2018

中国数据保护年度报告

元达 | MWE China Law Offices 律师事务所

元达 MWE CHINA DATA CENTER 数据中心 McDERMOTT DISCOVERY

LexisNexis

卷首语

2017 年对于数据保护来说是非凡的一年。数据的价值日益显现，数据正在成为企业内部最为重要的资产。在中国，习近平总书记提出“没有网络安全就没有国家安全”“没有信息化就没有现代化”的重要论断，由此开启了中国网络空间安全治理的顶层设计，网络安全成为国家综合国力提升和安全能力建设工作的重中之重。

数据价值的凸显带来的是与数据相关的争议及危机越来越多，国内外各种数据安全事件频繁登上新闻头条。同时，整个社会的个人信息保护意识也开始觉醒，以往许多司空见惯的侵犯个人信息的行为不断成为“众矢之的”。

《网络安全法》在 2017 年 6 月 1 日的正式生效意味着中国数据保护法律框架初步搭建完成。《网络安全法》生效后，行政部门在数据领域的执法力度也不断加强，因未妥善保护数据而受到处罚的公司日益增多。这些内外部环境的变化为企业的合规经营提出了全新的要求，迫使企业审慎对待数据合规这一全新的课题。数据合规已成为企业合规经营过程中的重要组成部分。

在元达律师事务所与 LexisNexis 律商联讯历时数月联合进行的调研中，我们发现为数众多的企业已经开始积累对数据合规义务的认知，但一个相对普遍的困扰是缺乏连结法律合规及技术现实的启动及运行机制。 同时，我们也注意到越来越多的企业头疼于跨国间的数据合规实践。

作为数据合规领域的先驱与实践者，我们于 2014 年成立的“元达数据中心”已经帮助大量客户开展数据合规工作，解决客户所面临的数据安全风险及法律问题，为合规经营保驾护航。在这样的背景下，将元达在数据合规领域多年积累的经验进行分享，指导行业数据合规工作，共同构建有序的数据利用规则，成为我们义不容辞的责任。

因此，我们联合 LexisNexis 律商联讯共同制作并发布此份《中国数据保护年度报告（2018）》，报告在充分调研的基础上，对中国数据合规所涉监管部门、处罚案例与相关的法规进行梳理，以期为企业在中国高速变化的数字环境下健康发展设立新的标准。

刘晨光 律师

2018 年 2 月 24 日

LexisNexis®

律商联讯是一家全球领先的内容和技术解决方案提供商，帮助法律、企业、税务、政府、学术和非营利性组织的专业人员作出知情决策，实现更好的业务成果。作为数字化先锋，公司率先通过 Lexis® 服务在网上提供法律信息。如今，律商联讯拥有先进的技术和世界一流的内容，帮助专业人士更快、更简便、更有效地工作。通过与客户密切合作，公司确保客户能利用其解决方案降低风险、改善生产力、提高盈利能力、促进业务发展。律商联讯作为服务于各领域专业客户的全球领先信息解决方案提供商—励讯集团（RELX Group PLC ）的旗下公司，向 175 个国家的客户提供服务，全球雇员人数超过 10000 名。

服务中国二十年，我们已经引进多个国际产品落地中国，包括全球最畅销的各类在线数据库，以及享有国际盛誉的进口原版图书，内容覆盖全球 175 个国家的超过 60 亿数据。同时，律商联讯与中国最具实务经验的专家团队合作，依靠自主创新技术及大数据分析，相继开发了律商网和律商实践指引系列产品。我们提供的不再只是查询法律的检索工具，而是贴近法律专业人士的实务工作流程，帮助其处理实务问题、撰写法律文书和高效法律检索的 360 度解决方案。

元达 MWE China Law Offices 律师事务所

元达 MWE CHINA DATA CENTER 数据中心 McDERMOTT DISCOVERY

元达律师事务所（“元达”）是成立于 2007 年的中国律师事务所，总部位于上海，并在北京拥有分所。元达成立同时，与国际知名的 McDermott Will & Emery 律师事务所建立了独家战略合作伙伴关系，这是西方律师事务所首次与一家中国大陆律所建立正式的紧密联营关系。

2014 年元达数据中心也基于此创新的商业模式而建立，并将独有的战略联盟框架和其本土资源与国际资源相结合的特质而受到广泛的关注。该战略联盟模式帮助避免国际律所在中国运营时所受到的限制，尤其是中国境内律师执业方面的限制。同时，战略联盟的形式还使得元达在处理纷繁复杂的国际法律事务时能有效利用其他法域内的强大资源，成功解决本土律所在处理该等事务时所面临的挑战。

作为首批关注数据隐私、数据安全、数据本地储存、数据传输以及受保护信息相关的数据咨询服务律师事务所，元达很早就在该领域深耕和研究，促进该领域法律服务的发展并紧跟客户创新和商业需求的步伐。在这个时刻变化和纷繁复杂的领域，元达通过巧妙的方式、尖端的科技以及对客户内部资源的有效利用，将法律与科技服务有机结合，我们经验丰富的律师也在不断更新和完善我们的方法与路径，与客户一同实现新的解决方案。

目 录

第一部分
调研问卷分析

《网络安全法》的实施，意味着各类公司及事业实体都需要承担相应的网络安全义务，这给数据安全领域的企业合规带来重大挑战。该调研问卷旨在帮助公司及事业实体进行数据合规现状的基本检查与分析，了解和掌握其数据管理现状，并帮助相关公司及事业实体在《网络安全法》框架下对自身数据管理的合规性进行初步评估，为未来的改进奠定基础。

为了解企业数据合规的真实情况，元达律师事务所与 LexisNexis 律商联讯设计并通过多种渠道发放了数万份调研问卷，受访对象的性质包括但不限于国有企业、民营企业、外商独资企业、中外合资企业等，覆盖金融业、制造业、信息服务业、租赁及商务业等行业，基本能够反映出不同性质、领域的公司及事业实体在数据安全合规领域的现状。调研问卷的内容围绕企业数据合规完成的状况展开，主要包括数据合规应对、数据保护以及《网络安全法》框架下网络安全义务的履行情况等。

经过历时数月的调研与分析，本报告发现，为数众多的企业已经开始积累对数据合规义务的认知，但一个相对普遍的困扰是缺乏连结法律合规及技术现实的启动及运行机制。此类困扰也将直接影响到数据合规义务履行的情况。本报告发现，还有大量企业的有关人员并不清楚自身义务的履行情况，或是并未履行法定义务。这会给企业的运营带来巨大的风险，不仅随时有可能发生网络安全事故，更有可能因为未履行义务而被有关部门处罚。因此，企业了解、贯彻数据合规已成为当务之急。

第一章
数据合规应对

1. 法律生效后企业的应对

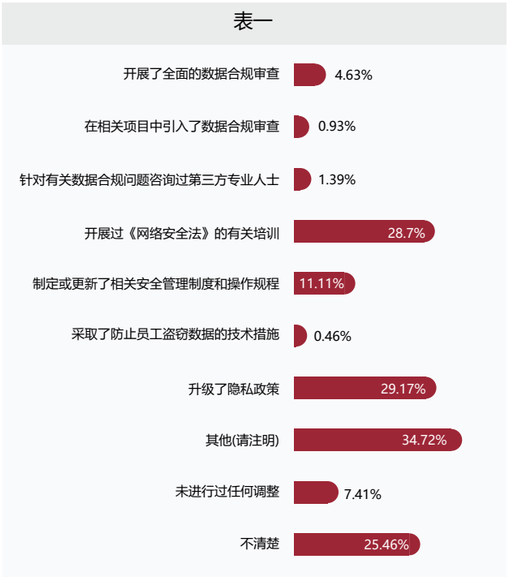
根据《网络安全法》的规定，几乎所有的企业都可以被纳入到网络运营者的范畴，因此企业应当主动采取相关措施，以应对《网络安全法》的生效。为了解在《网络安全法》生效后，企业是否采取对应措施，以及采取了何种对应措施，本报告问卷设置了一系列专项问题，而这也是本报告问卷的调研重点之一。

调研结果（表一）显示：有 25.46% 的受访对象不清楚其所在企业是否进行过调整，有 7.41% 的受访对象明确表示其所在企业没有进行过任何调整。这两部分受访对象共计占 32.87%。这说明，现阶段仍有部分企业的应对措施有待调整与加强。

值得注意的是，在受访对象所在企业已经采取的网络安全措施中，最常见的是开展有关《网络安全法》的相关培训、升级隐私政策，这两项各占大约 30% 左右。也有 11.11% 的企业制定或更新了相关安全管理制度和操作规程。但是，本报告发现，鲜有企业会在相关项目中引入数据合规审查，或者针对有关数据合规问题咨询第三方专业人士，也没有企业采取技术措施防止员工盗窃数据，可见企业在数据合规问题上仍有强化空间。

此外，本报告问卷还调研了企业是否遭遇过网络攻击、发生过数据泄漏事件或因为数据问题遭到过用户投诉。

表一



调研结果（表二）显示：有 26.37% 的企业曾遭遇过威胁网络安全的事件，其中曾感染计算机病毒的企业占比 15.74%，曾遭遇网络瘫痪、发生数据泄漏的企业均占 6% 以上，对是否遭受过网络攻击、遭受过用户投诉等情况，37.04% 的受访对象表示不清楚。

从表二可以看出，在形态多样的网络安全威胁事件中，系统感染计算机病毒是相对而言比较常见的一种情况。本报告建议，网络运营者应提前做好防范计算机病毒的准备。对于其它时发性的危机，诸如网站被篡改、数据被泄露以及网络瘫痪等情况，本报告建议，企业也应当提前做好应急预案，减少这些网络安全威胁所造成的损失。

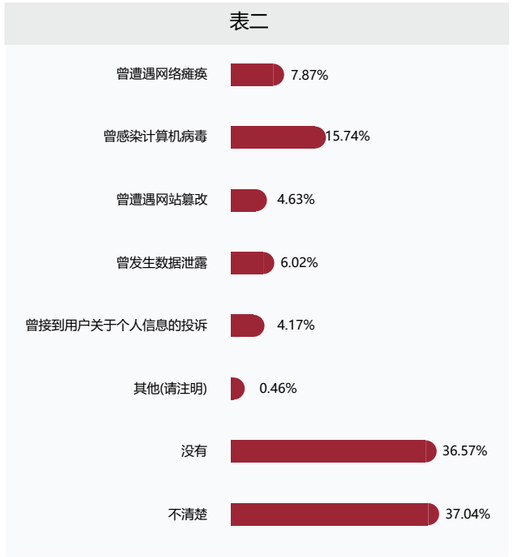
2. 与有关部门的接洽情况

网络安全的主管部门主要为网信部门、公安部门和通信管理部门等，每个部门依据职责分工对网络进行监管。根据《网络安全法》第八条的规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作，国务院电信主管部门、公安部门和其他有关机关在各自职责范围内负责网络安全保护和监督管理工作。因此，企业与有关部门的“接洽情况”，可以在一定程度上反映出现阶段的执法力度，以及有关部门对于网络安全问题的重视程度。

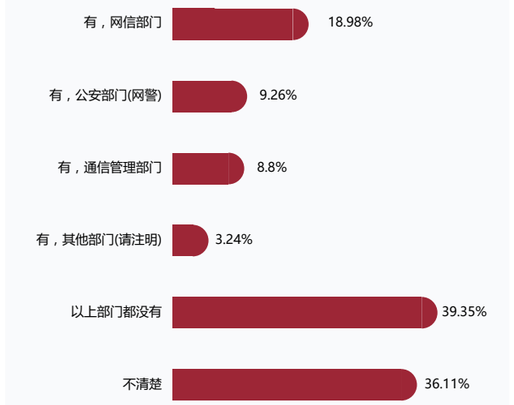
本报告调研了主管部门就网络安全或数据保护问题与受访对象所在企业进行沟通或检查的情况。

调研结果（表三）显示，受访对象所在企业与网信部门进行接洽的情况占比较多，侧面反映出国家网信部门在网络安全监管领域的主导作用。如前文所述，法律法规规定了相关监管部门的职能，涉及不同部门在各个领域、各个行业的具体监管义务，以进行严格的数据保护监督管理。企业与监管部门的沟通，不仅有利于政企双方收集建议与反馈，也利于企业精确地完善合规要求。因此，本报告建议，企业应当主动与网信部门、公安部门以及通讯管理部门等主管部门进行交流，帮助企业合规的不断完善。

表二



表三



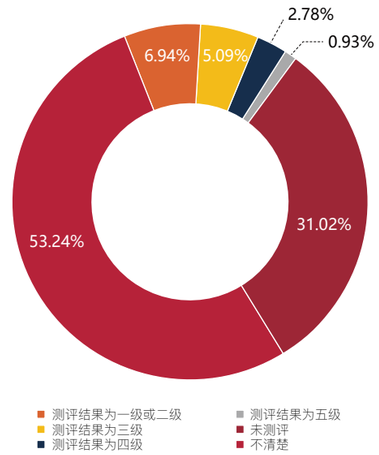
第二章
网络安全基础义务

《网络安全法》中将网络运营者定义为网络的所有者、管理者和网络服务提供者，这意味着所有的企业，只要拥有自己的网站、设立局域网或者管理工业控制系统等，均具有网络运营者的身份。而企业在《网络安全法》下的主体地位也未必单一，有可能既是网络产品、服务提供者，又是网络运营者。除此之外，企业还应当明确自身是否属于关键信息基础设施运营者。在此基础上，才能更清晰地界定企业应当承担的义务。

1. 等级保护测评义务

依据《网络安全法》第二十一条规定的网络安全等级保护制度，企业作为网络运营者，应当履行等级保护测评的义务。本报告问卷设置了专项问题，以调研企业的等级保护测评情况。

图一

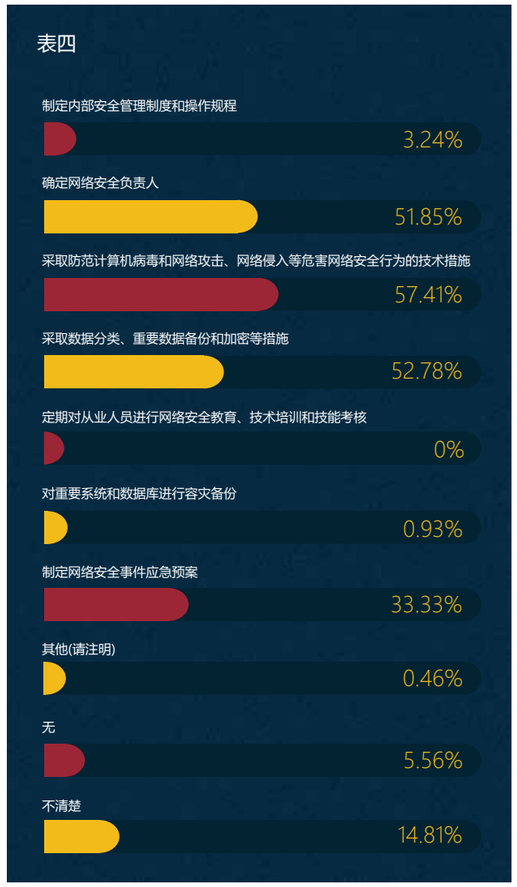


如上，调研结果（图一）显示，没有如实履行该项义务的受访企业占比 31.02%。这反映出一个值得注意的现状，即现阶段仍有部分网络运营者没有意识到定期进行等级测评的重要性。在 2017 年《网络安全法》出台之后，多地都曾发生因未落实网络安全等级保护的等级测评、定级备案工作而被予以行政处罚的案例。[1] 因此，本报告建议，企业可以通过有资质的等级保护测评机构进行认证，或参考关于等级保护测评的国家标准，以落实和加强等级测评工作。

2. 安全保护义务

《网络安全法》第二十一条详细规定了网络运营者应当履行的安全保护义务，包括但不限于：制定内部安全管理制度和操作规程、确定网络安全负责人、采取数据分类加密等措施、制定网络安全事件应急预案等。这些安全义务的履行是企业数据合规的重要内容之一。本报告在受访企业中对上述安全义务的履行状况进行的调研，调研结果见表四。

表四



由于受访企业包括一般的网络运营者与关键信息基础设施运营者，因此本报告将对调研结果分别进行分析。

本报告问卷设置的前四个选项是《网络安全法》规定的一般网络运营者需要履行的义务。本报告发现，如表四所示，3.24% 的受访对象制定了内部的网络安全管理制度和操作规程，该义务履行率极低；50% 左右的受访企业确定了网络安全负责人、采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施以及采取了数据分类、重要数据备份和加密措施。据此，本报告认为，部分企业对于一般网络运营者义务的履行仍不到位，需要采取相应技术措施以降低合规风险。

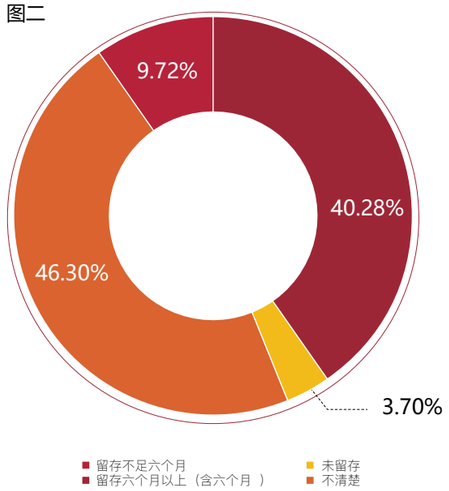
1. 可参见安徽省蚌埠怀远县教师进修学校网站因未落实等级保护制度而被予以行政处罚的案例。

本报告问卷还列举了《网络安全法》中关键信息基础设施运营者应额外履行的义务。根据本报告调研结果，有约三分之二的受访企业的业务可能涉及关键信息基础设施，然而本报告调研结果（表四）显示，企业对关键信息基础设施运营者相应的额外义务缺乏重视：除 33.33% 的受访企业制定了网络安全事件应急预案外，对重要系统和数据库进行容灾备份的企业不足 1%；同时，没有一家受访企业定期对从业人员进行网络安全教育、技术培训和技能考核。本报告认为，这个调研结果反映了现状下关键信息基础设施运营者对于部分义务的忽视，增加了违法的风险。因此，可能涉及关键信息基础设施的企业应全面关注相关义务的履行。

日志留存时限作为《网络安全法》下明确规定但又容易被企业忽视的一项义务，也被纳入本报告问卷的专项问题。根据《网络安全法》的相关规定，网络运营者应当采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关日志不少于六个月。本报告调研结果（图二）表明，切实履行《网络安全法》留存日志义务的企业仅占 40.28%，同时还有近乎半数的受访对象对此表示不清楚。

本报告提醒企业，网络日志对于追溯非法操作、未经授权的访问，并维护网络安全以及调查网络违法犯罪活动具有重要作用。此前虽然已经有一些法律文件对留存日志的时限做了规定，但是从法律位阶的角度来看，应以《网络安全法》的规定为准。因此，本报告建议，法务人员不仅要督促企业履行留存日志的义务，更要严格遵守《网络安全法》中规定的时限。

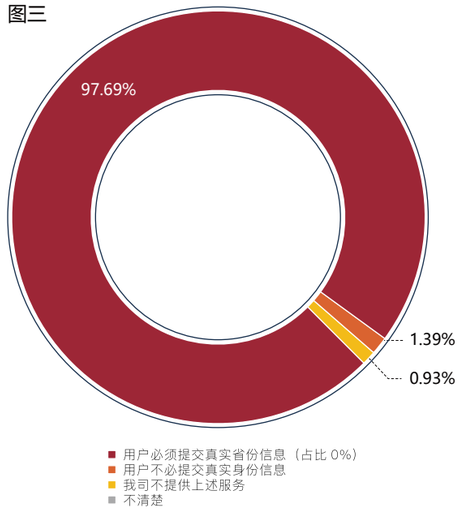
图二



3. 用户信息审核义务

根据《网络安全法》第二十四条，网络经营者在提供网络接入、域名注册、固定电话和移动电话入网手续、信息发布、即时通讯等服务时，应当要求用户提供真实身份信息，否则不予提供相关服务。本报告依据此项义务设置了问题。

图三



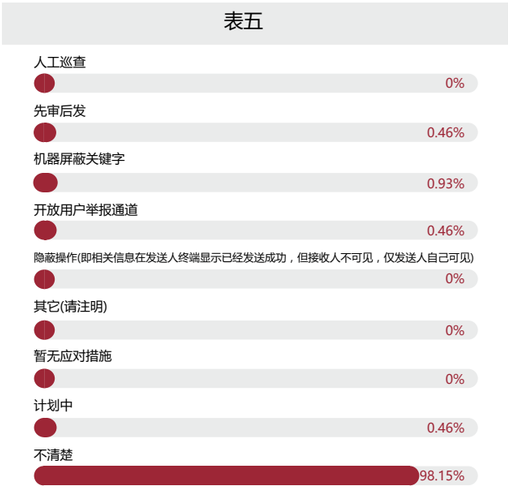
本报告统计（图三）发现，仅有 0.93% 的受访对象明确表示不提供上述服务，而绝大多数受访企业未要求用户必须提交真实信息，或是不清楚该义务的落实情况。可以看出，《网络安全法》中有关用户实名制义务的履行情况并不理想。本报告提醒企业，该义务不仅仅是法律规定的强行性义务，更是自 2012 年全国人大常委会制定《关于加强网络信息保护的决定》时起就一直高度重视的问题。如果企业作为网络经营者在提供上述服务时不能切实履行用户实名制义务，则将面临很高的合规风险。

