及信息安全风险管理方面也在与时俱进，加速转型。在本次“客户信息被售卖”风波中，交行就表示，该行始终高度重视数据安全保护工作，通过部署多层次网络安全纵深防御措施，切实保障客户信息安全。交行将积极配合相关部门严厉打击伪造贩卖公民信息、恶意造谣扰乱金融秩序的不法行为。

侵害金融信息安全权遭严惩

近年来，商业银行消费者金融信息保护意识不断增强，管理水平不断提升。但也有部分金融机构工作人员无视法律和规定，严重侵害消费者金融信息安全权，受到监管部门惩戒。

比如，2020 年 4 月，浙江岱山农商行违规泄露客户信息，被银保监会舟山监管分局罚款 30 万元。2020 年 5 月，脱口秀演员举报中信银行未经授权向第三方提供其作为银行客户的“个人流水”一事曾引发舆论广泛关注。随后，中信银行迅速处理，开除了涉事人员，银保监会也发布通报启动了立案调查程序。2020 年 10 月，中国人民银行重拳出击，宣布对建设银行、中国银行、农业银行旗下支行侵害消费者金融信息安全行为立案调查，并责令其整改。

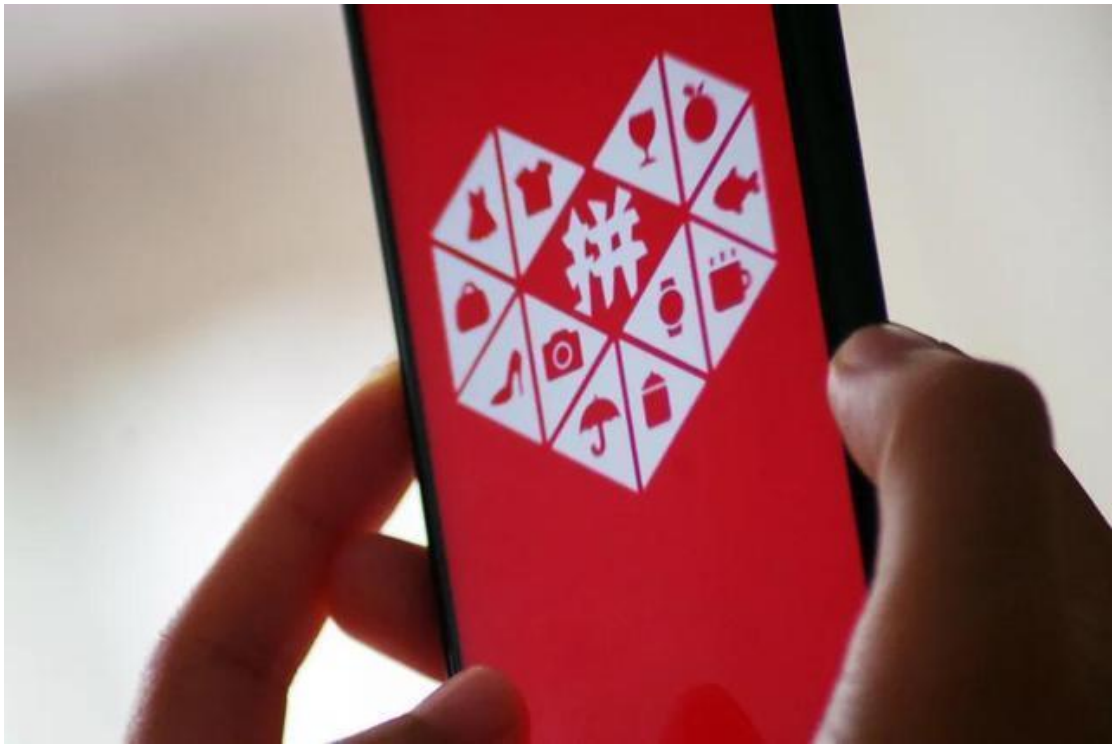
消费者需重点做好七个方面

根据央行此前对消费者金融信息安全的提示，消费者在信息安全方面需重点做好以下几步：

1. 要保管好身份证件、银行卡、银行（支付）账户等，不要转借他人使用；
2. 切勿向他人透露个人金融信息、财产状况等基本信息，不要随意在各类线上线下渠道留下个人金融信息；
3. 尽量亲自办理金融业务，切勿委托不熟悉的人或中介代办，谨防个人金融信息被盗；
4. 提供个人身份证件复印件办理各类业务时，要在复印件上注明使用用途；
5. 不要随意丢弃刷卡签购单、取款凭条、信用卡对账单等，及时销毁作废的金融业务单据；
6. 不要轻易点击来历不明的手机短信、邮件和不明链接，不要随意扫描来历不明的二维码，谨慎使用公共 WIFI、免密 WIFI；
7. 发现个人金融信息泄露风险，要及时联系公安等部门维权。（来源：中国银行保险报）