2. 参见杨合庆主编：《< 中华人民共和国网络安全法 > 解读》，中国法制出版社 2017 年版，第 50 页。

4. 公共信息巡查义务

《网络安全法》第四十七条是关于“网络信息安全”的相关规定，要求网络运营者切实加强对用户发布信息的管理。这种管理的形式应分为第一性的事前义务和第二性的事后义务。本报告调研问卷针对事前义务设置了问题，以期了解企业是否履行针对违法违规信息的事前信息巡查义务。

表五

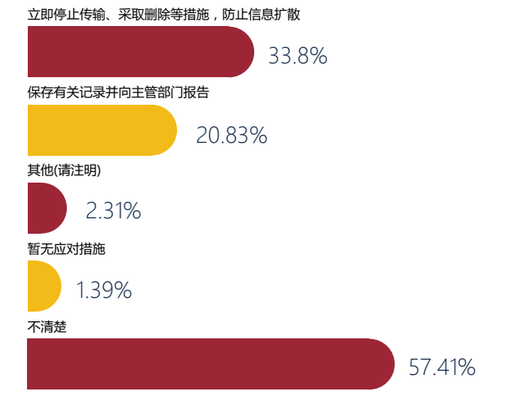


如上表五所见，本问题设置的选项列举了目前网络经营者管理发布信息常用的几个举措，如人工巡查、机器屏蔽关键字等等。然而调研结果（表五）显示，仅有极少数受访企业采取了上述措施。在本报告问卷列举的五项措施中，仅有三项被极少数企业实施，比如，0.46% 的企业采取“先审后发”，0.93% 的企业采取“机器屏蔽关键字”，0.46% 的企业“开放用户举报通道”。其中，企业设立用户举报措施是《网络安全法》第四十九条规定的义务。除此之外，0.46% 的企业处于计划采取应对措施阶段。而 98.15% 的企业却对这些常用应对措施表示不清楚。本报告分析，可能的原因在于：一是本问题中列举的措施实施起来具有较强的技术性，受访对象并不了解；二是企业对《网络安全法》下的信息管理义务落实不到位；三是企业可能对于条款理解不周全，仅考虑违法违规信息出现后的补救措施，而忽略了事前措施。本报告认为，无论何种原因，这个结果都能反映一个现实问题，即企业对违法违规信息处理的应对措施缺乏重视。

5. 违法信息处置义务

承接前述事前义务，本报告问卷设置了关于事后义务的问题，旨在调研企业在管理过程中发现违法违规信息之后的处置措施。同时，为了解该处置措施的落实情况，问卷亦设置了相关问题。

表六



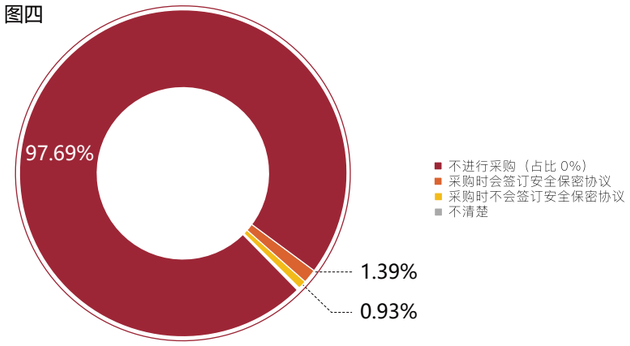
调研结果如表六所示，33.8% 的企业表示发现违法违规信息后会立即停止传输、采取删除等措施，防止信息扩散；20.83% 的企业表示会保存有关记录并向主管部门报告；少数企业会采取其他措施或者无应对措施；仍有 57.41% 的企业对此表示不清楚。

该义务是一项事后义务，在违法违规信息出现之前，企业实际中的普遍做法是“表明”自身会采取这些措施。因此，本报告也建议企业将该项义务纳入数据合规的相关规章制度中，同时也确保在真正面临违法信息时能够有据可依，妥善处理。

6. 第三方安全保密义务

根据《网络安全法》第三十六条，关键信息基础设施运营者在采购网络产品和服务时，应当按照规定与提供者签订安全保密协议。该义务虽然是法律规定要求关键信息基础设施运营者必须履行之义务，但是基于企业合规以及最佳实践考量，以及避免不必要的法律纠纷，本报告建议，每一网络经营者在向第三方采购时，均应签订书面的安全保密协议。为了解安全保密协议签订情况，本报告问卷设置了相关问题。

图四



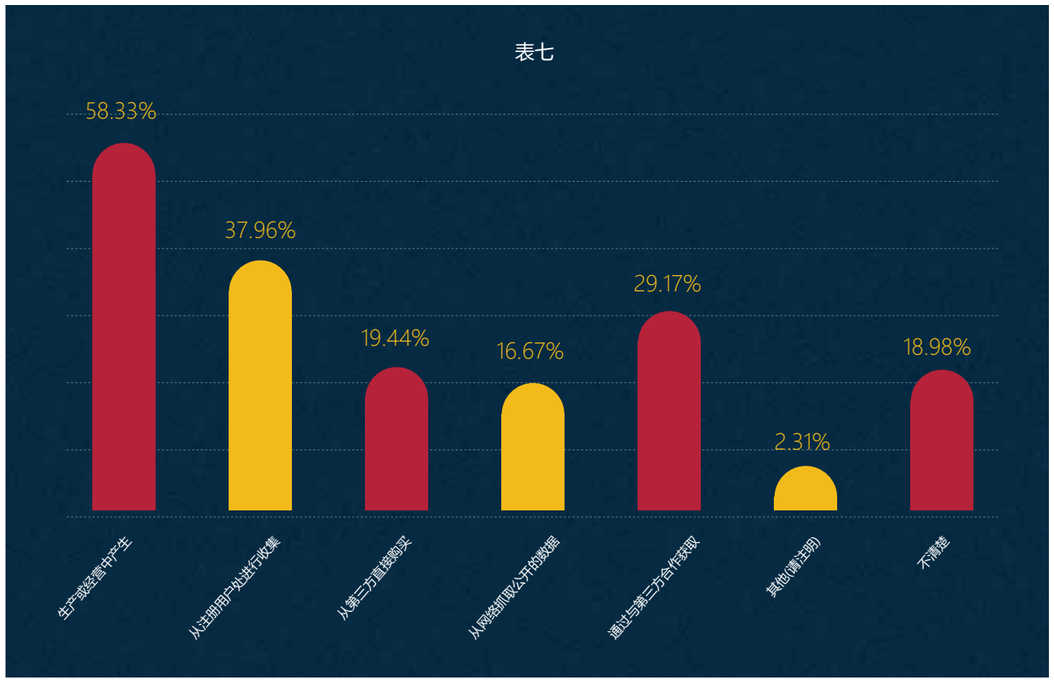
从调研结果（图四）来看，所有企业均存在向第三方采购的情况，但是签订过保密协议的企业仅占 1.39%，而高达 97.69% 的企业对此协议的签订与否表示不清楚。

本报告认为，事实上，向第三方采购可能会增加企业隐私数据泄露的风险，为使采购业务正常推进，同时最大程度保护企业数据安全，签订保密协议来规制第三方行为的做法值得企业借鉴。

第三章
数据保护情况

大数据时代，收集个人信息有助于企业为用户提供更加精准和优质的服务。但是不当收集、使用相关数据会增加企业侵犯个人信息或者不正当竞争的风险。为了解企业运营过程中获取数据的途径，本报告问卷设置了相应问题。

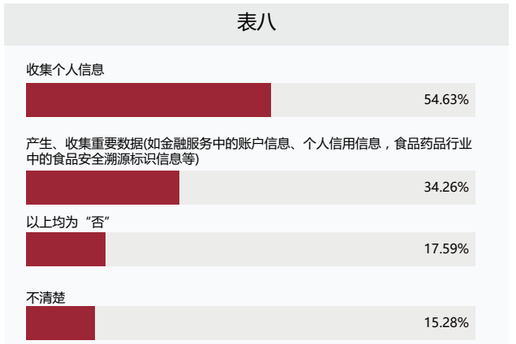
1. 数据收集、利用情况



调研结果如表七显示，每个选项都占有不低的比例，可见企业收集数据的途径是多种多样的。本报告提醒，企业无论以何种途径收集数据，均负有确保其安全的义务。

此外，为了解受访企业在运营过程中是否会收集用户个人信息，或产生、收集重要数据，本报告问卷亦设置了相应的问题。

表八

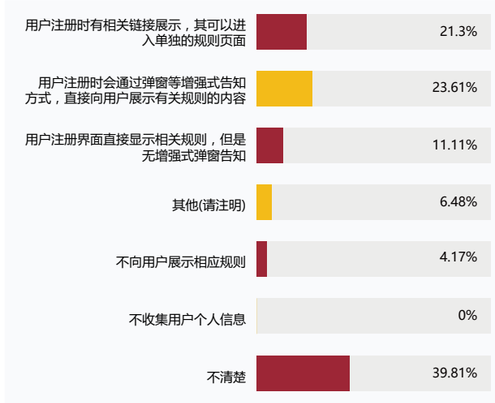


表八调研结果显示，过半数的企业表示会收集用户个人信息；约三分之一的企业表示会产生、收集重要数据；仅有少量企业表示既未收集用户个人信息，也未产生、收集重要数据。

为确认现阶段企业对个人信息的收集是否符合《网络安全法》的规定，本报告问卷还从以下方面设置了相应问题：

第一，企业在收集用户个人信息的过程中，是否向用户展示个人信息收集、使用的规则以及展示的方式。

表九

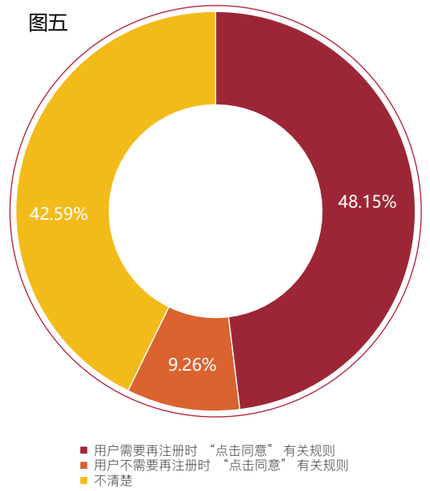


表九调研结果表明，多数企业会采取各种方式向用户展示收集信息的规则。这符合《网络安全法》的相关规定，即网络运营者收集个人信息时应“公开收集、使用规则”。

此外，表九问卷问题还列举了不同的展示方式。仅展示链接等方法可能并不会对用户产生提示，会有一定的合规风险；而“增强式”的告知方式最符合“公开”和“明示”的要求。因此，本报告建议，企业采用“增强式”的告知方式，以避免合规风险。

第二，用户在使用受访企业网站或受访企业提供的网络服务、产品时，是否需要对有关收集、使用其个人信息的相关规则表示同意。本问题旨在了解企业收集、使用用户个人信息是否征得用户同意的情况。

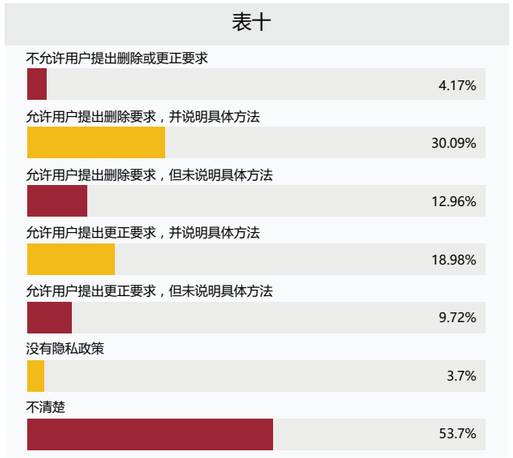
图五



根据《网络安全法》的相关规定，企业在向用户明示个人信息的收集、使用规则之后，仍应当征得用户的同意，这是一个“合意”的过程。本问题的设置即基于此并承接前面的问题。调研结果（图五）显示，仅有半数企业在收集用户个人信息时要求用户“点击同意”。对于未设置“点击同意”步骤的企业，即使企业对规则作了最大化地公开和明示，本报告提醒，不经过同意，其仍不能使用用户的个人信息。因此，本报告建议，相关企业应对以上步骤进行相应的调整，减少合规风险的产生。

在收集和利用个人信息的过程中，企业还应当注意，《网络安全法》第四十三条赋予了用户对其个人信息的删除权和更正权。本报告调研问卷中设置了相应的问题。

表十



本报告调研结果（表十）表明，网络运营者对于用户删除权和更正权的保障并不充分。

有 4.17% 的企业不允许用户删除和更正其个人信息。这显然未保障用户的合法权利。有 43.5% 的受访企业允许用户对个人信息进行删除，28.8% 的受访企业允许用户对个人信息进行更正。这说明部分受访企业或许基于效率考量，仅保障了用户对个人信息的删除权。而《网络安全法》规定用户既享有删除权又享有更正权，因此，本报告认为，部分企业对用户对其个人信息的删除权与更正权保障不充分。

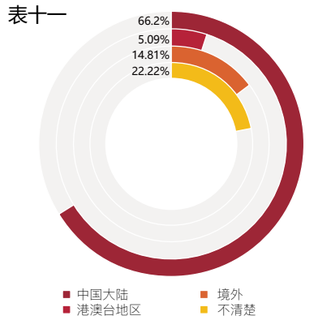
12.96% 的受访企业允许用户对其个人信息提出删除要求，却未告知具体方法；9.72% 的受访企业允许用户提出更正要求，却未告知具体方法。本报告认为，这些做法都阻碍了用户行使《网络安全法》规定的删除权和更正权。本报告建议，企业应该充分保障用户对其个人信息的删除权与更正权，以消除合规风险。

2. 数据跨境传输情况

《网络安全法》对数据的境内存储与跨境传输作出了相应的规定。为了解受访企业的数据境内存储与跨境传输情况，本报告问卷从以下角度对受访企业进行调研：

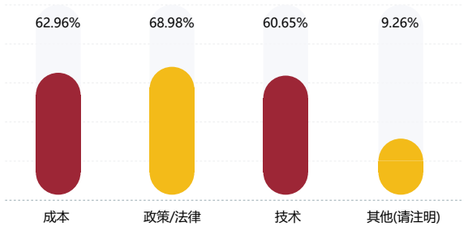
第一，企业在中国境内运营所产生或收集数据的储存地。调研结果（表十一）表明，66.2% 的企业将在中国境内运营所产生或收集的数据储存在中国大陆，14.81% 的企业将其储存在境外。针对这些将数据存储在境外的企业，数据跨境传输产生的法律问题尤为重要。

表十一



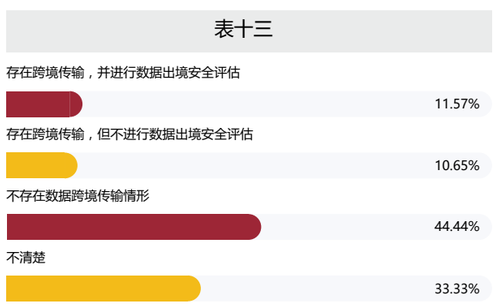
第二，企业选择数据储存地的考虑因素。调研结果（表十二）表明，将成本、政策和法律以及技术因素纳入考虑范畴的企业均超过 60%。由此可见，大部分企业确实将法律法规纳入了考虑范围。本报告建议，另外一小部分企业对于数据境内储存的规范还应加以重视，将成本、技术因素纳入考虑的同时也应考虑是否合乎政策法规，以合法合规为前提开展业务，避免合规风险。

表十二



第三，企业就个人信息和重要数据跨境传输情况。调研结果（表十三）表明，仍有 10.65% 的企业“存在跨境传输，但不进行数据安全出境评估”的情况。本报告建议，数据跨境传输需要数据安全出境评估是《网络安全法》的明确规定，企业应当予以重视。

表十三



第二部分
监管部门概览

我们首先来假设一种情形：一家瑞典企业在上海设立外商投资企业，使用中文面向中国市场在线提供产品（服务），并提供评论产品、服务的功能，且将所有中国用户数据存储在位于欧洲的服务器中。在这样的情况下，欧洲企业不仅需要承担《一般数据保护条例》（GDPR）中欧盟对个人数据保护的义务，还需要面对中国的数据监管压力。在中国该企业的合法合规运营首先需要在工信部门进行备案登记，并且根据具体的业务类型判断是否需要，且能否办理“增值电信业务许可证”。其次，该企业在网站运营 30 天内需要在公安机关进行备案，如果涉及新业务的运营，还需要留意新业务安全评估法规的要求（目前仍是征求意见阶段）。在运营后，公安部门主要负责等级保护等网络运行安全方面的监督管理工作，工信部门主要从互联网牌照、注册用户实名制方面进行监管，网信部门主要针对评论内容、数据本地存储等方面进行监管。除此以外，该企业还需要面对具体行业的监管。

可见，企业在运营过程中有必要处理好与监管部门的关系，在中国对企业数据保护情况进行监管行政部门众多。本报告选取了与数据监管关系最为密切的网信部门、公安部门与工信部门进行分析。三部门的监管范围既存在重合之处，又有明显的区别。因此，企业数据合规需明确不同部门的构架、职责与执法。

第四章
网信部门

1. 部门概况

中央网络安全和信息化领导小组办公室于 2014 年 2 月 27 日成立，旨在提高网络安全和促进信息化战略实施。中央网络安全和信息化领导小组办公室是中央网络安全和信息化领导小组的办事机构，承担具体职责。

国家互联网信息办公室（简称“国家网信办”）是经国务院批准设立的互联网信息监管机构，成立于 2011 年 5 月初。国家互联网信息办公室与中央网络安全和信息化领导小组办公室，是“一个机构，两块牌子”的关系，既是国务院办事机构，也被列入中共中央办事机构序列。[1]

网信部门包括国家网信办与地方网信办。地方网信办分别设立在省（自治区、直辖市）、市、区三级。国家网信办下设：[2]

- 网络评论工作局
- 网络新闻信息传播局
- 网络社会工作局
- 信息化发展局
- 移动网络管理局
- 社会工作局
- 网络安全协调局
- 信息服务管理局
- 国际合作局

在《网络安全法》中，明确列举了网信部门的主要职责：

- 负责统筹协调网络安全工作和相关监督管理工作（第八条）
- 会同其他部门，制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认（第二十三条）
- 会同其他部门，对关键信息基础设施运营者的采购行为进行安全审查（第三十五条）
- 对关键信息基础设施运营者跨境的重要数据与个人信息传输进行评估（第三十七条）
- 统筹关键信息基础设施保护（第三十九条）
- 统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息（第五十一条）
- 协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练（第五十三条）

除《网络安全法》以外，在《测绘法》中也规定县级以上人民政府和测绘地理信息主管部门、网信部门等有关部门应当加强对地图编制、出版、展示、登载和互联网地图服务的监督管理。在《国务院办公厅关于加强旅游市场综合监管的通知》中，网信部门负责依法清理网上虚假旅游信息，查处发布各类误导、欺诈消费者等虚假旅游信息的违法违规网站和账号等。

1 . 中华人民共和国中央人民政府网站（在“国务院办事机构”下可以看到国家互联网信息办公室与中央网络安全和信息化领导小组办公室是一个机构两块牌子的关系，列入中共中央办事机构序列），http://www.gov.cn/guowuyuan/zuzhi.htm，2017 年 10 月 30 日最后一次访问。

2.《中央网络安全和信息化领导小组办公室 2014 年公开选拔处级领导干部工作公告》，http://www.cac.gov.cn/2014-10/28/c_1113794507.htm，2017 年 12 月 13 日最后一次访问。

表十四

职责	法律依据
建立网络安全信息共享机制	《互联网新闻信息服务管理规定》第二十一条 《关键信息基础设施安全保护条例（征求意见稿）》第三十八条
接受个人或组织的举报，并对举报落实情况进行监督检查	《互联网用户公众账号信息服务管理规定》第十五条 《互联网群组信息服务管理规定》第十二条 《个人信息和重要数据出境安全评估办法（征求意见稿）》第十三条
接收网络服务提供者应当提供的备案	《互联网用户公众账号信息服务管理规定》第七条 《互联网群组信息服务管理规定》第七条
受理和决定相关行政许可	《互联网新闻信息服务管理规定》第九条 《互联网新闻信息服务许可管理实施细则》第十一条
建立失信黑名单制度和约谈制度	《互联网新闻信息服务管理规定》第二十一条 《互联网新闻信息服务单位约谈工作规定》第三条、第四条、第五条、第六条、 第七条、第八条

本报告调研结果（本报告第一部分表三）显示，有 18.98% 的受访对象所在企业与网信部门进行过接洽，侧面反映出国家网信部门在网络安全监管领域的主导作用。

尽管《网络安全法》赋予了网信部门统筹协调的权力，但是在《全国人民代表大会常务委员会执法检查组关于检查 < 中华人民共和国网络安全法 >< 全国人民代表大会常务委员会关于加强网络信息保护的决定 > 实施情况的报告》中承认：“网络安全监管‘九龙治水’现象仍然存在，权责不清、各自为战、执法推诿、效率低下等问题尚未有效解决，法律赋予网信部门的统筹协调职能履行不够顺畅。一些地方网络信息安全多头管理问题比较突出，但在发生信息泄露、滥用用户个人信息等信息安全事件后，用户又经常遇到投诉无门、部门之间推诿扯皮的问题。”因此，企业在开展数据合规工作时，需要面对多重监管的局面。

2. 行政权力

2.1 行政处罚

2017 年 6 月 1 日，国家互联网信息办公室制定的《互联网信息内容管理行政执法程序规定》正式施行。规定由网信部门依法实施行政执法，对违反有关互联网信息内容管理法律法规规章的行为实施行政处罚。

根据《互联网信息内容管理行政执法程序规定》，网信部门对互联网信息服务提供者违法行为作出行政处罚决定前，可以根据有关规定对其实施约谈。网信部门的行政处罚结果如果需由电信主管部门关闭网站、吊销互联网信息服务增值电信业务经营许可证或者取消备案的，转电信主管部门处理。

在《网络安全法》生效后，网信部门所进行的行政处罚主要集中在：违反信息内容管理义务、制作传播违法违规信息与缺乏许可备案三个领域，如北京市网信办因为新浪微博对用户发布传播淫秽色情信息、宣扬民族仇恨信息及相关评论信息未尽到管理义务而给予最高额罚款并责令整改，广东省网信办因为腾讯未对微信平台存在用户传播暴力恐怖、虚假谣言、淫秽色情等信息尽到管理义务而给予最高罚款并责令整改。

2.2 行政许可

根据 2017 年 6 月 1 日正式生效的《互联网新闻信息服务管理规定》，通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务，应当取得互联网新闻信息服务许可。截至 2018 年 1 月 30 日，中央互联网新闻信息服务单位共许可互联网站 94 个，应用程序 50 个，论坛 14 个，博客 6 个，微博客 2 个，公众账号 292 个，即时通信工具 1 个，网络直播 3 个，共计 462 个服务项。[3]

根据 2017 年 12 月 1 日正式施行的《互联网新闻信息服务新技术新应用安全评估管理规定》，此安全评估主

3. 中央互联网新闻信息服务单位许可信息（截至 2018 年 1 月 30 日），http://www.cac.gov.cn/2018-01/30/c_1122342261.htm，2018 年 1 月 31 日最后访问。

要是根据新技术新应用的新闻舆论属性、社会动员能力及由此产生的信息内容安全风险确定评估等级，审查评价其信息安全管理制度和技术保障措施的活动。国家网信办负责全国新技术新应用安全评估工作，省、自治区、直辖市互联网信息办公室依据职责负责本行政区域内新技术新应用安全评估工作，并且网信部门可以委托第三方机构承担新技术新应用安全评估的具体实施工作。

2.3 约谈

根据 2015 年生效的《互联网新闻信息服务单位约谈工作规定》，约谈是指国家和地方互联网信息办公室在互联网新闻信息服务单位发生严重违法违规情形时，约见其相关负责人，进行警示谈话、指出问题、责令整改纠正的行政行为。约谈体现了柔性执法的精神。[4]

在 2017 年，全国网信系统全年依法约谈网站 2003 家，暂停更新网站 1370 家，会同电信主管部门取消违法网站许可或备案、关闭违法网站 22587 家，移送司法机关相关案件线索 2045 件。有关网站依据服务协议关闭各类违法违规账号群组 317 万余个。[5]

在 2017 年 12 月 29 日，国家网信办指导北京网信办，针对今日头条、凤凰新闻手机客户端持续传播色情低俗信息、违规提供互联网新闻信息服务等问题，分别约谈两家企业负责人，责令其停止违法违规行为。今日头条手机客户端部分频道暂停更新 24 小时，凤凰新闻手机客户端部分频道暂停更新 12 小时。[6] 因此，互联网新闻信息服务单位应注意做好内容管理的工作。

根据《互联网新闻信息服务单位约谈工作规定》，若互联网新闻信息服务单位未按要求进行整改，将受到警告、罚款、责令停业整顿、吊销许可证等处罚，若被多次约谈依然存在违法行为则将被从重处罚。在 2018 年 1 月底，新浪微博违反国家有关互联网法律法规和管理要求，传播违法违规信息，存在严重导向问题，对网上舆论生态造成恶劣影响。国家互联网信息办公室指导北京市互联网信息办公室约谈新浪微博负责人，责令其立即自查自纠，全面深入整改。新浪微博对问题突出的热搜榜、热门话题榜、微博问答功能、热门微博榜明星和情感版块、广场头条栏目情感版块下线一周进行整改。

第五章
公安部门

1. 部门概况

在网络安全方面，公安部负责“指导、监督地方公安机关对国家机关、社会团体、企事业单位和重点建设工程的治安保卫工作以及群众性治安保卫组织的治安防范工作和公共信息网络的安全监察工作。”[7] 本报告调研结果（本报告第一部分表三）显示，有 9.26% 的受访对象所在企业就网络安全或数据保护问题与公安部门进行过沟通或接受过检查。

根据 2011 年修订的《计算机信息系统安全保护条例》

表十五

网络安全保卫部门层级体系（示例）

国家级	公安部网络安全保卫局
省（直辖市、自治区）级	北京市局网络安全保卫总队 上海市局网络安全保卫总队 江苏省厅网络安全保卫总队 广东省厅网络安全保卫总队
地市级	东城分局网络安全保卫大队 黄浦分局网络安全保卫支队 苏州市局网络安全保卫支队 深圳市局网络安全保卫支队
区县级	姑苏分局网络安全保卫大队 福田分局网络安全保卫大队
派出所	【不设网安保卫部门】

4. 马民虎：《网络安全法使用指南》，中国民主法制出版社 2017 年版，第 228-229 页。

5.“约谈网站 2003 家！ 2017 年全国网信行政执法工作大盘点”，https://mp.weixin.qq.com/s/gSW8eDZy4t07du6UZ7gzRg，2018 年 2 月 5 日最后访问。

6.《北京网信办约谈今日头条、凤凰新闻手机客户端负责人，两家企业将暂停部分频道内容更新》，http://mp.weixin.qq.com/s/KkPLy0uiSZiO4wbvxmL7QA，2018 年 1 月 2 日最后访问。

7. 公安部概况，http://app.mps.gov.cn:9000/gdnps/content.jsp?id=4949776，2017 年 10 月 29 日最后访问。

第十七条，公安机关对计算机信息系统安全保护工作行使下列监督职权：

- 监督、检查、指导计算机信息系统安全保护工作；
- 查处危害计算机信息系统安全的违法犯罪案件；
- 履行计算机信息系统安全保护工作的其他监督职责。

网络安全保卫工作主要由公安部门内设的网络安全保卫部门负责。公安部下设网络安全保卫局，在省、自治区、直辖市一级设立网络安全保卫总队，在地市一级设立网络安全保卫支队，在区县一级设立网络安全保卫大队。

2.1 行政许可和备案

在备案工作方面，全国公安机关互联网安全管理服务平台和中国网络安全等级保护网承担了前文所述的两项重要备案职能，即联网备案和等级保护备案。

2.1.1 联网备案

在 1994 年国务院制定的《计算机信息系统安全保护条例》中，明确公安部主管全国计算机信息系统安全保护工作，条例要求进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

在 1997 年公安部制定的《计算机信息网络国际联网安全保护管理办法》中，明确公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。《管理办法》第十二条要求互联网企业应当自网络正式联通之日起 30 日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

全国公安机关互联网安全管理服务平台是相关网络经营者开办网站和运营 APP 市场等进行备案以及为公众提供查询服务的平台。通过阅读该平台下发的《全国公安机关互联网站安全服务平台备案手册》，目前在公安机关进行的备案将统一在该平台上操作。

备案类型包括网站备案、接入商数据报备和 APP 市场用户备案。根据《备案手册》，非交互式网站初步审核完成后即完成备案，交互式网站需要进行当面审核或实地检查，具体时间将以短信告知。如收到公安机关面审通知，主体应按照短信通知的时间携带所需证件到公安机关进行材料完整性检验；如收到公安机关实地审核通知，主体应按照通知的时间做好准备，配合公安民警进行安全检查。

值得注意的是，公安机关的备案与工信部门的备案并不相同。工信部备案的依据在于国务院颁布的《互联网信息服务管理办法》，其中提到“国家对经营性互联网信息服务实行许可制度；对非经营性[8]互联网信息服务实行备案制度”，在信息服务的范畴下，获得许可即取得 ICP 经营许可证[9]，备案即通过 ICP 备案。ICP 备案将在工信部的“ICP/IP 地址 / 域名信息备案管理系统”中进行。

工信部的 ICP 备案和公安部的备案所填信息几乎一致，唯填写平台和法律依据不同。在现行法律框架下，可以理解为工信部备案是“入场券”，是对网站基本信息在主管部门的一种登记存放，如此才可使网站联通互联网，因此 ICP 备案的审核通常较为宽松；而公安部的备案更加侧重“联通网络后的网络安全”一面，如其备案项目涉及“信息安全负责人”，同时其应在联网之后的 30 日内完成。

2.1.2 等级保护

根据 2011 年修订的《计算机信息系统安全保护条例》，计算机信息系统实行安全等级保护，而具体的实施办法，国务院将其授权给了公安部门制定。此后，公安部制定了表十六中的一系列有关等级保护的规章和规范性文件。

其中，公安部 2007 年 6 月 22 日发布的《信息安全等级保护管理办法》中第三条也规定，由公安机关负责信息安全等级保护工作的监督、检查、指导，同时该办法对于等级保护中各个等级的划分、具体实施和管理方法作了细致的规定。

管理办法第十五条具体规定了等级保护备案的内容。

在等级保护备案的过程中，总的原则是被确定为第二级以上的信息系统才需履行备案义务，而办理机关是设区的市级以上的公安机关。对于等级的确定，一般原则是自主定级，有主管部门的，应当经主管部门审核批准。另外，跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级；对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。

8. 此处对于经营性的判断与企业是否盈利无关，而是指用户能否直接无偿使用网站上显示的信息，一般通常浏览的互联网站均属如此。

9.ICP 经营许可证是我国《电信条例》中规定的《增值电信业务经营许可证》中的一种，一般包括移动信息服务业务经营许可证（SP 经营许可证）、互联网信息服务许可证（ICP 经营许可证）、互联网数据中心经营许可证（IDC 许可证）、互联网接入服务业务经营许可证（ISP 许可证）和呼叫中心经营许可证等。本文中将重点探讨的是 ICP 备案，此处不再做赘述。

表十六

文号	法规名称
公通字[2004]66号	《关于信息安全等级保护工作的实施意见》
公通字[2007]43号	《信息安全等级保护管理办法》
公信安[2007]861号	《关于开展全国重要信息系统安全等级保护定级工作的通知》
公信安[2007]1360号	《信息安全等级保护备案实施细则》
公信安[2008]736号	《公安机关信息安全等级保护检查工作规范》
公信安[2009]1429号	《关于开展信息安全等级保护安全建设整改工作的指导意见》
公信安[2009]1487号	《信息系统安全等级测评报告模版（试行）》
公信安[2014]2866号	《信息安全等级保护测评报告模版（2015年版）》

2.2 行政处罚

行政处罚是公安部门进行网络安全执法的重要权力，根据《网络安全法》，公安部门在网络安全与数据保护领域主要承担以下职责：

- 对从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助的行为进行行政处罚；
- 对窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息的行为进行行政处罚；
- 对设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息的行为进行行政处罚；
- 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果，可以对该机构、组织、个人采取冻结财产或者其他必要的行政强制措施。

2.3 巡查执法

从 2017 年 6 月 1 日起，首批 50 个省市公安机关统一标识为“网警巡查执法”的微博、微信和百度贴吧账号集中上线。[10] 网警巡查执法的职责主要为：公开巡查、警示教育、服务群众、宣传引导、矛盾化解，部分地区的公众号也可以进行在线报案，包括非法集资、传销、电信诈骗等进行举报。[11]

网警巡查执法不仅是处理违法信息，发现严重违法行为时也会及时部署，进行多部门联动。如果接到涉及其他地区的举报，一般情况会与其他地区的网警直接沟通，情节严重的则上报公安部统一部署。公安部首批 50 个官方账号的共同上线，形成了良好的协作机制。

网络犯罪通常是异地或跨区域犯罪，单一警种较难侦破案件，有必要启动全国网警巡查机制。另外，各类网站日常监管存在盲点，一些网络案件的管辖也急需明确，网络违法犯罪行为需要法律定性，在实施调查权、强制权标准和程序方面也需要进一步完善。[12] 协调工信部门加速推进网络实名制将极大有益于网警巡查执法，目前实名制的要求已在《网络安全法》中被规定为一项经营者的强行性义务。

2.4 监督检查

根据国务院于 2011 年 1 月 8 日修订并发布的《计算机信息系统安全保护条例》，第三章“安全监督”中第十七条规定：“公安机关行使下列监督职权，包含监督、检查、指导计算机信息系统安全保护工作。也即除了行政许可、备案、行政处罚和行政强制以外，公安机关在日常的工作中也保持着持续性的监督和检查。”如公安部于 2000 年 4 月 26 日发布的《计算机病毒防治管理办法》第四条明确公安机关主管计算机病毒防治管理工作，这是一项特别的行政管理权力。

可以认为，涉及计算机信息系统和网络安全、利用互联网施行的违法和犯罪行为都是公安机关日常监管的事项。其中比较重要的几项行政监督检查权力如表十七。

表十七

序号	检查事项	法律依据
1	对计算机信息系统安全专用产品销售许可证进行监督检查	《计算机信息系统安全专用产品检测和销售许可证管理办法》第五条
2	对从事国际联网业务的单位和个人进行监督检查	《计算机信息网络国际联网安全保护管理办法》第三章
3	对计算机病毒防治工作进行监督检查	《计算机病毒防治管理办法》第十五条
4	对信息安全等级保护工作进行监督检查	《信息安全等级保护管理办法》第三条
5	对互联网上网服务营业场所信息安全进行监督检查	《互联网上网服务营业场所管理条例》第四条

第六章
工信部门

1. 部门概况

工业与信息化部（简称“工信部”）是主管信息化事务的国务院部门，与其下属的地方主管部门通信管理局和各级经信部门共同承担了保障网络安全的部分职责。本报告调研结果（本报告第一部分表三）显示，有 8.8% 的受访对象所在企业就网络安全或数据保护问题与通信管理部门进行过沟通或接受过检查。

工信部设立于 2008 年“大部制”改革的背景下，根据《工业和信息化部主要职责内设机构和人员编制规定》，国家发展和改革委员会的工业行业管理和信息化有关职责、原国务院信息化工作办公室等部门的有关职责被划给工信部。2015 年，工信部进行有关职责调整，根据《中央编办关于工业和信息化部有关职责和机构调整的通知》，信息化推进、网络信息安全协调等职责被划给国家网信办。调整后，工信部与网络安全相关的职权主要包括负责：

- 电信网、互联网网络与信息安全技术平台的建设和使用管理；
- 负责信息通信领域网络与信息安全保障体系建设；
- 拟定电信网、互联网及工业控制系统网络与信息安全规划、政策、标准并组织实施，加强电信网、互联网及工业控制系统网络安全审查；
- 拟订电信网、互联网数据安全管理政策、规范、标准并组织实施；
- 负责网络安全防护、应急管理和处置。

工信部共有 24 个内设机构，其中主要负责分管网络安全方面事务的有信息通信管理局与网络安全管理局。信息通信管理局的职责主要有：依法对电信和互联网等信息通信服务实行监管，承担互联网（含移动互联网）行业管理职能。[13]

网络安全管理局是工信部的内设机构之一，与数据保护相关的主要职责是：[14]

（一）组织拟订电信网、互联网及其相关网络与信息安全规划、政策和标准并组织实施；

（二）承担电信网、互联网网络与信息安全技术平台的建设和使用管理；

（三）承担电信和互联网行业网络安全审查相关工作，组织推动电信网、互联网安全自主可控工作；承担建立电

10. 参见：《公安部：建立网警常态化公开巡查执法机制 全国首批 50 个省市网警执法账号亮相网络空间》，http://www.cyberpolice.cn/wfjb/html/gzdt/20150531/1649.shtml，于 2017 年 10 月 31 日最后访问。

11. 参见：http://www.360doc.com/content/17/0414/15/39856387_645565648.shtml，于 2017 年 10 月 31 日最后访问。

12. 参见：《全国 50 个省市公安机关 6 月 1 日起启动网警巡查执法机制，有专家和全国人大代表建议一完善立法，为网警巡查执法“助威”》，http://news.163.com/15/0622/07/ASMT1TF400014AEE.html#，于 2017 年 10 月 31 日最后一次访问。

13. 信息通信管理局，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057711/c3607337/content.html，2018 年 1 月 2 日最后访问。

14. 网络安全管理局，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057725/c3635780/content.html，2018 年 1 月 2 日最后访问。

信网、互联网新技术新业务安全评估制度并组织实施；

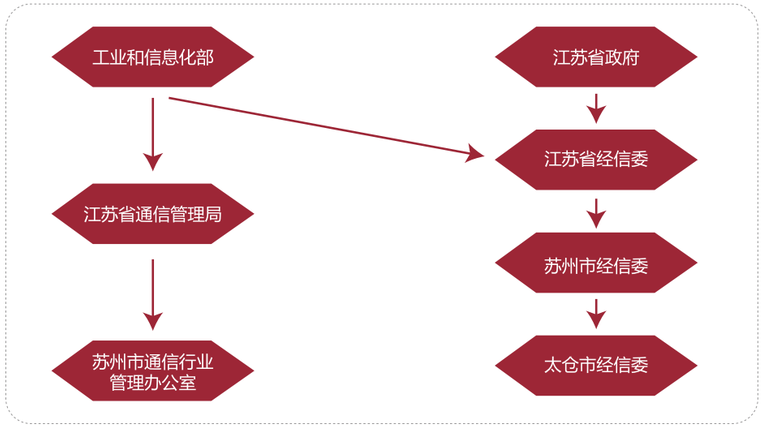
（四）指导督促电信企业和互联网企业落实网络与信息安全管理责任，组织开展网络环境和信息治理，配合处理网上有害信息，配合打击网络犯罪和防范网络失窃密；

（五）拟订电信网、互联网网络安全防护政策并组织实施；

（六）承担电信网、互联网网络与信息安全监测预警、威胁治理、信息通报和应急管理与处置；

（七）承担电信网、互联网网络数据和用户信息安全保护管理工作。

各省（自治区、直辖市）的通信管理局为工信部派驻地方的通信管理部门，实行垂直管理。除此以外，部分省份还在省内地级市成立了通信监管派出机构，如经济与信息化委员会于江苏省省级、市级、区级行政单位均有设立，属同级人民政府的组成部门。



通信管理局是工信部下设的地方管理机构，各个省级单位都设有通信管理局。它是该行政区域内通信行业的主管部门，在工信部的领导下，依照《电信条例》和有关法律法规，对该行政区域内的通信行业实施政府监督管理职能。其内设的主管网络安全的部门包括信息通信管理处、网络安全管理处、互联网管理处等。

经济与信息化委员会，也称“工业与信息化委员会”或“经济与信息化厅”，在省级、市级、区级设置，或与其他部门合并设置，是地方各级人民政府的组成部门，负责工业、软件和信息服务业发展，推进信息化工作。

以北京市经信委为例，北京市经信委负责贯彻执行国家关于工业、软件和信息服务业、信息化方面的法律、法规、规章和政策，起草本市相关地方性法规草案、政府规章草案，并组织实施。承担北京市网络与信息安全管理责任；负责协调维护信息安全和信息安全保障体系建设；指导监督政府部门、重点行业的重要信息系统与基础信息系统的安全保障工作；协调处理网络与信息安全的重大事件；承担北京市通信保障和信息安全应急指挥部的具体工作。其中设信息安全协调处、网络安全管理处等部门。

2. 行政权力

2.1 网络实名及其他

在网络实名制落实方面，2016 年 11 月至 12 月，工信部网络安全管理局曾针对虚拟运营商实名制落实情况进行抽查暗访，由工信部电话用户真实身份信息登记工作领导小组办公室下发整改通知，对存在违规行为的虚拟运营商通报批评，并组织对违规行为严重的远特通信、天音通信进行约谈，要求相关企业立即进行整改，并要求对相关责任部门、责任人、违规网点进行严肃处理。[15]

工信部也曾对电信行业数据安全和用户个人信息保护进行检查，具体体现为全面检查被抽查企业数据安全管理、防范外部攻击和内部人员违规获取数据、安全审计和定级备案等方面制度措施的落实情况。要求相关企业立即进行整改，督促企业落实安全责任；对于违反行政管理要求的，依法予以行政处罚；对于涉嫌犯罪的，移交司法机关处理。

2.2 行政许可

2.2.1 互联网信息服务许可与备案

根据《国务院互联网信息服务管理办法》（国务院 292 号令）的第三条规定，“经营性互联网信息服务”是指通过互联网向上网用户有偿提供信息或者网页制作等服务活动。“非经营性互联网信息服务”是指通过互联网向上网用户无偿提供具有公开性、共享性信息的服务活动。

根据本办法，经营性互联网信息服务许可以及非经营性互联网信息服务备案均由省级通信管理局负责。经营性互联网信息服务许可以及非经营性互联网信息服务备案的依据为本办法第四条、第七条、第八条；互联网电子公告服务专项审批和备案为本办法第九条的要求。

2.2.2 新业务审批

2017 年 6 月 8 日，工信部发布《互联网新业务安全评估管理办法（征求意见稿）》，就企业开展互联网新业务需要进行的安全评估活动公开征求意见。在该征求意见稿中，只要电信业务经营者开展新的在线业务，就需要进行安全评估。而电信业务的范围非常宽泛，尤其是在《电信业务分类目录》B25 类“信息服务业务”下，囊括了绝大多数的互联网服务类型，而且因为电信管理机构负责网站备案，所以会涉及能否顺利备案问题。

安全评估涉及以下内容：

- 用户个人信息保护
- 网络信息安全
- 网络安全防护
- 管理制度
- 身份认证
- 落实责任
- 远程访问安全

2017 年 3 月，工信部发布《关于做好 2017 年互联网新技术新业务安全评估重点工作的通知》，就互联网新技术新业务安全评估提出六大重点工作任务，以切实维护人民群众的合法权益。