➢ 网友称拼多多 App 远程删除照片：拼多多称将对产品做改进

2021 年 1 月 12 日报道，有网友上传系列视频，爆出了自己在参与拼多多 App 活动时的遭遇：参加 App 裂变活动，邀请新用户返现一百元，结果钱没拿到，证据截屏还被 App 远程删除。剑指拼多多 App“利用安装时赋予的权限侵犯用户隐私”，手机照片可以删除，用户还有什么隐私可言?”**此事随即引爆社交媒体，#网友称被拼多多 App 远程删除图片#话题冲上热搜第一**。



记者实测发现，在 vivo 手机中，拼多多 App 为操作系统预装，运行时需要用户授予存储权限。但对于具体授予的是读取还是写入权限，并未进行清晰说明。依据 vivo 客服解释，应用在获取权限后，可以针对手机的整个存储目录进行读取或者写入。

网友指责拼多多远程删除用户照片

据爆料网友介绍，其最初是参加拼多多 App 上的“邀请 1 人，直接提现 100 元”的获客活动，但在其成功邀请新用户后，只收到了随机金额的提现优惠，并非广告中所称“提现 100 元”，于是向客服反馈。反馈过程中，该网友曾向客服表示，自己有邀请后的全程录像以及重要截图拍照证据。但让该名网友意想不到的是，自己手机在此之后弹出了提示：“检测到‘拼多多’已删除了相册里的照片或视频”，自己手机中的上述取证照片被删除，出现在“最近删除”的文件夹内。

对此，该名网友认为，是拼多多 App 远程删除了自己手机上的证据照片，并表示拼多

多方面已向其否认删除照片一事，称可以“从经济补偿角度出发，补贴 30 元无门槛代金券”。

拼多多回应称删除文件为“缓存图片”

1 月 12 日晚间 7 时许，拼多多官方博账号就此事发表公开说明，称用户在拼多多 App 客服聊天页面中“拍摄”图片，如在发送前进行了剪裁、美化等编辑动作，会删除 App 在美化前“缓存”在系统相册的图片，“这导致了 vivo 系统认为有删除图片的操作”。

然而，上述回应并未完全平息舆论的相关质疑。在拼多多官方回应的微博下评论区中，有网友直言，被删照片用户的图片为系统截图功能生成，“又不是用拼多多拍照，为什么还能删?”依据爆料网友此前提供的视频内容，vivo 官方客服曾向其解释称，用户允许对应的权限，该软件就可以获取到对应信息。

App 能够远程删除用户数据吗?

作为一款手机 App，拼多多是否能做到远程删除用户手机内的其他软件数据?对于这一关注焦点，多位软件开发业内人士向记者证实，“从技术上可以实现”。

具体到此次事件中，爆料网友将证据视频发给拼多多客服的前提，需要授权拼多多 App 读写手机存储的权限。有了读写权限授权，App 如何找到并删除用户手机内的数据?知乎网友“Nathan”给出了一种猜想路径：客服诱导用户发送所有证据——App 记录用户发送文件路径——客服通过聊天内容判断是否删除用户发送过的文件——如需删除，依据文件路径运用读写权限，实现远程删除文件。“文件访问权限就可以实现远程文件管理，客服通过配套工具可以像查看自己手机相册一样查看用户外部存储空间的所有文件，只是实现起来比较复杂”，“Nathan”说。但同时，也有软件开发业内人士向记者表示，拼多多此次官方回应中提到的删除缓存照片被手机系统检测到的情况也存在可能性，“此次事件中具体是什么原因导致用户数据被删，还需要手机方 vivo 给予详细说明”。即便如此，这种产品设计思路也是对用户隐私的无视。（来源：互联网综合整理）

信息安全意识产品服务

021-33663299