2.3 工业控制系统安全管理

工业控制系统运用数字通信和网络技术，基于网络运行，《网络安全法》中“网络”的范围非常宽泛，工业领域中使用的“工业控制系统”也被纳入了网络的范围，对工业控制系统的保护同样适用《网络安全法》。[16]

2016 年 10 月，工业和信息化部印发《工业控制系统信息安全防护指南》，面向工业企业，从以下几方面，对其提出了 30 项工控安全防护要求：

- 安全软件选择与管理
- 安全监测和应急预案演练
- 配置和补丁管理
- 资产安全
- 边界安全防护
- 数据安全
- 物理和环境安全防护
- 供应链管理

后在 2017 年 8 月 11 日，工信部印发了《工业控制系统信息安全防护能力评估工作管理办法》，提出设立全国工控安全防护能力评估专家委员会，负责提供建议与咨询；设立全国工控安全防护能力评估工作组，具体负责管理工控安全防护能力评估相关工作，工作组下设秘书处，秘书处设在国家工业信息安全发展研究中心。

2.4 行政处罚

2017 年 9 月，广东省通信管理局根据《网络安全法》等有关规定，连续依法查处了广州荔支网络技术有限公司、深圳市三人网络科技有限公司、广州市动景计算机科技有限公司、阿里云计算有限公司等四家互联网企业违反《网络安全法》案件，率先开启了通信行业主管部门依据《网络安全法》行政执法新的一页。[17]

广东省通信管理局的处罚涉及不同的义务，其处罚的行为主要是：

- 用户利用平台发布和传播违法有害信息未立即停止传输，防止信息扩散，保存有关记录并向主管部门报告；
- 未要求用户提供真实身份信息提供网络电话服务，存在被利用于从事信息通信诈骗活动的安全隐患；
- 网络产品服务存在安全缺陷和漏洞风险，未能及时全面检测和修补，被用于传播违法有害信息，造成不良影响；
- 企业为用户提供网络接入服务未落实真实身份信息登记和网站备案相关要求，导致用户假冒其他机构名义获取网站备案主体资格。

可见，工信部门的执法涵盖了《网络安全法》主要的两项义务分类即网络运行和信息安全义务。在执法时，除了以《网络安全法》为依据，还依据了《互联网信息服务管理办法》、《电话用户真实身份信息登记规定》等法律法规。

15. 工信部组织对虚拟运营商实名制落实情况进行抽查暗访，http://www.cac.gov.cn/2017-02/08/c_1120428853.htm，2018 年 1 月 30 日最后访问。

16. 杨合庆：《中华人民共和国网络安全法释义》，中国民主法制出版社 2017 年版，页 151。

17. 广东省通信管理局《网络安全法》执法率先出手，https://www.gdca.gov.cn/gdcmsnet/gdcms/content/staticView?path=/54/3103.html，2018 年 1 月 30 日最后访问。

第三部分
案件与争议

网络安全不仅对企业的正常运用至关重要，更关乎社会稳定与国家安全，在《网络安全法》生效后，有关部门依据《网络安全法》频频开展执法活动，打击未履行网络安全义务的行为。

随着数据价值的日益提升，与数据有关的纠纷也越来越多。对数据相关案件、纠纷的研究，有助于企业在法规尚不完善的情况下了解数据收集利用的规则，提前进行应对，也有助于企业了解执法与司法裁判的尺度，更好地帮助企业在激烈的市场竞争中规避法律风险。

近年来，侵犯公民个人信息的事件时有发生，所有人都深受信息被泄露、滥用的困扰。公众的个人信息安全意识不断增强，公安部门也将打击个人信息泄露问题作为重点工作之一。因此，个人信息保护成为了一个需要企业严肃对待的问题。而企业间围绕数据的诉讼更是会直接影响到运营模式能否维系，是企业经营不可回避的问题。

有关部门的执法活动对企业的运营同样影响重大，尽管罚款的额度并不算高，也主要以“约谈”为主，但这些执法措施通常会伴随着产品（服务）的暂停运营进行整改，这无疑会对企业的运营以及用户体验造成巨大影响。尤其是在中国，某些特殊时期，一些身处敏感行业的企业，在被约谈后如果未能对网络安全管理制度进行整改，造成违法信息大量传播、用户信息泄露、刑事案件证据灭失等危害国家利益或社会公众利益的严重后果，甚至可能需要承担刑事责任。除此以外，企业还有必要采取措施，防止破坏计算机信息系统、金融系统等关键系统或危害国家安全、领土完整等敏感信息出现在自己所管理的网络空间内，避免引起不必要的社会或政府关注。

第七章
行政处罚案件

在 2017 年 6 月 1 日《网络安全法》生效后，根据公开新闻报道，有关部门援引《网络安全法》处理涉及数据保护及网络安全相关的行政执法案件有 44 起，见表十八。这些案件可以分为违反网络运行安全义务和违反网络信息安全义务两大类。

违反网络运行安全义务的案件可以进一步分为四种类型：网络运营者未履行网络安全保护义务，未履行身份验证义务，网络产品、服务不符合国家标准强制性要求，从事危害网络安全的活动或者为此提供支持。

表十八

类别	《网络安全法》规定的义务		案例数量	合计	
网络运行安全	网络安全保护义务	采取防范计算机病毒和网络攻击等危害网络安全行为的技术措施	7	20	44
		采取监测、记录网络运行状态等技术措施，留存日志不少于6个月	4		
		其他网络安全保护义务	2		
		身份验证义务	4		
	网络产品、服务符合相关国家标准的强制性要求（针对网络产品、服务提供者）		1		
	不得从事危害网络安全的活动或提供支持		2		
网络信息安全	不得发布或者传输违法信息		24	24	

1. 网络运行安全

网络运行安全是《网络安全法》中的一项重要制度，以网络安全等级保护为基础，还包括身份验证义务，设立应急预案制度。关键信息基础设施保护业务也是网络运行安全的重要组成部分。

2017 年，违反网络运行安全义务的行政处罚案件共计 20 起。本报告对案件按照以下分类进行分析：未履行网络安全保护义务，未履行身份验证义务，网络产品、服务未符合国家标准强制性要求，从事或支持危害网络安全的活动。

对危害网络运行安全的行为，主要的执法部门为公安部门与通信管理部门。公安部门不仅负责等级保护工作，还负责监督、检查、指导计算机信息系统安全保护工作。工信部门的执法不仅针对违反网络运行安全义务的行为，也针对违反网络信息安全义务的行为，涵盖了《网络安全法》主要的两项义务分类。在执法时，除了以《网络安全法》为依据，还依据了《互联网信息服务管理办法》、《电话用户真实身份信息登记规定》等法律法规。

1.1 案件概况

1.1.1 未履行网络安全保护义务

在《网络安全法》中，网络运行安全的基础是网络安全等级保护制度。调研结果（本报告第一部分图一）显示，有 84.26% 的企业不清楚或未进行登记保护测评。

目前，网络安全等级保护制度只见于 1994 年国务院制定的《计算机信息系统安全保护条例》与 2007 年公安部等部门制定的《信息安全等级保护管理办法的规定》。由于《网络安全法》的实施，等级保护相关规定正在进行修订，以期与《网络安全法》配套。

表十九

处罚时间	处罚机关	处罚对象	违法行为	处罚结果
2017.6	忻州市、县两级公安机关网安部门	山西忻州市某省事业单位	存在SQL注入漏洞，严重威胁网站信息安全	警告 责令其改正
2017.7	重庆市公安局网安总队	重庆市首页科技发展有限公司	在提供网络服务过程中，未依法留存用户登录网络 日志	警告 责令限期十五日内进行整改
2017.7.20	汕头网警	汕头市某信息科技有限公司	2016年至检查日未按规定定期开展等级测评	警告 责令改正
2017.7.22	宜宾网安部门	宜宾市翠屏区“教师发展平台”网站	网络安全防护工作落实不到位，导致网站存在高危 漏洞，造成网站发生被黑客攻击入侵	处一万元罚款 对法人代表处五千元罚款
2017.8.12	蚌埠市公安局网安支队	蚌埠怀远县教师进修学校	自上线运行以来，始终未进行网络安全等级保护的 定级备案、等级测评等工作	处以一万五千元罚款 对副校长处以五千元罚款 该学校的法定代表人兼怀远县人民政府分管副县长被 约谈
2017.8.24	吴忠市公安局	宁夏某集团吴忠分公司	未确定网络安全责任人、信息系统未采取防范计算 机病毒和网络侵入等危害网络安全的技术措施；采取 监测、记录网络运行状态、网络安全事件的技术措施 留存日志最长为一个月，低于不少于六个月的规定	警告 责令限期整改
2017.8.30	哈尔滨市公安局网安支队	方正县农业技术推广中心	其设立的“方正农业社会化服务平台”遭受黑客攻击 入侵	责令立即整改 罚款二万元

2017.9	银川市兴庆分局网安大队	宁夏一家电话服务平台	自运行以来，未履行网络安全保护义务、未落实网 络安全保护责任、堡垒机运维日志未达到六个月日志 留存规定、操作系统登录口令复杂度不符合要求	警告 责令限期整改
2017.9.14	当阳网警	当阳某网络信息公司	未对整个网络采取检测、记录网络运行状态、网络 安全事件的技术措施，且未按规定留存相关网络日志 不少于六个月	给予警告处罚
2017.9.28	淮南市公安局网安支队	淮南职业技术学院	系统存在高危漏洞，系统存储的4000余名学生身 份信息已经造成泄露	警告 责令立即整改
2017.10.11	修武县公安局网警大队	修武县某电厂	未履行安全保护义务，未对网络安全负责人进行安 全背景审查	警告 责令限期整改
2017.10.17	合肥市公安局高新分局	辖区内一家单位的门户网站	被植入木马病毒	警告

1.1.2 未履行身份验证义务

《网络安全法》第 24 条对网络用户的身份管理进行了规定，明确网络运营者在与用户签订协议或确认服务时，要求用户提供真实身份信息。该项义务实际上是网络实名制的体现。在 2012 年 12 月底全国人大常委会制定的《关于加强网络信息保护的决定》中，就对网络实名制进行了要求。后在工信部制定的《互联网用户账号名称管理规定》与国家网信办制定的《互联网用户账号名称管理规定》中，都要求适用用户实名登记。

表二十

处罚时间	处罚机关	处罚对象	违法行为	处罚结果
2017.8	北京市网信办	BOSS直聘	违规为未提供真实身份信息的用户提供了信息发布服务；未采取有效措施对用户发布传输的信息进行严格管理，导致违法违规信息扩散	下达行政执法检查记录 责令立即整改
2017.9	广东省通信管理局	深圳市三人网络科技有限公司	提供网络电话服务，未要求用户提供真实身份信息，存在被利用于从事信息通信诈骗活动的安全隐患	责令立即整改 罚款五万元 责令停业整顿 关闭网站
2017.9	广东省通信管理局	阿里云计算有限公司	为用户提供网络接入服务未落实真实身份信息登记和网站备案相关要求，导致用户假冒其他机构名义获取网站备案主体资格	责令立即整改
2017.10.4	三亚市吉阳区网警支队	“格雷电竞”网吧以及郭某、陈某	未落实网吧实名制登记上网规定，接受未成年人提供虚假身份证件上网	对“格雷电竞”网吧处以警告并罚款九千五百元 对郭某处以罚款两百元 对陈某处以警告并罚款两百元

1.1.3 网络产品、服务未符合相关国家标准的强制性要求

《网络安全法》第 22 条要求网络产品和服务的提供者应当保证产品和服务安全，符合国家标准的强制要求，一旦发现存在漏洞会安全隐患，需要立即采取补救措施，并及时告知用户并向有关部门报告。

表二十一

处罚时间	2017.9
处罚机关	广东省通信管理局
处罚对象	广州市动景计算机科技有限公司
违法行为	该公司提供的UC浏览器智能云加速产品服务存在安全缺陷和漏洞风险，未能及时全面检测和修补，已被用于传播违法有害信息，造成不良影响
处罚结果	责令立即整改

1.1.4 从事或支持危害网络安全的活动义务

《网络安全法》第 27 条要求任何个人和组织不得从事或支持危害网络安全的活动。

表二十二

处罚时间	2017.8.21	2017.10.23
处罚机关	南京浦口警方	象州县公安局
处罚对象	嫌疑人赵某	嫌疑人覃某
违法行为	未经国家相关部门批准，租用境外服务器非法架设网络“翻墙”工具，并在网络上贩卖“翻墙”服务，非法获利1080元	通过微信及QQ等即时通讯工具在网上买卖家庭摄像头账号、密码，并通过账号、密码侵入他人家庭摄像头偷看他人生活视频，涉及隐私，影响恶劣
处罚结果	行政拘留三日 没收违法所得	行政拘留十五日 没收违法所得

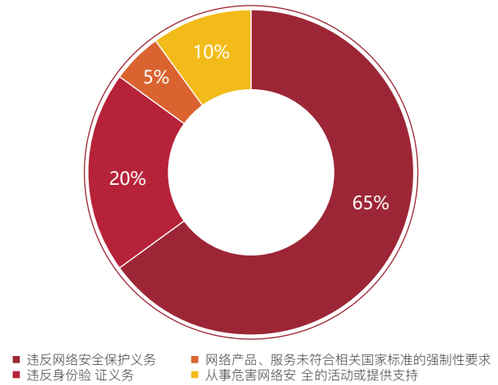
1.2 案例分析

本报告发现，在违反网络运行安全义务的案例（见表十九）中，单位或企业违反网络安全保护义务的情形占比最大，约为总数的 65%。

违反身份验证义务的单位或企业（见表二十）占比 20%。身份验证义务是网络运营者在为用户办理入网手续或者提供即时通讯等服务的情况下，与用户签订协议或者确认提供服务时，应当要求用户提供真实的身份信息。只有满足该条件，网络运营者才能为其提供相关服务。

此外，网络产品、服务未符合相关国家标准的强制性要求的单位或企业占总数的 5%；从事危害网络安全的活动或提供支持的单位或企业占总数的 10%。

1.2.1 网络安全保护义务



A. 采取防范危害网络安全行为的技术措施义务

在涉及网络安全保护义务的执法案例中，企业或单位因没有采取防范计算机病毒和网络攻击等危害网络安全行为的技术措施而遭遇处罚的，在本报告以上整理的违反网络安全保护义务的案件当中，占近一半的比例。

其中较引人注目的是淮南职业技术学院四千余名学生身份信息遭到泄漏一案。[1] 淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码口令存在问题。学院既没有落实网络安全管理制度，也没有建立网络安全防护技术措施，更没有采取数据分类、重要数据备份和加密措施，致使系统内存储的四千多名学生的身份信息泄漏。

1. 参见：《国内首例高校违法案例诞生，因为落实等保制度致学生信息泄漏》，https://mp.weixin.qq.com/s/9K4eSK7m_2unWYApUO8ZcA，2017 年 11 月 23 日最后一次访问

针对教育行业网络安全问题，教育部网络安全与信息化领导小组已于 2017 年 2 月 20 日下发了《关于印发教育部网络安全和信息化领导小组第二次会议会议纪要的通知》，强调要加快推进网络安全等级保护工作。教育部网络安全与信息化领导小组对于教育行业的网络安全综合治理给予了高度的重视。

另外，安徽省蚌埠市怀远县教师进修学校也发生过该类事件。由于学校网站自上线以来始终没有进行过网络安全等级保护的定级备案、等级测评等工作，被黑客入侵。最终，蚌埠市公安局网安支队依法对网络运营单位怀远县教师进修学校处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。该学校的法定代表人与怀远县人民政府分管副县长也被相关部门约谈。这起案例的特殊性在于，最终涉及到的责任人员不仅包括直接责任人，还包括行业主管领导。

以上案例虽然均发生在教育行业，但对于其他行业而言，同样需要以此为警示，完善针对计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，落实网络安全等级保护的定级备案、等级保护工作。

B. 监测、记录网络运行状态义务

在上表的案例汇总中，未履行网络安全保护义务的案件共有 13 起，其中没有按照规定监测、记录网络运行状态以及留存日志的案例占 4 起。

湖北省宜昌市当阳县警方对当阳某网络信息公司予以行政处罚，该公司既没有对整个网络采取检测、记录网络运行状态、网络安全事件的技术措施，也没有按照规定对相关网络日志留存达六个月，并且该公司将租用的网络 IP 地址私自分配给多个单位使用，未履行网络安全监管义务，造成网络管理混乱。

另一起案件是宁夏一家电话服务平台的堡垒机运维日志不符合六个月以上的日志留存规定，因而被当地的网安大队给予警告处罚，并被责令限期整改。

这两起案件都涉及到网络信息公司以及电话服务平台，涉及大量的数据收集工作，一旦被恶意利用，所造成的影响将难以预估。

C. 其他网络安全保护义务

2017 年 7 月 20 日，汕头网警对汕头市某信息科技有限公司进行警告处罚，原因是该公司于 2015 年 11 月向公安机关报备的信息系统安全等级为第三级，经测评合格后投入使用，但是自此之后至 2016 年至检查当日，该公司直都没有按照规定再次开展定期等级测评。

定期开展测评也属于《网络安全法》下规定的义务，根据《信息安全等级保护管理办法》，对于信息系统安全保护等级为第三级的信息系统，应当在每年进行不少于一次的等级测评。

此外，还有一起电站厂未对网络安全负责人进行安全背景审查而被处罚的案件。2017 年 10 月 11 日，河南省焦作市修武县公安局网警大队在对某电厂日常安全检查中发现，该电厂未履行安全保护义务，未对网络安全负责人进行安全背景审查，因此给予该企业责令限期整改，警告处罚。[2] 由于该电厂属于关键信息基础设施运营者，因此除了应履行网络运营者的一般义务之外，还应当履行额外的安全保护义务，例如应当设置专门安全管理机构和安全管理负责人，并对该负责人予以安全背景审查，同时应当注意定期对从业人员进行网络安全教育、技术培训和技能考核，对重要系统进行容灾备份，制定网络安全事件应急预案并定期进行演练等。

1.2.2 身份验证义务

调研结果（本报告第一部分图三）显示，有 97.69% 的企业网络用户实名制的履行情况，具有较大的提升空间。在本报告收录的案例中，涉及未履行身份验证义务的案例共有 4 起。在其中涉及身份验证义务的 3 起案例中，包括北京网信办对“BOSS 直聘”相关人员进行约谈，责令其进行整改一案。该案较其他两起案件而言，具有较为广泛的社会影响力。

“BOSS 直聘”之所以引起广泛关注是因为李文星事件：该事件中，东北大学毕业生李文星通过“BOSS 直聘”求职，却因深陷传销组织而死。北京市网信办认为，“BOSS 直聘”在为用户提供信息发布服务的过程中，为没有提供真实身份信息的用户提供信息发布服务，没有采取有效措施对用户发布传输的信息进行严格管理，导致违法违规信息扩散。因此，北京市网信办对“BOSS 直聘”相关人员进行了约谈。约谈之后，“BOSS 直聘”官方发出道歉信表示，自李文星事件发生以来，公司采取了相应紧急措施，

2. 修武县公安局网警大队查处全县首例违反《网络安全法》案件，https://mp.weixin.qq.com/s/bdimQxyNGc2GVAyr-qHGbA，2018 年 1 月 2 日最后访问。

过去所有未经过“机器 + 人工”审核认证的招聘者，只要再次进行招聘，需要重新进行核验。

1.2.3 网络产品、服务应当符合相关国家标准的强制性要求

在本报告收录的案例中，违反该义务的仅有一案，即广东通信管理局查实：广东动景计算机科技有限公司所提供的 UC 浏览器智能云加速产品服务存在安全缺陷和漏洞风险，未能及时全面检测和修补，被用于传播违法有害信息，造成不良影响。

《网络安全法》规定了网络产品、服务应当符合相关国家标准的强制性要求。广东通信管理局依据该规定，责令该公司立即整改，采取补救措施，并要求其开展通信网络安全防护风险评估，建立新业务上线前安全评估机制和已上线业务定期核查机制，对已上线网络产品服务进行全面检查，排除安全风险隐患，避免类似事件再次发生。网络产品和服务的安全缺陷、漏洞等，由于技术等原因在所难免，但是安全缺陷、漏洞出现时，如未能及时修补而被不法分子加以利用，则会导致不良后果的发生。因此企业应当定期检测、排查网络产品和服务可能存在的安全缺陷和漏洞风险，并及时采取补救措施，排除隐患。

1.2.4 不得从事危害网络安全的活动或者为其提供支持

涉及违反该项义务的 2 起案例，其处罚对象均为自然人，行政机关所做出的行政处罚也多为行政拘留加没收违法所得。

其中一起案例涉及通过微信及 QQ 等即时通讯工具买卖家庭摄像头账号、密码，并通过账号、密码侵入他人家庭摄像头偷看他人生活视频，涉嫌侵犯公民隐私，影响恶劣。另一起案件是未经国家相关部门批准，租用境外服务器非法架设网络“翻墙”工具，并在网络上贩卖“翻墙”服务，以非法获利。

《网络安全法》规定了任何个人和组织都不得从事非法入侵他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动，也不得提供专门从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序和工具。显然，以上两起案例均严重违反所述规定。

2. 网络信息安全

网络信息安全所涉及的义务主要规定于《网络安全法》的第四章，而关于网络信息安全的行政执法案例主要集中在信息内容管理。《网络安全法》规定了网络运营者不仅对自身的行为负有相应义务，对其平台上的用户发布的信息也负有管理义务。

2.1 行政处罚案例

表二十三

处罚时间	处罚机关	处罚对象	违法行为	处罚结果
2017.7	铜陵市公安局网安支队	网民金某	因对公安机关处置某案件不满，多次在微信群中转发、传播不实信息和谣言，并煽动和组织他人参加非法集会，造成恶劣的社会影响	行政拘留十日
2017.8	海南省网信办	天涯社区 凯迪网络网站	存在用户传播淫秽色情、低俗媚俗等信息，未尽到管理义务	严厉批评 限期整改
2017.8	宿城公安分局网安大队	江苏宿迁市华睿科技有限公司	服务器内接入一违法网站，涉及法律、行政法规禁止传输的信息	警告 立即整改
2017.8	浙江省网信办	淘宝网	其店铺售卖破坏计算机信息系统工具、违禁管制物品，贩卖非法 VPN 工具、网络帐号，未尽到管理义务	警告 整改下架违法违规商品，对违法违规店铺进行严肃处理
		同花顺金融网 配音秀网	存在导向不正、低俗恶搞等信息，未尽到管理义务	责令整改 暂停有关系统运行，追究有关人员责任
		蘑菇街互动网 虾米音乐网	存在违法违规帐号注册等问题	责令整改 暂停新用户注册 7 天
2017.8	广东省网信办	腾讯微信	其平台存在用户传播暴力恐怖、虚假谣言、淫秽色情等信息，未尽到管理义务	最高罚款 责令整改
2017.9	北京市网信办	新浪微博	对其用户发布传播淫秽色情信息、宣扬民族仇恨信息及相关评论信息未尽到管理义务	最高罚款 责令整改
2017.9.8	宁夏中卫市公安局网安支队 沙坡头分局网安中队	天天网	未对网民发布的信息进行审核，导致该交互式网站出现大量违法信息	警告
2017.11	湖北荆州市公安县公安局网安大队 舆控中队 县网信办	男子喻某	在微信群里传播交通事故谣言，且造成不良影响	训诫教育 加入黑名单 将面临信用等级降低、管理权限暂停、建群资格取消等后果
2017.10.20	湖北孝感市汉川网警	“城市中国汉川”论坛	出现 20 余条违法信息，审核不严格，未及时进行消除	警告 限期整改
2017.10.25	湖北孝感市云梦县网安大队	云梦房网	网站存在用户发布的赌博链接 2 条，未尽到管理义务	警告 限期整改
2017.11	上海市网警	“K歌达人”APP	APP 及运营网站未对委托其发布的信息内容进行审核，导致违法信息出现	停机整顿六个月
2017.11	莆田市荔城公安分局网安大队	福建某文化传媒有限公司	“莆田某论坛”运行机制未符合相关规定，网站长时间出现大量关于赌博的违法信息，未及时发现处理，并未按规定向公安机关报告	警告 立即整改
2017.11	咸阳市网信办	微信公众号 “直播咸阳” “掌上咸阳”	其发布虚假不实信息，在网上大范围传播，虽事后进行了删除，但已造成不良社会影响	停止更新 10 天 限期整改 若整改不力或出现反复，将依法依规进一步严肃查处
		微信公众号“乾县逗事” “微淳化”	其发布虚假不实信息，在网上大范围传播，虽事后进行了删除，但已造成不良社会影响	约谈 停止更新 7 天、限期整改 整改完毕经网信部门验收合格后方可恢复运营

在网信部门处罚案件中（表二十三），比较引人注意的是 2 起企业被处以最高罚款的案例，分别由北京市网信办对新浪微博和广东省网信办对腾讯公司做出。其原因是：新浪微博上存在用户发布的淫秽色情信息、宣扬民族仇恨信息及相关评论，新浪微博对其平台用户发布的法律法规禁止发布的信息未尽到管理义务；腾讯微信平台存在用户传播暴力恐怖、虚假谣言、淫秽色情等信息，微信对其平台用户发布的法律法规禁止发布的信息未尽到管理义务。北京市网信办和广东省网信办对这两家企业做出了最高罚款的行政处罚，并且责令其深入整改。相比于大企业受到的严重处罚，还有一些存在类似问题的网站可能由于规模较小、情节较轻，受到的处罚也相对轻微。天涯社区、凯迪网络网站被海南省网信办查明存在用户传播淫秽色情、低俗媚俗等信息，网站未尽到管理义务，仅受到批评并被要求限期整改。

通过现有的案例可以看出，很多处罚都是网安部门在日常工作或日常巡查中发现的。在网安部门的 8 起处罚案例中，除了 2 起公民传播不实信息的案件之外，其余 6 起都是对于企业未尽信息内容管理义务的处罚。

云梦房网、“城市中国汉川”论坛、天天网、福建某文化传媒有限公司、江苏宿迁市华睿科技有限公司都是因为其网站存在违法违规信息而未尽到管理义务受到所在地公安局网安大队的警告处罚。“K 歌达人”APP 被上海市网警在日常工作中发现，APP 及运营网站未对委托其发布的信息内容进行审核，导致违法信息出现。

除此之外，还有 2 起公民在微信群中转发、传播不实信息和谣言，造成不良影响从而受到处罚的案例，分别被训诫教育并加入黑名单和被处以行政拘留十日的行政处罚。

2.2 约谈案例

约谈制度规定于《互联网新闻信息服务单位约谈工作规定》第二条：“国家互联网信息办公室、地方互联网信息办公室建立互联网新闻信息服务单位约谈制度。本规定所称约谈，是指国家互联网信息办公室、地方互联网信息办公室在互联网新闻信息服务单位发生严重违法违规情形时，约见其相关负责人，进行警示谈话、指出问题、责令整改纠正的行政行为。”约谈是柔性执法的体现。表二十四是 5 起约谈案例。

表二十四

约谈时间	行政机关	约谈对象	约谈事由
2017.8	湖南省网信办 长沙、常德等网信部门	楼盘网、易读天涯网、协众图片网、牛游戏网、凤舞爱读网、搜白度盘网、他乡家乡人网	普遍存在对信息发布审核把关不严、日常管理不到位等问题
2017.10.15	天津市网信办 河北区网信办	龙之声科技发展有限公司	网站用户长期发布违法违规信息，未进行严格管理，导致违法违规信息扩散
2017.7.21	北京市网信办 北京市规划国土委	58同城 赶集网 闲鱼	均存在违法违规发布“大棚房”租售的信息
2017.11	张家界市网信办 张家界市市委统战部 张家界市市公安局 张家界市市工商局 张家界市市文化市场综合执法局	网络用户“米米七月”	违规制作、发布、传播内容低俗媚俗庸俗视频，擅自在网上开展直播服务，没有按照规定在市委网信办登记备案
		微信公众号“今日张家界”	违规转载发布低俗媚俗庸俗内容视频，不具备互联网新闻信息服务许可，违规转载时政类新闻
		微信公众号“张家界大庸妹儿”	违规转载发布低俗媚俗、血腥视频和图片，违规转载时政类新闻，违规开展网络投票，未落实跟帖评论管理主体责任
2017.12.29	北京市网信办	今日头条 凤凰新闻手机客户端	传播色情低俗信息、违规提供互联网新闻信息服务等问题

从表二十四可以看出，在网络信息安全部分，实践中处罚最多的案件，仍然集中在网站的信息内容管理方面，后果主要集中在约谈、警告、罚款和责令整改方面。网络运营者应该提高对这一部分法律规定的认识，加强对其用户发布的信息的管理；发现法律、行政法规禁止发布或者传输的信息，立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。另外，任何个人和企业都应当遵守互联网信息服务的规定要求，避免在网络上发布传播不实信息等违法违规内容。

第八章
民事案件

随着数据价值的提升，围绕着数据使用所产生的纠纷也开始频频出现。本报告挑选了在 2017 年具有代表性的数据相关案例，为企业在面对数据纠纷时提供参考。

1. 庞理鹏诉东方航空、趣拿公司案

1.1 案情基本信息

案件名称	庞理鹏与北京趣拿信息技术有限公司等隐私权纠纷
案号	（2017）京 01 民终 509 号（二审） （2015）海民初字第 10634 号（一审）
审理法院	北京市海淀区人民法院（一审） 北京市第一中级人民法院（二审）
案由	隐私权纠纷
原审原告（上诉人）	庞理鹏
原审被告（被上诉人）	北京趣拿信息技术有限公司（去哪儿网）； 中国东方航空股份有限公司
法院判决	一、北京趣拿信息技术有限公司于本判决生效后十日内在其官方网站（www.qunar.com）首页以公告形式向庞理鹏赔礼道歉，赔礼道歉公告的持续时间为连续三天； 二、中国东方航空股份有限公司于本判决生效后十日内在其官方网站（www.ceair.com）首页以公告形式向庞理鹏赔礼道歉，赔礼道歉公告的持续时间为连续三天。

1.2 案情简介

2014 年 10 月 11 日，鲁超受庞理鹏的委托在去哪儿网（北京趣拿信息技术有限公司，以下简称“趣拿公司”）上为其购买中国东方航空股份有限公司（以下简称“东方航空”）的机票一张（2014 年 10 月 14 日 MU5492 泸州至北京），并预留自己的手机号码，全程并未提交过庞理鹏的手机号码。当日稍晚，鲁超手机收到去哪儿网发来的出票短信和防诈骗短信各一条。10 月 13 日，庞理鹏的手机收到短信称该航班因故取消，鲁超手机未收到类似短信，鲁超遂与东方航空联系，发现该短信为诈骗短信，并与东方航空分别确认了鲁超与庞理鹏的手机号码。10 月 14 日当天，庞理鹏收到东方航空发来的该航班延误的短信三条，后又得知该航班因故取消。

庞理鹏向一审法院起诉，认为东方航空和趣拿公司泄露其隐私信息（姓名、手机号码、行程安排），侵犯其人身权利。趣拿公司认为，机票实际上是从代理商处购买，自己作为交易平台在此过程中从未接触过庞理鹏手机号码，且已经向鲁超发送了防诈骗短信。代理商出具书面意见称，在此过程中，自己仅知道鲁超手机号，从未接触过庞理鹏手机号。而东方航空公司称，在此过程中，自己仅知道代理商电话，从未接触过庞理鹏手机号，并且称，该订票信息储存于订票服务系统中航信，而非东航系统中。

一审法院认为，庞理鹏提供的证据不足，无法证明两家公司在此案过程中接触过其手机号码，进而无法证明两家公司将其隐私信息泄露，判决驳回庞理鹏的诉讼请求。庞理鹏不服提起上诉，二审法院认为，庞理鹏作为一名普通人，举证证明对方公司内部事务能力有限；现存事实中，庞理鹏通过去哪儿网从东方航空买票，且东方航空和去哪儿网存有庞理鹏手机号码（虽无法证明是通过本案过程获得的，但不排除是庞理鹏之前购票时所留存的手机号码）。两项事实证明，庞理鹏的隐私信息有高度可能性是由趣拿公司和东方航空匹配并泄露的。并且，趣拿公司和东方航空在信息安全管理方面存在疏于防范的过错，应当承担侵权责任，判决东方航空和趣拿公司向庞理鹏赔礼道歉。

1.3 争议焦点

本案与网络安全密切相关的争议焦点有二：

・本案中，庞理鹏的姓名、电话号码及行程安排等事项是否属于法律保护的隐私信息；

・在东方航空和趣拿公司有高度可能泄露庞理鹏隐私信息的情况下，其对于信息的泄露是否具有过错。

首先，本案中庞理鹏的姓名、电话号码及行程安排等事项是否属于法律保护的隐私信息。东方航空在二审中提出，姓名、手机号码以及行程安排是运输合同中的内容，不属于个人隐私。然而，本案中的信息不是被孤立地泄露，而是在相互匹配的状况下一同被泄露。在数据时代的背景下，姓名、手机号码、行程安排这一类的数据和信息一旦被收集和匹配，很可能可以得出关于一个人的详细资料。如果此类信息都被泄露公开，则个人将毫无隐私可言。因而，这些信息应当是属于受到法律保护的个人隐私。本案的二审法院也支持这一点：“根据《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第十二条的界定，自然人基因信息、病历资

料、健康检查资料、犯罪记录、家庭住址、私人活动等是属于隐私信息的。据此，庞理鹏被泄露的上述诸信息中，其行程安排无疑属于私人活动信息，从而应该属于隐私信息，可以通过本案的隐私权纠纷主张救济。”

其次，在东方航空和趣拿公司极有可能泄露庞理鹏隐私信息的情况下，对于信息的泄露是否具有过错。本案为一般侵权责任纠纷，适用过错责任原则，所以即使东方航空和趣拿公司有泄露信息的高度可能性，其是否应该承担责任也需取决于其对于信息的泄露是否存在过错。本案中，东方航空和趣拿公司因为其性质均掌握大量的用户个人信息，这使其更加负有保护这些信息免于泄露的责任和义务。从消费者保护的角度来讲，《消费者权益保护法》第二十九条第二款规定：“经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。”东方航空和趣拿公司并未做到防止消费者个人信息泄露、丢失，从这一点上来讲，两家公司对于信息的泄露具有过错。

1.4 启示

除了前述争议焦点外，本案中还有一些问题值得我们思考：

第一，在鲁超购买了机票之后，趣拿公司虽然向鲁超发送了提醒短信，提醒用户提高警惕，谨防诈骗，但是法院并未考虑这一部分因素，趣拿公司不因为此条提醒短信而免责。发送此提醒短信并不意味着趣拿公司尽到了其保护用户信息不被泄露的义务。

第二，法院最终认定，趣拿公司和东方航空具有泄露庞理鹏信息的高度可能性，其中考量了 2014 年间趣拿公司和东方航空因为涉嫌泄露乘客隐私见诸报端的事件。无论是否属实，法院确实在衡量证据的时候考虑了这一部分因素。

第三，东方航空称自己所用的系统是由中航信提供的，因此中航信也掌握庞理鹏的隐私信息，很有可能此次信息的泄露是由中航信造成的。但是法院认为，无论是中航信与东方航空同时泄露，还是只有中航信一方泄露，东方航空都可以成为适格被告。

第四，一审法院认为，庞理鹏提供的证据不足以证明东方航空和趣拿公司在本案发生的过程中接触到了庞理鹏的手机号码，遑论泄露。但二审法院能够改判，一个关键点就在于，二审法院认为庞理鹏作为一个普通人，能够举证证明企业内部事务的能力十分有限，不能要求其证明两家公司在本案发生的过程中接触到了其手机号码。现有证据已经足够证明两家公司存有其手机号码，虽然有可能只是庞理鹏在以前买票时留下的，但两家公司确实有能力将庞理鹏的手机号码和其此次出行安排相匹配，而庞理鹏又确实通过趣拿公司在东方航空购买了机票，两家公司有能力获知庞理鹏此次出行安排。在排除了庞理鹏恶意诉讼以及其他人刚好同时知晓其姓名、手机号码、航班信息等的小概率事件之后，法院认为现有证据已经可以证明两家公司具有泄露庞理鹏信息的高度可能性。从中我们可以看出，法院在判决的时候充分考虑了普通人举证企业内部事务的困难性。

最后，庞理鹏诉趣拿公司和东方航空一案最终以二审改判，庞理鹏胜诉告终。趣拿公司和东方航空被判向庞理鹏赔礼道歉。本报告调研结果（本报告第一部分表八）显示，有 54.63% 的企业会在经营中收集用户个人信息。但近些年来，企业泄露用户个人信息而被起诉的案件屡见不鲜，此案是少数最终胜诉的案件之一。本案庞理鹏能够胜诉的根本原因还是在于东方航空和趣拿公司没有尽到对用户个人信息的保护义务。企业为合理规避这一部分风险，应建立健全用户信息保护制度，尽到足够的预防义务，有效防止用户信息的泄露。

2. 新浪微博诉脉脉案

2.1 案件基本信息

案件名称	北京微梦创科网络技术有限公司与北京淘友天下技术有限公司等不正当竞争案
案号	(2016) 京 73 民终 588 号（二审） (2015) 海民 (知) 初字第 12602 号（一审）
审理法院	北京知识产权法院（二审） 北京市海淀区人民法院（一审）
案由	不正当竞争纠纷
原审原告（上诉人）	北京微梦创科网络技术有限公司
原审被告（被上诉人）	北京淘友天下技术有限公司； 北京淘友天下科技发展公司

法院判决	一、北京淘友天下技术有限公 司、北京淘友天下 科技发展有限公司停止涉案不正当竞争行为 二、北京淘友天下技术有限公 司、北京淘友天下 科技发展有限公司共同在脉脉网 站（网 址为 www.maimai.cn）首页，脉脉客 户端软件首页连 续四十八小时刊登声 明，就本案不正当竞争行为为 北京微梦创科网络技术公司消除影响； 三、北京淘友天下技术有限公 司、北京淘友天下 科技发展有限公司共同赔偿北京微梦创科网络技术 公司经济损失两百万元及合理费用二十万八千九百 九十八元

2.2 案情简介

北京微梦创科网络技术有限公司是新浪微博的运营者。北京淘友天下技术有限公司、北京淘友天下科技发展公司经营的脉脉软件是一款基于移动端的人脉社交应用软件，通过分析用户的微博和通讯录数据，帮助用户发现新的朋友，并且可以使他们建立联系。

2014 年 8 月，微博方面发现，在脉脉产品内，大量非脉脉用户直接显示有微博用户头像、名称、职业和教育等信息，而且在从未通过微博登录脉脉的情况下，脉脉上仍能够搜索到用户的微博个人信息。

脉脉方面表示，其与微博合作期间，用户使用手机号或微博帐号注册脉脉，需要上传个人手机通讯录联系人，脉脉账号的一度人脉来自脉脉用户的手机通讯录联系人和新浪微博好友，二度人脉为一度人脉用户的手机通讯录联系人和微博好友；与微博方面合作结束后，用户只能通过手机号注册登录，一度人脉仅是脉脉用户的手机通讯录联系人，并不包括微博用户。

后来双方终止合作，但是非脉脉用户的微博用户信息并没有在合理的时间内被删除。微博方面据此对脉脉提起诉讼，认为其非法抓取、使用微博用户信息。

微博方面认为脉脉存在四项不正当竞争行为：

一、非法抓取、使用新浪微博用户职业、教育等信息；

二、非法获取并使用脉脉注册用户手机通讯录联系人与新浪微博用户的对应关系；

三、模仿新浪微博加 V 认证机制及展现方式；

四、发表言论诋毁微梦公司商誉。

2016 年 4 月，北京市海淀区人民法院一审结案，认定脉脉非法抓取、使用新浪微博用户信息等行为构成不正当竞争。此后，脉脉提起上诉。2016 年 12 月 30 日，北京知识产权法院做出终审判决，驳回上诉，维持原判。

2.3 争议焦点

该案中涉及到数据保护方面的争议焦点主要有三个：一是脉脉方面与微博方面是否存在竞争关系；二是脉脉方面获取、使用微博用户信息的行为是否构成不正当竞争；三是脉脉方面获取、使用脉脉用户手机通讯录联系人与微博用户对应关系的行为是否构成不正当竞争。

针对争议焦点一，一审法院认为，双方在对相关用户社交类信息的使用等方面存在竞争利益，具有竞争关系。二审法院同时予以认可。

针对争议焦点二，二审法院根据举证责任分配规则，推定脉脉方面通过 Open API 方式获取微博用户的职业信息、教育信息。一审法院对于脉脉方面获取职业信息、教育信息的技术手段没有查明，就直接认定“不论二被告采取何种技术措施，都能认定二被告在双方合作期间存在抓取涉案新浪微博用户职业信息、教育信息的行为”不妥，二审予以纠正，原因在于：

首先，二审法院分析认为，Open API（开放应用编程接口）开发合作模式是在互联网环境下实现数据信息资源共享的新途径；

其次，按照相关法律规定，网络服务提供者收集、利用用户信息应当遵循合法、正当、必要的原则并经被收集者同意。所以，Open API 开发合作模式中数据提供方向第三方开放数据的前提是数据提供方取得用户同意，同时，第三方平台在使用用户信息时还应当明确告知用户其使用的目的、方式和范围，再次取得用户的同意。

因此，在 Open API 开发合作模式中，第三方通过 Open API 获取用户信息时应坚持“用户授权”+“平台授权”+“用户授权”的三重授权原则。

本案中，脉脉方并没有基于《开发者协议》在取得用户同意的情况下读取非脉脉用户的新浪微博信息，没有充分尊重《开发者协议》的内容，未能尊重用户的知情权及自由选择权，一定程度上破坏了 Open API 合作开发模式。

二审法院认为，脉脉方获取新浪微博信息的行为存在主观过错，违背了在 Open API 开发合作模式中的三重授权原则，违反了诚实信用原则和互联网中的商业道德，故脉脉方获取并利用微博用户信息的行为不具有正当性。

针对争议焦点三，首先，二审法院根据证据举证规则的适用，推定脉脉方在获取手机通讯录联系人与微博信息对应关系时存在通过手机号码、其他类似手机号码的用户

精准信息进行匹配的行为；

其次，根据这一事实，二审法院分析了脉脉方展示用户通讯录联系人与新浪微博用户之间的对应关系的行为构成不正当竞争的原因，包括：

第一，脉脉通过用户上传手机通讯录展示非脉脉用户的微博信息，损害了非脉脉用户的知情权和选择权，违反了诚实信用原则和公认的商业道德；

第二，脉脉方所展示的用户通讯录联系人手机号与新浪微博账号的对应关系并不属于行业惯例。脉脉表示新浪微博、微信、人脉通、得脉等其他应用软件也展示了手机通讯录与应用软件之间的对应关系，但从公证书的内容来看，新浪微博、微信、人脉通、得脉软件中展示的对应关系是手机通讯录与其自身软件注册的关系，而并非展示手机通讯录与其他应用软件之间的对应关系。因此，现有证据不能证明脉脉方展示的对应关系符合行业惯例；

第三，脉脉获取并展示对应关系的行为损害了公平的市场竞争秩序，同时，一定程度上损害了微博的竞争利益。

2.4 启示

二审法院在认定脉脉方获取、使用微博用户信息的行为是否构成不正当竞争行时，关键一点在于，在 Open API 开发合作模式中，数据提供方向第三方开放数据时有无取得用户同意；同时，第三方平台在使用用户信息时，还应当明确告知用户其使用的目的、方式和范围，再次取得用户的同意。

在本案中，微博方作为网络平台提供方，脉脉方作为第三方应用，应当遵守双方签订的《开发者协议》，在读取和运用用户数据时，以“用户同意”+“平台同意”+“用户同意”的三重同意为原则，以保护用户的隐私权、知情权和选择权为底线，以公平、诚信为行为准则，实现数据经济的合作共赢。

有鉴于此，本报告建议：第一，对于那些没有得到授权便抓取网络平台提供方以及他人合法拥有的数据信息的行为，企业可以通过反不正当竞争的路径来应对；第二，第三方应用通过开放平台，例如 Open API 来获取用户信息时，应当坚持三重授权原则；第三，第三方应用与数据提供方之间进行共享用户数据的合作时，必须订立书面协议，防止处于相对优势地位的互联网经营者的非诚信经营带来损失。

3. 乐动卓越诉阿里云案

3.1 案件基本信息

案件名称	阿里云计算有限公司与北京乐动卓越科技有限公司侵害作品信息网络传播权纠纷案
案号	一审判决书案号无法检索，本案仍在二审阶段
审理法院	北京市石景山区人民法院（一审）
案由	侵害作品信息网络传播权纠纷
原审原告（上诉人）	阿里云计算有限公司（“阿里云”）
原审被告（被上诉人）	北京乐动卓越科技有限公司（“乐动卓越”）
法院判决	（一审）根据《中华人民共和国侵权责任法》第三十六条之规定，阿里云侵害了乐动卓越公司对涉案游戏的信息网络传播权，判决阿里云赔偿乐动卓越经济损失 250000 元及诉讼合理支出 11240 元。

3.2 案情简介

乐动卓越系手游《我叫 MT online》和《我叫 MT2》的权利人。2015 年 8 月乐动卓越接到玩家投诉称：域名为 www.callmt.com 的网站提供的名为《我叫 MT 畅爽版》的游戏在游戏图标、人物形象、游戏界面、游戏规则、游戏中的文字等方面与《我叫 MT online》完全相同。乐动卓越无法查询到该网站经营人的相关信息，但通过网络封包分析软件，检测出《我叫 MT 畅爽版》的游戏内容存储服务器的 IP 地址属于阿里云服务。随后在 2015 年 10 月 10 日和 30 日，乐动卓越曾两次发函致阿里云，要求删除侵权游戏，并提供云服务租赁人联系方式。在未获回应的情况下，乐动卓越认为阿里云的行为构成共同侵权，诉至北京市石景山区人民法院，要求判令阿里云断开链接，停止为涉案侵权游戏继续提供服务器租赁服务，将储存在其服务器上的游戏数据库信息提供给乐动卓越，并赔偿经济损失共计 100 万元。

一审法院认为，阿里云作为服务器提供商，虽然其不具有事先审查被租用的服务器中存储内容是否侵权的义务，但在他人重大利益因其提供的网络服务而受到损害时，其作为服务器服务的提供者，应当承担其应尽的义务，采取必要的、合理的、适当的措施积极配合权利人的维权行为，防止权利人的损失持续扩大。因此综观全案事实，阿里云对此应当承担相应的法律责任，法院遂判决阿里云赔偿乐动卓越经济损失 250000 元及诉讼合理支出 11240 元。

阿里云不服向北京知识产权法院提起上诉，目前本案尚在二审阶段。

3.3 争议焦点

本案的争议焦点主要可归纳为：（1）阿里云所提供网络服务的性质认定；（2）阿里云是否有义务采取措施；（3）阿里云在本案中是否要承担民事责任。

首先，按照法院援引的《信息网络传播权保护条例》的规定，阿里云落入了其第十四条中“网络服务提供者”的范畴。根据条例规定，提供信息存储空间或者提供搜索、链接服务可以被视作提供网络服务。显然，法院认为其是一种“信息存储空间”，进而将其界定为“网络服务提供者”。

其次，对于网络服务提供者，法律一般不设定其事前审查义务，即“避风港原则”，此原则被规定在该条例第二十三条。本条例项下的网络服务提供者在接到权利人的通知书后，如断开链接则不承担赔偿责任；如果是“明知”或“应知”的情形则应承担责任。尽管其中涉及的具体证据不明，但是从现在掌握的资料来看，乐动卓越无法证明阿里云在此案当中存在过错。所以只需关注阿里云是否履行了相应的“事后义务”即可。乐动卓越书面通知的形式和内容是否符合法律规定也同样不明确，但是从利益平衡的角度出发，阿里云在两次接到乐动卓越的书面通知后均未做任何回应，明显违反了其作为一家服务器提供商应履行的义务。

最后，由于阿里云未及时采取措施，因此应就乐动卓越在进行通知后的损失扩大部分承担连带侵权责任，法院依此确定了数额并作出判决。

3.4 启示

本案是一起著作权侵权纠纷，法院的说理和裁判也均围绕此展开。但对于网络经营者而言，数据安全的问题同样值得关注。

一家网络服务提供者，无论提供的是何种网络服务，均不具有绝对的事前审查义务，但是也并非如阿里云在本案中的抗辩所言，仅在司法机关或者其他国家权力机关正式通知时才有必要采取措施。按照“避风港原则”，当权利人或者被侵权人发出正式的书面通知时，其也应当采取相应的措施。

本报告认为，问题也恰在于此：

第一，《侵权责任法》第三十六条是采取不完全列举的方式对应采取的必要措施进行规定的，因此在司法实践中存在解释的空间。阿里云始终认为网络用户的“数据安全”是第一要务，其不可能根据对方一份通知就直接将其他用户正常运行当中的服务器关闭或者屏蔽，此举可能会带来更大的损害；

第二，虽然法律规定权利人通过书面通知可以要求服务提供者立即采取必要措施，但是为了用户的数据安全，网络服务提供者不应当仅做形式审查，因为材料可能是伪造的；但做实质审查又会违背“数据安全”的初衷，因为需要结合相关用户的数据来进行具体判断。

本报告建议，企业需要做出利益平衡，即审慎对待来自著作权权利人的通知。首先，对于权利人发来的书面通知，应当形式审查该通知的格式等是否符合法律规定。如果缺少相关项目，可拒绝采取措施；如果在形式上符合要求，网络服务提供者就应当视自己所提供的服务情况决定是否采取措施。如本案中，阿里云仅是服务器提供商，其不可能在不审查核实的情形下就擅自采取关闭服务器的措施；但是其同时作为中立的技术提供者，又不能无条件地审查核实，因为这事关网络用户的数据安全。权衡之下，最稳妥的措施是继续保持“中立”，虽不直接采取措施，但是应当向通知的权利人披露有关租用服务器的用户的相关信息，抑或是向该用户披露权利人的信息，最终由该两方进行交涉。如若交涉不成进入诉讼阶段，则此时服务提供者采取的任何措施只要遵照司法机关的要求即可。

如若该网络服务提供者负有审查用户数据的义务，则该提供者应当对权利人发来的书面通知进行实质审查，联合法务部门、技术部门乃至其他专业法律服务机构，对是否侵权进行判定，并进一步采取措施。

根据以上案件的启发，本报告建议，权利人一旦发现疑似侵权事件，首先应和侵权人联系沟通，直接要求其停止侵害。但如果像本案一样无法检索到侵权人的信息，则此时应当最大限度地搜集和保存证据，充实对于侵权要件的判断，同时建议聘请相关法律服务机构协助草拟通知书，向该网络服务提供者发出正式通知。最后，如若该提供者不予回应或者拒绝采取措施，则应当尽快诉诸其他法律途

径，如向相关主管机关投诉，或者向法院提起诉讼。

至于数据安全和知识产权权属的界限如何，本着客户利益至上和数据安全的原则，本报告认为，在合规的背景下，一个中立的技术提供者在无权查看数据的情形下，应当避免参与到相关知识产权权属的纠纷中，但可向一方披露另一方，让当事人双方进行协商交涉。这就要求网络服务提供者在日常的经营管理中对各用户的信息切实核实、审查、记录乃至公示，以便尽到自己必要的义务。

第九章
刑事案件

2017 年以来，公安部组织全国公安机关深入推进打击整治网络侵犯公民个人信息犯罪专项行动，侦破了一批大要案件。据统计，截至 2017 年 12 月 20 日，全国公安机关当年累计侦破侵犯公民个人信息案件 4911 起，抓获犯罪嫌疑人 15463 名，打掉涉案公司 164 个。[4] 本报告选取了在 2017 年具有影响力与代表性的若干案件进行分析，为企业的合规经验提供参考。

根据国双大数据的有关统计：约有 78.5% 的侵犯公民个人信息犯罪案件被告人通过购买的方式获取公民个人信息；约 5.4% 的案件被告人通过窃取的方式获取公民的个人信息，窃取形式大多是利用职务或工作之便、侵入计算机系统等。除了常见的购买、窃取等方式，还有业务合作、手机、跟踪、偷拍、内部员工交流透露、无偿提供信息等直接或间接获取信息的方式。[5]

由上述可见，在所有非法获取个人数据的方式中，购买无疑是最普遍，也较容易形成灰色产业链的一种。相较于个人作案，此类犯罪团伙作案的概率更大。多个犯罪嫌疑人正是通过先窃取再购买的方式完成整个犯罪。

1. 杜天禹侵犯公民个人信息案

1.1 案件基本信息

案件名称	杜天禹侵犯公民个人信息案
案号	（2017）鲁1311刑初332号
审理法院	临沂市罗庄区人民法院
案由	侵犯公民个人信息罪
被告	杜天禹
法院判决	一、被告人杜天禹犯侵犯公民个人信息罪，判处 有期徒刑六年，并处罚金人民币六万元。 二、没收违法所得14100元及作案工具银色移动硬盘一个、摩托罗拉牌手机一部、戴尔牌笔记本电脑 一台、无线上网卡一个，上缴国库。

1. 去年公安机关侦破侵犯公民个人信息案件 4900 余起，http://www.legaldaily.com.cn/zt/content/2018-01/09/content_7443903.htm?node=90103，2018 年 1 月 15 日最后访问。

2. 参见：《侵犯个人信息类刑事案件，上海、广东、浙江、江苏进前五》，http://mp.weixin.qq.com/s/X_6M4Cy22n3AG3ioUpMQFg，2017 年 12 月 4 日最后一次访问。

1.2 案情简介

徐玉玉事件事发于 2016 年，社会影响极大。被害人徐玉玉是一名家境贫寒的 18 岁准大学生，因被电信诈骗骗走学费导致最终心脏骤停不幸去世，电信诈骗得以实施的原因正是考生个人信息的泄露。该案对我国打击电信诈骗和保护个人信息意义重大。

徐玉玉事件涉及两案，一是陈文辉等人犯诈骗罪和侵犯公民个人信息罪一案，二是“黑客”杜天禹犯非法获取公民个人信息罪一案。

被告人杜天禹通过山东省 2016 年普通高等学校招生考试信息平台网站存在的漏洞，向其植入木马病毒，从而窃取该网站上的高考考生个人信息 64 万余条并出售。被告人陈文辉从杜天禹处买得部分信息实施诈骗。受害者徐玉玉被骗取 9900 元，其后与父亲去派出所报警，回家途中突发身体不适，经抢救无效死亡。

2017 年 4 月 17 日山东省检察机关对“徐玉玉被电信诈骗案”提起公诉。在一审过程中，该案两位鉴定人作为证人出庭作证，均认为诈骗行为的实施与徐玉玉的死亡之间存在因果关系。最终，陈文辉犯诈骗罪、侵犯公民个人信息罪被判处无期徒刑。被告人杜天禹犯非法获取公民个人信息罪被判有期徒刑 6 年，并处罚金 6 万元。

徐玉玉离世后，社会反响强烈。最高人民检察院联合最高人民法院、公安部共同出台了《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》。徐玉玉因个人信息泄漏遭遇诈骗致死，唤醒了社会的公民个人信息保护意识，对后续个人信息保护、打击电信诈骗有着深远的影响。

1.3 启示

从网络安全的角度来讲，本案的关键点有二：一是杜天禹通过招考信息平台的网络漏洞，将山东省 2016 年的高考考生信息下载并出售，直接导致了徐玉玉的个人信息被诈骗分子取得；二是山东省 2016 年普通高等学校招生考试信息平台作为教育部门下属的网站平台，安全意识低下，对网站的安全防护义务履行不到位，致使网站存在漏洞，考生信息遭到泄露。

值得注意的是，此案发生时《网络安全法》还尚未通过，但如今《网络安全法》已经生效，其中着重规定了网络运营者的安全保护义务和对个人信息的保护义务。对于山东省教育考试院来说，其下属的网站存在安全漏洞，违反了网络运营者的安全保护义务。对于杜天禹来说，通过木马程序非法入侵网络平台，获取公民个人信息并倒卖，违反了对个人信息保护的规定。

2. 雀巢员工侵犯公民个人信息案

自 2015 年 11 月《刑法修正案（九）》施行后，侵犯公民个人信息罪这一概念进入公众视野，引发人们对侵犯公民个人信息的高度重视与警惕。雀巢公司婴儿部经理、员工为了母婴市场份额，向医务人员有偿获取有关母婴信息。涉案员工、涉案医务人员最终获刑，警示了企业高管、员工，应坚守保护公民个人信息的底线。

2.1 案件基本信息

案件名称	雀巢员工侵犯公民个人信息案
案号	（2017）甘 01 刑终 89 号（二审） （2016）甘 0102 刑初 605 号（一审）
审理法院	兰州市中级人民法院（二审） 兰州市城关区人民法院（一审）
案由	侵犯公民个人信息罪
被告（上诉人）	雀巢（中国）有限公司西北区婴儿营养部市务经理郑某 兰州分公司婴儿营养部甘肃区域经理杨某、员工杨某甲等 兰州大学第一附属医院妇产科护师王某等医务人员
法院判决	2016 年 10 月 31 日，兰州市城关区人民法院一审宣判，以侵犯公民个人信息罪分别判处杨某等人拘役 4 个月至有期徒刑 1 年 6 个月不等的刑罚，附加罚金。之后，郑某等人以涉案行为属于单位犯罪等理由提出上诉。2017 年 5 月 31 日，兰州市中级人民法院作出二审终审裁定：驳回上诉，维持原判。

2.2 案情简介

2011 年至 2013 年 9 月，雀巢（中国）有限公司西北区婴儿营养部市务经理郑某、兰州分公司婴儿营养部甘肃区域经理杨某，为了抢占市场份额，推销雀巢奶粉，授意该公司员工通过拉关系、支付好处费等手段，从多家医院医务人员手中非法获取公民个人信息。其中，郑某与杨某通过上述手段，各非法获取公民个人信息四万余条；其他员工通过上述手段，均非法获取大量公民个人信息。期间，涉案的医务人员利用医院妇产科护师的便利，将其在工作

中收集的公民个人信息非法提供给雀巢公司涉案员工，收取“好处费”。

2.3 争议焦点

本案在被告是否涉嫌侵犯公民个人信息罪上并无明显争议，本案的主要争议在于其是否属于单位犯罪。多名辩护人提出本案系单位犯罪，应追究雀巢（中国）有限公司的刑事责任的辩护意见。

而法院认为，依据“雀巢公司 DR 任务材料、雀巢公司证明、雀巢公司政策、员工行为规范等，证明雀巢公司不允许向医务人员支付任何资金或者其他利益。不允许员工以非法方式收集消费者个人信息。对于这些规定要求，雀巢公司要求所有营养专员接受培训并签署承诺函 。被告人在明知法律法规以及公司禁止性规定的情况下，为完成工作业绩而置法律规范、公司规范于不顾，违规操作进而贿买医务人员，获取公民个人信息的行为，并非雀巢公司的单位意志体现，故本案不属于单位犯罪” 。

2.4 启示

第一，对于企业员工而言，追求商业利益需要遵守不侵犯公民个人信息的底线。对于销售母婴产品的企业员工而言，向待产孕妇进行推销这一诉求固然合理，但本案中，雀巢员工为追求业绩，贿买医务人员非法获取待产孕妇个人信息，无疑是侵害公民个人信息以获利的违法行为。从这一案例可以看出，商业活动中扩大客户群体的定向推销、定向宣传等行为，应以不侵犯公民个人信息为底线，禁止以非法获取公民个人信息的方式扩大潜在消费者群体。

第二，对于企业而言，应该通过协议明确员工的消费者信息保护义务，设置相应的公司章程。这不仅仅有助于警示员工，同样也能帮助企业自身避免涉嫌侵害公民个人信息的单位犯罪。本案中，雀巢公司在《雀巢指示》以及《关于与保健系统关系的图文指引》等文件中明确规定，“对医务专业人员不得进行金钱、物质引诱”。雀巢公司举证证明，其要求所有营养专员接受培训并签署承诺函，不允许员工因推销 0–12 月龄健康婴儿使用的婴儿配方奶粉为目的，直接或间接地与孕妇、哺乳妈妈或公众接触、不允许员工未经正当程序及经公司批准而主动收集公民个人信息。因此法院认定，此案中的侵犯公民个人信息行为系部分员工的个人行为，而非雀巢公司单位意志的体现，故本案不属于单位犯罪，雀巢公司免受法律的制裁。

第十章
争议事件

除了执法案件与诉讼，围绕着数据还产生了大量的争议事件，这些争议事件虽最终没有通过官方渠道解决，但仍然可以作为前车之鉴，为企业数据的收集、利用和提供方式提供参考。

1. 华为与微信用户数据争议事件

1.1 争议基本情况

据《华尔街日报》（中文网）2017 年 8 月 4 日的报道，华为发布的荣耀 Magic 智能手机，通过收集用户的活动信息，以打造其人工智能功能，例如使手机能够基于用户的短信内容推荐餐厅。其收集的信息包括热门社交应用微信的聊天信息。

而腾讯方面则认为，华为的上述做法实际上是在夺取腾讯的数据，并侵犯了微信用户的隐私权。华为则否认其侵犯用户隐私权，因其仅在用户通过手机设置予以授权的情况下收集用户活动信息。所有用户数据都属于用户，而不属于微信或是荣耀 Magic，该公司在荣耀 Magic 设备上处理用户数据之前经过了用户的授权。

两家公司在数据上的分歧还不止于此。持有华为新近推出设备的用户无法在微信支付中使用指纹完成支付。可见，华为和腾讯在很多方面均未能达成一致。

对此，工信部表示，在用户个人信息保护方面，将会依照《电信和互联网用户个人信息保护规定》等有关法律法规，督促企业加强内部管理，自觉规范收集、使用用户个人信息行为，依法保护用户的合法权益。对信息通信企业之间的分歧和纠纷，工信部会依据职责积极组织协调、引导行业自律，为大众创业、万众创新营造良好的市场秩序。

1.2 争议焦点

本事件中更值得关注的问题可能不仅仅在数据的属性和性质，因为在静态的权利持有上，一般不会存在法律价值上的冲突。本报告认为，更值得注意的是在动态流转中获取和利用的问题：第三方对于数据的合法获取需要重点关注。这就存在另外一个问题，第三方对用户数据获取和使用的边界究竟如何界定？根据《网络安全法》中的相关规定，网络经营者收集个人信息应当遵守合法、正当、必

要的原则，需征得个人的明确同意，同时确保信息的安全。

1.3 启示

近些年来，人工智能得以快速发展，各大互联网公司的数据互通也是其中一个重要的基础。但是目前我国尚不存在一套系统的数据互通体系，还是各个网络经营者之间在协商解决数据互通问题。

2. 菜鸟驿站与顺丰速运就物流数据争议事件

2.1 争议基本情况

2017 年 6 月 1 日下午 14 时左右，菜鸟网络官方微博发布了《关于顺丰暂停物流数据接口的声明》，主要声称两件事：其一，顺丰暂停了物流数据接口；其二，顺丰对于菜鸟信息安全升级工作的不予配合。

当日，丰巢科技的投资人之一顺丰集团官方微博发布了《关于菜鸟称物流数据接口暂停的回应》，回应了菜鸟网络的主张。顺丰认为，菜鸟基于自身商业利益出发，要求丰巢提供与其无关的客户隐私数据，且此类信息隶属于客户，因而拒绝这一不合理要求。

之后，菜鸟网络再次回应，指出丰巢快递柜和菜鸟数据对接后，一直大量调取淘宝用户电话号码等信息，并超过合理使用范围，存在严重安全隐患，这是此次事件的核心起因。

最后，国家邮政局召集菜鸟网络和顺丰速运高层来京，

就双方关闭互通数据接口问题进行协调。双方同意从 6 月 3 日 12 时起，全面恢复业务合作和数据传输。

2.2 争议焦点

该事件争议焦点主要有：

第一，菜鸟以“信息安全升级”为由，要求丰巢提供物流数据信息的诉求是否合理。先从目的来看，无论是“信息安全升级”还是“为消费者提供代收服务”，菜鸟网络对于个人信息收集的目的正当，与用户的权益息息相关；故而判断其行为是否合法，要判断菜鸟网络是否有经被收集者同意。因此争议焦点之一是：菜鸟经过数据接口对接取得、使用用户信息时是否需要得到用户授权。

第二，顺丰“大量调取淘宝用户电话号码信息”的行为是否合理。针对菜鸟的主张，顺丰若证明其行为的合理性，必须提供一定举证：其一，顺丰调取淘宝用户电话号码信息的行为有必要性，与提供的物流服务有关，否则违反“网络运营者不得收集与其提供的服务无关的个人信息”的要求；其二，顺丰调取信息的程度应在合理范围内，否则违反网络运营者收集个人信息的“必要”原则；其三，若网络安全隐患确实存在，顺丰无疑有义务采取必要的手段，防止数据泄漏毁损。

第三，在菜鸟“信息安全升级”的诉求真实存在的情况下，丰巢是否存在配合义务。根据《网络安全法》的相关规定，网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面可以进行合作，提高网络运营者的安全保障能力。

2.3 启示

菜鸟、顺丰就物流数据的争议，主要集中于数据接口对接问题。数据接口对接可以实现数据相互的传输，提高合作效率，但是其中数据保护问题亟待注意。故而本报告认为，该争议事件可以从以下多方面给予企业启示：

第一，对于企业，要对其收集信息目的、方式、范围予以公示，并经被收集者同意。本事件中，顺丰认为菜鸟有“基于自身商业利益出发，要求丰巢提供与其无关的客户隐私数据”之嫌，是因为菜鸟未将数据收集、使用的目的予以充分说明，对数据的收集、使用未得到被收集者同意；菜鸟认为顺丰不合理“调取淘宝用户电话号码等信息，并超过合理使用范围”，无疑是质疑其收集使用的范围、用途，最终引发双方关闭数据接口激化矛盾。该矛盾并非偶然，另一例是今年 7 月京东关闭“天天快递”数据接口，断绝合作关系。

故而，本报告建议，企业在签订数据对接协议时，应该事先明确双方收集信息的规则，以及收集使用信息的目的、手段与范围，以免在合作过程中，因数据对接接口问题，双方无法就数据收集问题达成一致，引发合作关系的终止；并且也应该采取设立违约条款等手段，避免一方“突然关闭数据接口”，引起消费者的不便与企业自身的利益损失。

第二，应该告知用户“数据接口对接”的存在，提醒其数据传输至其他系统，以征求其同意。企业收集用户数据后，应该告知其数据将会通过接口传输至另一系统，遵守《网络安全法》中“未经被收集者同意，不得向他人提供个人信息”的规定。此外，在数据传输的过程中，对于额外增加的数据泄漏、毁损风险，企业要采取必要的手段保障数据安全。

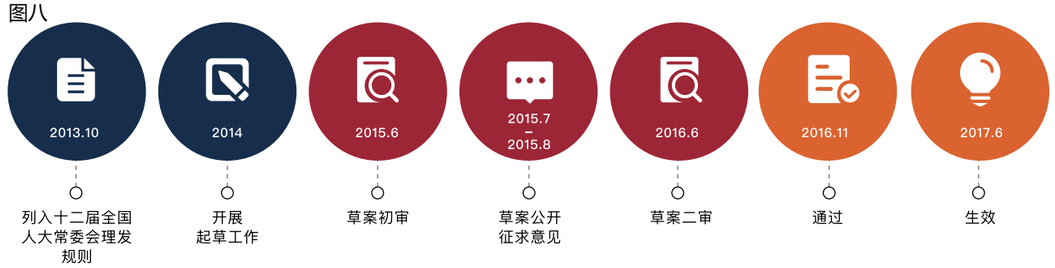
第三，对于数据接口对接的过程中，应该采取技术手段，对数据共享予以一定限制。网络安全法规定，网络运营者不得收集与其提供的服务无关的个人信息。本事件中，菜鸟认为顺丰收集了与其物流服务无关的淘宝订单信息。故而从技术层面上，在数据共享的过程中，可以采取技术措施，使另一方系统通过接口对接收集的信息是有限的、只和其提供服务有关的个人信息与数据，防止企业通过“数据共享”手段无休止地肆意收集数据、滥用数据，侵犯用户权利。

第四，商业利益对于公共利益的让渡。顺丰对于自身物流数据的“寸土不让”，菜鸟声称顺丰对于淘宝信息的觊觎，一定程度上源于现今各大企业的共识：数据具有巨大的商业利益。本事件最终以国家邮政局的出面划上句号，以“积极寻求解决问题的最大公约数，共同维护市场秩序和消费者合法权益”为解决之道。正如菜鸟网络发布的声明，企业追求商业利益，应以保护用户个人信息、保护数据安全为底线。

第四部分
法律法规概述与分析

在 2017 年，网络安全问题日益凸显，成为国际社会难以回避的巨大挑战。国家主席习近平曾指出：“没有网络安全就没有国家安全，没有信息化就没有现代化”。作为立法机关的全国人大常委会同样高度重视网络安全工作，2012 年 12 月即已审议通过《全国人民代表大会常务委员会关于加强网络信息保护的决定》。2016 年 11 月，全国人大常委会审议通过《中华人民共和国网络安全法》（简称《网络安全法》），并于 2017 年 6 月 1 日正式施行（见图八）。

图八



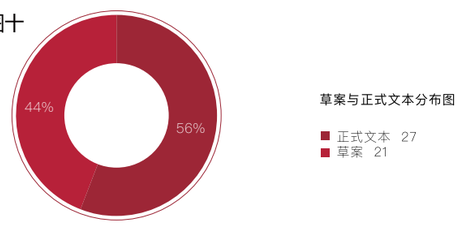
《网络安全法》是在习近平总体国家安全观指引下，结合中国互联网管理的实际经验，对网络和信息安全事项作出的全方位规范。法律分为总则、网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置、法律责任、附则七章，共七十九条。

对于企事业单位，需要重点关注《网络安全法》第三章“网络运行安全”和第四章“网络信息安全”。本部分旨在对该两章下的规定进行解读，同时对在 2017 年出台的相关配套法律法规和文件进行归纳整理和分析。

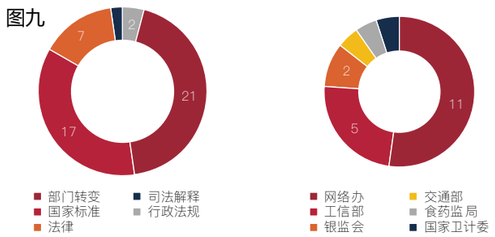
2017 年，数据保护方面的法律、司法解释、行政法规、部门规章和国家标准等法律文件共计有 48 部，其中包括法律 7 部、司法解释 1 部、行政法规 2 部、部门规章 21 部、国家标准 17 个。它们均在 2017 年制定、公布、生效，或以草案的形式征求意见。21 部部门规章中，网信办制定 11 部，工信部制定 5 部，银监会制定 2 部，交通部、食药监总局、国家卫计委各制定 1 部（见图九）。

48 部法律法规中，正式文件有 27 个，征求意见稿草案有 21 个。征求意见稿大多集中于国家标准部分（分布比例见图十）。

图十

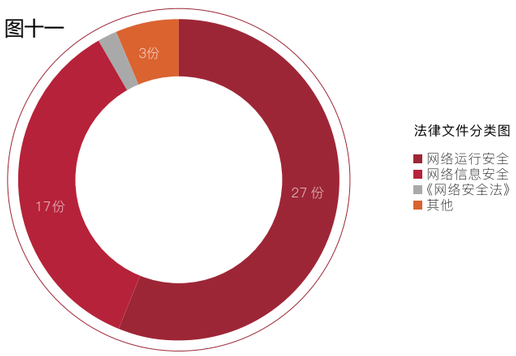


图九



48 份法律文件中，《网络安全法》是基本法律，网络运行安全和网络信息安全均有涉及。在其他 47 份文件中，有 27 份法律文件涉及网络运行安全，17 份法律文件涉及网络信息安全。图中的“其他”是指既不属于网络运行安全的范畴，也不属于网络信息范畴的法律文件，共计有 3 份（见图十一）。

图十一



第十一章
网络运行安全

网络运行安全是《网络安全法》中的一项重要制度，以网络安全等级保护为基础，还包括身份验证义务，设立应急预案制度。关键信息基础设施保护业务也是网络运行安全的重要组成部分。据不完全统计，2017 年违反《网络安全法》中网络运行安全义务的行政处罚案件至少有 20 起，主要涉及未履行网络安全保护义务，未履行身份验证义务，网络产品、服务不符合国家标准强制性要求，从事或支持危害网络安全的活动等违法行为。

本章将按照网络运营者、网络产品 / 服务提供者、关键信息基础设施运营者三个主体进行分类，针对不同主体所面临义务的新规进行说明。但需要注意的是，这三个主体的关系并非是“非此即彼”，企业可能既是网络运营者，又是网络产品、服务提供者，还是关键信息基础设施运营者。

1. 网络运营者义务的一般规定

1.1 等级保护制度

信息安全等级保护，是对信息和信息载体按照重要性等级分级别进行保护的一种工作，信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段。

1994 年，国务院颁布《计算机信息系统安全保护条例》，规定计算机信息系统实行安全等级保护。随着《网络安全法》的实施，等级保护制度在今天已上升为法律，并在法律层面确立了其在网络安全领域的基础、核心地位。等级保护制度是《网络安全法》中规定的重点内容，该制度是基于我国现阶段互联网技术的发展以及社会各个领域对于网络空间安全的要求而建立起来的。日新月异的互联网技术在为社会各个行业带来便捷的同时，也带来了诸多安全隐患，尤其是政府机关、能源、金融、交通、水利、教育、国防科工等涉及到可能危害国家安全、国计民生、公共利益等领域，一旦发生数据泄露或境内境外攻击等网络安全事件，其影响将不可估量，难以控制。为避免此类事态，网络安全等级保护制度作为一种网络安全保护途径应运而生。对此，本报告发现，有一个值得关注的现状是，31.02% 的受访企业在《网络安全法》实施后，没有履行等级测评义务（本报告第一章图一）。

需要注意的是，网络安全等级保护制度与现行的信息安全保护制度在主体与监管部门等各方面都存在区别。信息安全等级保护制度的主体是信息系统的运营者和使用单位，其信息系统特指为金融、税务、工商、海关、能源、党政机关办公系统等重要信息系统，其监管部门为公安机关。但是，网络安全等级保护制度的主体是网络运营者，其监管部门为网信部门。国务院的电信主管部门、公安部门和其他有关部门在各自的职责范围内负责网络安全保护和监督管理工作（详情见本报告第二章）。

关于网络安全等级保护制度的具体内容，由《网络安全法》第二十一条规定。企业对于这些规定的履行现状，从本报告第一章调研数据和分析可见一斑。

关于网络等级保护措施，在诸多法律法规中也有所提及。

1.1.1《信息安全技术 网络安全等级保护基本要求 第 3 部分：移动互联安全扩展要求》（征求意见稿）

与传统等级保护对象相比，该标准针对的是移动互联技术等级保护对象，区别在于移动终端可以通过无线方式接入网络，因此突出三个关键要素：移动终端、移动应用和无线网络。

该标准将移动互联技术的等级保护一共定为四级，每一级都有相应的技术要求和管理要求。技术要求中包含“物理和环境安全”、“网络和通信安全”、“设备和计算安全”、“应用和数据安全”这四个要素。管理要求中包含“安全策略和管理制度”、“安全管理机构和人员”、“安全建设管理”和“安全运维管理”这四个要素。

1.1.2《信息安全技术 网络存储安全技术要求》（征求意见稿）

该标准规定了为满足存储市场对于网络存储产品安全性的要求，网络存储应采取的安全技术措施。根据《网络安全法》第二十一条的要求，网络运营者负有防止网络数据泄露或者被窃取、篡改的安全保护责任。数据存储是保障数据安全的重要前提之一，因此该标准的制定目的在于落实该条规定。

目前网络存储领域的现状是：一方面，随着数据价值的提升，网络存储的重要性也在不断提升。另一方面，由于个人信息保护的要求，网络存储也面临信息安全方面的挑战。本标准专门细化规定了对于网络存储的安全技术要

求，包括安全功能要求、安全保障要求，同时针对这两种技术要求，又分别根据安全功能的强弱和安全保障要求的高低，将网络存储安全保障要求分成三个等级，便于相关组织更好地开展工作。

1.2 用户实名制义务

《网络安全法》对用户实名制进行了规定：网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。关于网络实名制的要求，在《信息安全技术 网站可信评估指标》（征求意见稿）中也有体现。

1.2.1《信息安全技术 网站可信评估指标》（征求意见稿）

本标准规定了网站可信评估指标、网站基本级要求、网站增强级要求、评估方法、评估结果展示和撤销等内容。本标准适用于国内所有合法接入的互联网网站，其中，提出了包括身份要求以及系统安全要求的网站基本级要求以及网站增强级要求，包括身份真实性评估以及系统安全评估的网站基本级评估方法和网站增强级评估方法，以及有关网站可信评估指标的详细要求。

其中，身份真实性评估顺应了《网络安全法》中用户实名制的要求，在《网络安全法》要求用户提供真实信息的前提下对信息进行核实、评估。此外，系统安全评估也可以列为有关部门判断网络运营者是否履行网络安全义务的参考依据，以维护网络运行安全。

1.3 网络应急处置措施

为了应对突发事件，网络运营者还应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

关于网络应急处置措施，在诸多法律法规中也有所提及。

1.3.1《国家网络安全事件应急预案》

《网络安全法》在其“监测预警与应急处置”一章中，对于“应急工作”确有初步的涉及和大致框架，给网络安全应急工作提供了方向。但是对于相关具体的应急处置内容仍然有待细化，例如“相应的应急处置措施”具体步骤的空白、“按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级”的具体分级标准的不清等问题，不利于应急工作的有效落实。

2017 年 6 月 27 日，中央网信办印发《国家网络安全事件应急预案》（简称《应急预案》）。其中规定了“网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件”。其主要划分标准包括该网络事件对国家安全、社会秩序、经济建设和公众利益构成的威胁、影响程度，具体分类的依据包括该网络安全事件令重要网络和信息系统遭受的系统损失程度，造成的系统瘫痪面积、业务处理能力的影响、国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒造成的威胁情况等。

结合《网络安全法》的相关规定，“网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。”《应急预案》较明确地规定分级制度，列举了可供分级的客观依据，令分级有章可循，有利于贯彻“统一领导、分级负责”、“坚持谁主管谁负责、谁运行谁负责”的网络

的内容以及事后的分析总结工作，与《网络安全法》中关于应急预案的规定相对应，即网络运者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

由此可见，工作指南中应急处置一章的规定对应的是《网络安全法》中的应急预案制度，但是在工业控制系统信息安全领域，工作指南所做出的是针对该领域的特定要求，体现了《网络安全法》在工业控制信息安全领域的细化。

1.3.3《信息安全技术 信息安全风险处理实施指南》

信息安全风险管理是信息安全保障工作的一项重要基础性工作，贯穿于信息系统生命周期的全过程，主要包括风险评估和风险处理两个基本步骤：风险评估是对风险管理对象所面临的风险进行识别、分析和评价的过程；风险处理是根据风险评估的结果、选择和实施安全措施的过程。

可见，这两者都是针对网络安全事件所采取的应急手段，提高《网络安全法》中规定的应急手段效率，将风险应急工作原则，提高工作效率与资源分配的合理性，也为后续的预警分级制度提供依据。

1.3.2《工业控制系统信息安全事件应急管理工作指南》

2017 年 6 月，工业和信息化部引发《工业控制系统信息安全事件应急管理工作指南》，工作指南适用于工业和信息化主管部门、工业企业开展工控安全应急管理工作。该指南对于“工控安全事件”作出解释，即由于人为、软硬件缺陷或故障、自然灾害等原因，对工业控制系统、工业控制系统数据造成或者可能造成严重危害，影响正常工业生产的事件。归纳起来就是三个原因，即人为原因、软硬件原因和自然灾害原因。相关主体应根据不同的归因采取不同的安全事件应急管理工作。

该《工作指南》主要规定的是应急处置的问题，对于可能发生或已经发生的工控安全事件，工业企业应立即开展应急处置，采取科学有效方法及时施救，力争将损失降到最小，尽快恢复受损工业控制系统的正常运行。当事发工业企业应急处置力量不足时，可请求上级主管部门协调应急技术机构提供支援。

另外，该指南也对应急处置开展后的报告信息和事件分析总结工作进行了相关规定。其关于报告信息所应包含与损失最小化。具体而言，本标准针对风险评估工作中反映的各类信息安全风险，从风险处理工作的组织、管理、流程等方面给出了相关描述，用户指导组织形成客观、规范的风险处理方案，促进风险管理工作的完善。

1.3.4《信息技术 安全技术 信息安全事件管理 第 1 部分：事件管理原理》（征求意见稿）

标准提出，对于任何期望具有强健信息安全计划的组织，采取有计划的方法开展如下活动十分必要，包括：发现、报告和评估信息安全事件；响应信息安全事件，包括启动适当的控制措施来防止和降低影响并从中恢复；报告信息安全脆弱性，以便对其进行评估和适当处理、从信息安全事件和脆弱性中汲取经验教训，建立预防性控制措施，并整体改进信息安全事件管理办法。该标准以这种有计划的方法作为主线，提供相应指南，以提高网络运营者的应急能力。

1.3.5《信息安全技术 网络安全事件应急演练通用指南》（征求意见稿）

该指南是为了应对越来越严峻的网络安全事件，而建立的一套培训、检验政府、企事业单位、社会团体的演练标准。本标准为相关单位进行网络安全事件应急响应检验

及平时应急演练，提供了一个可具体操作的基本框架，详细规定了网络事件应急预案中的应急响应组织与流程，以及分类应急处置措施，还规定了网络安全事件的应急演练形式和组织环节。

1.3.6《公共互联网网络安全突发事件应急预案》

网络安全突发事件指由突发网络攻击、网络入侵等导致的，造成或可能造成严重社会危害的事件。该预案规定了相关主体包括基础电信企业、域名机构、互联网企业等对于网络安全突发事件的事前预防义务与网络安全事件发生时企业和有关部门应采取的应急措施，以维护网络运行安全。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的单位或个人，由电信主管部门给予约谈、通报或依法、依规给予问责或处分。基础电信企业有关情况纳入企业年度网络与信息安全责任考核。

1.4 开展网络安全认证、风险评估

《网络安全法》要求网络经营者开展网络安全认证、检测、风险评估等活动，并将网络安全事件及时对社会公众进行公布。新近的《信息安全技术 数据库管理系统安全评估准则（征求意见稿）》主要对安全评估的内容进行了具体规定。

1.4.1《信息安全技术 数据库管理系统安全评估准则》（征求意见稿）

根据该标准的引言：数据库管理系统是为数据库的建立、使用和维护而配置的软件。它建立在操作系统的基础上，对数据库进行统一的管理和控制，用户使用的各种数据库命令以及应用程序的执行，都要通过数据库管理系统，数据库管理系统还提供对数据库的维护支持，按照系统管理人员的规定要求，保证其安全。

由此可见，数据库作为储存数据的载体，其安全性对保护数据安全有极大的重要性。故而通过安全评估，评估数据库的数据安全可靠程度，确保其安全地应用在存储、格式化、维护和管理用户数据，避免损失与风险发生。

1.5 禁止危害网络安全

《网络安全法》对于网络运营者规定了禁止性义务，例如“不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动”。此外，禁止危害网络安全的规定也出现在新近的《治安管理处罚法（征求意见稿）》中。

1.5.1《治安管理处罚法》（征求意见稿）

2017 年 1 月，公安部网站发布了《治安管理处罚法》的修订公开征求意见稿，向社会公开征求意见。这也是本法自 2006 年 3 月 1 日起施行以来，迎来的首次大修。此次的征求意见稿对电子商务、互联网金融中的网络安全、个人信息保护、快递物流中的寄件安全等“互联网 +”时代亟待解决和完善的问题，予以了明确回应。[1] 此次的修改征求意见稿中涉及网络安全的规定主要集中在第三十一条和第三十二条。第三十二条规定主要是针对网络服务的提供者，在以下网络产品服务提供规范一节中再做阐述。

该征求意见稿第三十一条规定了五种禁止性行为：

（一）违反国家规定，侵入计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对计算机信息系统实施非法控制，造成危害的；

（二）违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成危害的；

（三）违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

（四）故意制作、传播计算机病毒等破坏性程序，造成危害的；

（五）提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，造成危害的。

值得注意的是，此条所禁止的五种行为与刑法中规定的相关罪名做到了对应。例如非法获取计算机信息系统数据罪；破坏计算机信息系统罪；故意制作、传播计算机病毒罪；提供用于侵入、非法控制计算机信息系统的程序、工具罪等。在企业或者个人触犯此条规定时，应对个案进行分析以确定是否涉嫌犯罪。

2. 网络产品、服务提供者的义务

《网络安全法》对网络产品、服务提供者进行了一系列规范：网络产品、服务应当符合相关国家标准的强制性要求；网络产品、服务的提供者不得设置恶意程序；网络产品、服务的提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施并采取告知义务等。以下将对网络产品、服务提供者的义务进行分析。

1.《修订治安管理处罚法与时俱进值得点赞》，http://www.chinacourt.org/article/detail/2017/02/id/2542584.shtml，2017 年 10 月 17 日最后访问。

2.1 网络产品、服务提供规范

网络产品、服务在各种领域都有广泛的应用，包括但不限于电子商务。除《网络安全法》外，2017 年的法律法规对于网络产品、服务提供者有其他的规定，对《网络安全法》中网络产品、服务提供者“安全审查”、“安全维护”等义务进行具体化。如本报告第三章表二十一显示，广州动景计算机公司因违反《网络安全法》被广东省通信管理局通报，并被要求开展通信网络安全防护风险评估，建立新业务上线前安全评估机制和已上线业务定期核查机制，对已上线网络产品服务进行全面检查，排除安全风险隐患，避免类似事件再次发生。

2.1.1《治安管理处罚法》（征求意见稿）

此次的修改征求意见稿的第三十二条对网络服务提供者的信息网络安全管理义务作出了细致的规定：（一）用户信息登记和保护；（二）公共信息发布审核和巡查；（三）日志留存；（四）发现、拦截、处置违法信息并向公安机关报告；（五）为公安机关、国家安全机关依法履行职责提供技术支持与协助；（六）建立和执行信息网络安全管理制度和措施。

上述规定对于用户信息登记和保护义务，安全防护义务，支持协助义务，信息管理义务进行了着重的强调，需要网络服务提供者注意。

2.1.2《网络产品和服务安全审查办法》（试行）

2014 年 5 月，国家网信办宣布，为维护国家网络安全、保障中国用户合法利益，中国将推出网络安全审查制度。《网络安全法》中规定：“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。”而 2017 年 5 月 2 日国家网信办发布的《网络产品和服务安全审查办法（试行）》（简称“审查办法”），作为《网络安全法》的配套法规，即是对其中“安全审查”作出的具体规定。它与《网络安全法》一同于 2017 年 6 月 1 日生效。

审查办法规定，对可能影响国家安全的网络产品和服

务进行安全审查，其目的是为了提高网络产品和服务的安全可控水平，防范供应链安全风险，维护国家安全和公共利益。其安全审查的重点是产品和服务的安全性、可控性，包括产品被非法控制、干扰和中断运行的风险，产品提供者非法收集用户信息的风险等。

2.1.3《信息安全技术 网络产品和服务安全通用要求》（征求意见稿）

该征求意见稿从三个方面对网络产品和服务提供者的义务进行具体的阐释：

第一，网络产品和服务提供者应禁止提供危害安全的产品、服务，具体包括：

（一）禁止在网络产品和服务的研发、生产、交付、运维等过程中植入恶意程序；

（二）禁止设置隐蔽接口或未明示功能模块；

（三）禁止加载能够禁用或绕过安全机制的组件；

（四）必须建立和实施网络产品和服务的完整性保护措施，减少产品和服务的关键组件、过程和数据被篡改、伪造的风险。

第二，网络产品和服务提供者应对其提供的产品、服务进行安全风险测试。在网络产品和服务的设计、开发环节识别安全风险，制定安全策略，网络产品和服务在交付前必须进行安全性测试；建立和执行针对网络产品和服务安全缺陷、漏洞的应急响应机制和流程；在发现网络产品和服务存在安全缺陷、漏洞时，立即采取修复或替代方案等补救措施，及时告知用户安全风险，并向有关主管部门报告。

第三，网络产品和服务提供者应对其提供的产品、服务进行安全维护，不得因业务变更、产权变更等原因单方面中断或终止安全维护。

2.1.4《信息安全技术 信息技术产品安全可控评价指标 第 5 部分：通用计算机》（征求意见稿）

本标准规定了通用计算机产品安全可控评价指标，适用于评价实施方对通用计算机产品安全可控程度进行评价，也适用于产品采购、企业自查时参考。该征求意见稿着重介绍了通用计算机产品安全可控评价指标包括：产品设计实现透明性、产品实现验证、供应链安全保障能力、产品持续保障能力、产品安全生态适应性五个指标项。

2.2 接受安全检测与安全认证义务

网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

与安全认证有关的的文件如下：

2.2.1《信息安全技术 移动应用网络安全评价规范》（征求意见稿）

本标准是就移动应用领域的网络安全评价制作的专门规范，主要规定了对移动应用进行网络安全评价的内容、流程与方法，针对保密性、完整性、可用性、可控性和不可否认性等要素，在技术层面上对源代码、算法、存储数据和权限等做了安全评价的要求。该标准适用于移动应用的客户端程序和服务端程序在程序开发、测试评价和审核发布等各个阶段的安全性评价。对应了《网络安全法》中对于网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求的规定。

3. 关键信息基础设施运营者义务

关键信息基础设施运营者是指一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生、公共利益的信息基础设施。根据全国人民代表大会常务委员会执法检查组于 2017 年 12 月 24 日在第十二届全国人民代表大会常务委员会第三十一次会议上所作的《关于检查＜中华人民共和国网络安全法＞、＜全国人民代表大会常务委员会关于加强网络信息保护的决定＞实施情况的报告》，在 2016 年国家网信办等部门组织开展的关键信息基础设施摸底排查工作中，可以得知目前我国约有 1.1 万个关键信息系统。

3.1 重点安全保护义务

《网络安全法》对关键信息基础设施实行重点保护，对其安全管理要求和技术要求作出了更加严格的规定。因此，关键信息基础设施运营者除了应当履行《网络安全法》第二十一条规定的安全保护义务外，还要履行额外的重点安全保护义务。

3.1.1《公共互联网网络安全威胁监测与处置办法》

《网络安全法》第五章为“监测预警与应急处置”，重点提出负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。同时国家网信部门应协调有关部门建立健全网络安全风险评估和

应急工作机制。在这种背景下，针对这部分内容，工信部作为主管部门，在原有法规的基础上发布了该《处置办法》，对于网络安全的威胁监测与处置制定了较为详细的操作办法。

本办法的规制对象为公共互联网中的网络威胁。“网络威胁”是指公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件。从本条看出，其对《网络安全法》中监测预警和应急处置的对象作了一定的解释，法律中只点出了“网络安全”和“安全事件”等较为宽泛的说法，而办法则细化到了四大类和更多的小类，这些分类下还有相应的应急处置措施（表二十五）。

表二十五

分类	解释与列举	相关处置措施
网络资源	被用于实施网络攻击的恶意 IP 地址、恶意域名、恶意 URL、恶意电子信息，包括木马和僵尸网络控制端，钓鱼网站，钓鱼电子邮件、短信 / 彩信、即时通信等	采取停止服务或屏蔽等措施
恶意程序	被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序等	清除本单位网络、系统或网站中存在的可能传播扩散的恶意程序
安全隐患	网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等	采取整改措施，消除安全隐患；对涉及党政机关和关键信息基础设施的，同时通报其上级主管单位和网信部门
安全事件	网络服务和产品已被非法入侵、非法控制的网络安全事件，包括主机受控、数据泄露、网页篡改等	N/A

除此之外，《处置办法》中对于争议解决的方式作了规定，如果对于上述处置措施不服，可以进行申诉；而相关部门如果未进行处置，本办法又将行政责任的设置指向了《网络安全法》，由有关部门依照规定进行约谈或给予警告、罚款等行政处罚。

3.1.2《关键信息基础设施安全保护条例》（征求意见稿）

条例的制定是为了保障关键信息基础设施的安全。根据本条例第二条，在中国境内规划、建设、运营、维护、使用关键信息基础设施以及开展关键信息基础设施的安全保护，都适用该条例。该条例同时涉及了重点安全保护义务、“三同步”原则、数据境内保存与跨境传输规则以及定期安全检测评估义务。

该条例中涉及到的重点安全保护义务，主要是对相关人员作出的具体规定，包括网络安全管理负责人、关键岗位的专业技术人员以及相关从业人员。

其对人员做出的具体规定，与《网络安全法》中规定的安全保护制度相对应。《网络安全法》第三十四条中同样规定了关键信息基础设施运营者应当设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查，以及应当定期对从业人员进行网络安全教育、技术培训和技能考核等。

3.1.3《信息安全技术 金融信息保护规范》（征求意见稿）

依据该征求意见稿的规定，金融信息服务提供商应建立独立的部门，落实信息安全管理相关职责。主要要求如下：

金融信息提供商的主要负责人为信息安全管理第一责任人，同时指定分管领导负责企业信息安全管理日常工作；另外，金融信息提供商应成立信息安全领导小组或者信息安全管理办公室负责具体信息安全管理实施工作。其职责主要包括：研究和执行国家和行业有关信息安全的政策、法律和法规；制定和推广企业信息安全管理总体策略、管理规范和技术标准等。

3.2“三同步”原则

“三同步”制度要求，保障关键信息基础设施运行安全的技术措施，应当与关键信息基础设施的主体工程同步规划，同步建设，同步使用，在我国《密码法》征求意见稿中也有所涉及。

机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

该规定与《网络安全法》对于关键信息基础设施加强保护的立法思想一致。关键信息基础设施一旦发生数据泄露，往往会产生重大的社会负面影响，故而需要加强保护。而《密码法》草案要求对关键信息基础设施所使用的密码加强保护、确保对密码保障系统进行安全审查，将关键信息基础设施发生数据泄露的风险进一步控低。

3.3 接受国家安全审查义务

《网络安全法》规定关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。关于“安全审查”在我国《密码法（征求意见稿）》与《关键信息基础设施安全保护条例（征求意见稿）》中也有所涉及。

3.2.1《中华人民共和国密码法》（征求意见稿）

2014 年 12 月，国家密码管理局成立起草小组，着手《密码法》起草工作。2016 年国务院印发“十三五”国家信息化规划中，交代了要“推动出台网络安全法、密码法、个人信息保护法，研究制定未成年人网络保护条例”。最终《密码法》草案征求意见稿于 2017 年 4 月 13 日向社会公众公布，征求其意见。

《密码法》以“规范密码应用和管理，保障网络与信息安全，保护公民、法人和其他组织的合法权益，维护国家安全和利益”为立法目的，其中规定：关键信息基础设施应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护，同步规划、同步建设、同步运行密码保障系统，若发生密码失泄密案件的，由有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

密码本身就是一种保护数据安全的技术。通过加强密码安全审查，确保密码安全保障能力，是对数据安全的间接保护。

3.3.1《中华人民共和国密码法》（征求意见稿）

《密码法》征求意见稿规定国家对关键信息基础设施的密码应用安全性进行分类分级评估，按照国家安全审查的要求对影响或者可能影响国家安全的密码产品、密码相关服务和密码保障系统进行安全审查。若违反本法或者有关法律、法规规定，发生密码失泄密案件的，由有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

3.3.2《关键信息基础设施安全保护条例》（征求意见稿）

《关键信息基础设施安全保护条例》中对运营者采购、使用产品和服务作出规定：运营者采购网络产品和服务，可能影响国家安全的，应当按照网络产品和服务安全审查办法的要求，通过网络安全审查，并与提供者签订安全保密协议。

这与《网络安全法》中的国家安全审查制度相对应，启动的前提都是可能影响国家安全。本报告认为，相较于《网络安全法》的相关规定，该法条还是有值得注意的地方。《网络安全法》中规定该安全审查是国家网信部门会同国务院有关部门组织进行的审查，但是在该条例中并没有明确指出审查部门，只是规定了按照网络产品和服务安全审查办法的要求。

若运营者使用未经安全审查或安全审查未通过的网络产品或者服务的，由国家有关主管部门依据职责，责令停止使用，并对直接负责的主管人员和其他直接责任人员处以罚款。

3.4 数据境内保存与跨境传输规则

数据作为一种“战略资源”，对于国家和企业的重要性不言而喻。2017 年 8 月 25 日，全国信息标准化技术委员会发布了《信息安全技术数据出境安全评估指南（征求意见稿）》的第二次审议稿，对数据出境的概念进行了明确，对安全评估的流程进行了细化。《网络安全法》中要求关键信息基础设施运营者将在我国境内运营中收集和产生的个人信息和重要数据在我国境内存储，确实需要向境外提供的，应当进行安全评估。

3.4.1《关键信息基础设施安全保护条例》（征求意见稿）

《关键信息基础设施保护条例》的制定是为了保障关键信息基础设施的安全，作为《网络安全法》的下位法，该条例对关键信息基础设施运营者的安全保护义务以及产品和服务安全作出了更加细致的规定。

《网络安全法》规定了运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照个人信息和重要数据出境安全评估办法进行评估；法律、行政法规另有规定的，依照其规定。该条例中的个人信息境内存储的相关规定与之对应。两部文件的基本原则都是个人信息和重要数据应在境内存储，确需出境的需要对其进行评估。本报告认为，此项规定需要关键信息基础设施运营者引起重视。

3.4.2《个人信息和重要数据出境安全评估办法》（征求意见稿）

按照该办法的规定，数据出境是指“网络运营者”将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织和个人。而在《网络安全法》中，仅要求“关键信息基础设施的运营者”承担此项义务，对“网络运营者”并无此项要求。

首先，出境的个人信息和重要数据是在中国境内的运营中收集和产生的，而后被用于提供给境外的机构、组织和个人。而《信息安全技术 数据出境安全评估指南》（征求意见稿）中将对这一概念进行了更具体的阐述，即所谓提供，可以是直接提供，也可以是“通过开展业务、提供服务、产品等方式提供”；可以是一次性活动，也可以是连续性活动。并且该办法列举了属于数据出境的若干情况。

其次，该办法还提出了个人信息和重要数据出境的安全评估流程、要点和方法，其适用于网络运营者开展的个人信息和重要数据出境安全自评估，也适用于国家网信部门、行业主管部门组织开展的对于个人信息和重要数据出境的安全评估，细化了《网络安全法》中关于个人信息与重要数据的规定。此外，该办法增加了有关个人敏感信息、对个人信息和重要数据的加工处理、数据出境安全风险、数据脱敏处理和个人信息主体同意等要求。

3.4.3《信息安全技术 数据出境安全评估指南》（征求意见稿）

全国信息安全标准化委员会于 2017 年 8 月 30 日发布了《信息安全技术 数据出境安全评估指南》的征求意见稿。在该征求意见稿中，本报告认为，有几则要点需要注意。

首先，该评估指南对于限制数据出境的主体进行了扩大化的解释。《网络安全法》中规定，关键信息基础设施运营者在中国境内运营中收集和产生的个人信息和重要数据应当在境内存储，即《网络安全法》中对于限制数据出境的主体仅包括关键信息基础设施运营者。但是该评估指

南中却规定：“本标准适用于网络运营者开展的个人信息和重要数据出境安全自评估，以及国家网信部门、行业主管部门组织开展的个人信息和重要数据出境安全评估。”即该评估指南将限制数据出境的主体扩大为所有的网络运营者，这是与《网络安全法》的相关规定违背的。

其次，该评估指南对“境内运营”进行了定义。其规定没有在中国境内注册的网络运营者，但是在中国境内开展业务或向中国境内提供产品或服务的，属于境内运营。而判断的参考因素如下：是否使用中文；是否以人民币作为结算货币；是否向中国境内配送物流等。若满足这些参考因素中的一种或多种，即使未在中国境内注册的网络运营者也被视为在境内运营，需要按照《网络安全法》第三十七条的规定视具体情况进行安全评估。

再次，该评估指南对数据出境的情形进行了列举，还规定，非在境内运营中收集和产生的个人信息和重要数据经本国出境，未经任何变动或加工处理的，不属于数据出境；非在境内运营中收集和产生的个人信息和重要数据在境内存储、加工处理后出境，不涉及境内运营中收集和产生的个人信息和重要数据的，不属于数据出境。

最后，该评估指南对于数据安全评估的总体流程进行了细化。规定首先评估数据出境的目的；数据出境目的不具有合法性、正当性和必要性的，不得出境。在此基础上评估数据出境安全风险，将数据出境及再转移后被泄漏、损毁、篡改、滥用等风险有效地降至最低限度。

3.5 定期安全检测评估义务

加强网络安全保护首先要了解到网络自身的脆弱性和所面临的风险，因此开展定期检测评估活动就是获取此类信息的重要途径。关键信息基础设施的运营者应当履行每年至少进行一次检测评估的义务，可以自行依照相关规范和标准进行检测和评估，也可以委托网络安全服务机构开展此项工作，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门，对于定期安全检测评估义务，2017 年的法律法规规定如下。

3.5.1《互联网新业务安全评估管理办法》（征求意见稿）

该办法以安全评估报告制度为核心，并配有其他相关制度。安全评估报告制度基本流程以及对于电信业务经营者的相应要求如表二十六所示。

表二十六

评估启动

评估启动的情形包括：
（一）拟将互联网新业务面向社会公众上线的（含合作推广、试点、商用试验）；
（二）电信管理机构书面要求电信业务经营者进行安全评估的。

评估方式

电信业务经营者可以采取自行评估的方式，也可以委托专业机构实施评估。

风险控制

电信业务经营者发现存在重大网络信息安全风险的，应当及时改正。

评估报告

电信业务经营者应当在互联网新业务面向社会公众上线后 45 日内，向相应电信管理机构告知评估情况。

纠正措施

电信业务经营者提供的互联网新业务安全评估材料不齐全的，电信管理机构应当指导电信业务经营者补正。

以上是新业务安全评估的简单流程，有关评估的标准，尚待工信部后续出台更为细致的办法；有关评估的要求，应当按照相应的标准，同时注重于用户个人信息保护、网络安全防护、网络信息安全、建立健全相关管理制度等方面。

除了最重要的安全评估制度之外，企业内部还需建立重大网络信息安全事件应急处置机制，内部互联网新业务安全评估管理制度和保障制度，以及相关的员工的培训和考核制度。而监管机关自身也要对相应的经营者开展日常的监督检查，涉及的措施有监测、约谈改正和行业通报。

在上述制度执行的情形下，企业应对此进行按期至少每 6 个月自查，应保留自查记录，一旦开展互联网新闻信息服务单位内容管理从业人员管理办法则要求在 45 日内完成评估。同时，为了鼓励企业的自身发展，当开展电信业务满 3 年之时就纳入日常监管，不再进行安全评估以囿于企业开展业务。

3.5.2《关键信息基础设施安全保护条例》（征求意见稿）

该条例中涉及到的安全监测评估义务与《网络安全法》的评估制度相一致，规定了运营者应当建立健全关键信息基础设施安全检测评估制度，关键信息基础设施上线运行前或者发生重大变化时应当进行安全检测评估。运营者应当自行或委托网络安全服务机构对关键信息基础设施的安全性和可能存在的风险隐患每年至少进行一次检测评估，对发现的问题及时进行整改，并将有关情况报国家行业主管或监管部门。

3.5.3《信息安全技术 信息安全服务提供方管理要求》

该管理要求细化了《网络安全法》中对于网络安全服务的规定。《网络安全法》中规定，关键信息基础设施的运营者应当自行或者委托网络安全服务机构其网络的安全性和可能存在的风险每年至少进行一次检测评估的义务。

3.5.4《信息安全技术 关键信息基础设施安全检查评估指南》（征求意见稿）

该评估指南主要规定了检查评估方对于个人信息和重要数据保护情况的检查内容：

第一，检查关键信息基础设施运营单位搜集个人信息和重要数据的目的和范围，是否存在超出用户授权范围的内容或违反相关法律法规的情况；

第二，检查关键信息基础设施运营单位是否建立健全用户信息保护制度；

第三，检查关键信息基础设施运营单位应具有个人信息和重要数据安全事件的投诉和举报机制，查看其相关证明材料；

第四，检查关键信息基础设施运营单位公开或对外提供的用户个人信息范围，是否超出法律、行政法规规定和用户约定的范围。

以上检查评估的内容，顺应了《网络安全法》中规定的关键信息基础设施运营者对于个人信息和重要数据的保护义务。

第十二章 网络信息安全相关法律法规

网络信息安全主要涉及网络个人信息保护、违法信息处置等问题。随着个人信息保护立法的日益完善，企业需妥善履行用户个人信息保护义务。在网络信息安全执法的角度，实践中的案件主要集中在网站的信息内容管理方面，后果主要集中在约谈、警告、罚款和责令整改方面，具体可见第三章表二十三。

1. 个人信息保护义务

1.1《民法总则》

《民法总则》在其第一百一十一条对个人信息的保护进行了概括性的规定，要求“任何组织和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”。

该条将个人信息权正式纳入了民事保护的范围，规定了个人信息的获取者有确保信息安全的义务：在获取信息的过程中应该对信息安全或遭遇的威胁与风险予以高度审慎与警惕，同时要求信息的收集、使用、加工、传输他人信息的过程必须遵循合法的手段并征求被收集者的同意。从字面不难发现，该条款直接规定了个人信息安全的保护规则，规定了个人信息收集者“确保信息安全”的义务，从而保护个人信息安全。

此外，《民法总则》还主张自然人享有隐私权，将个人信息权与隐私权做出区分，确立了个人信息权的独立地位，增加个人信息权遭到侵害时受害者可以选择的救济途径，体现了大数据环境下对于个人信息保护的高度重视。结合《网络安全法》中对于个人信息的定义，将隐私权与个人信息权做出明确的区分，从而为个人信息权遭到侵害提供独立的请求权基础，为个人信息权提供有效的救济手段，对保护个人信息权大有裨益。

《民法总则》第一百二十七条将“虚拟财产”明文纳入保护范围，扩大数据保护的宽度，能够更加全面地保护数据安全与公民财产。虚拟财产常见的有网络游戏空间存在的虚拟财物，包括游戏账号等级、游戏货币、游戏人物拥有的各种装备等等。这些虚拟财产在一定条件下可以转换成现实中的财产。本条弥补了我国法律在虚拟财产保护上的空白，正式承认了网络虚拟财产的财产属性，为虚拟财产的保护了提供法律依据。然而，需要注意的是，该条款具有概括性、宣示性，无法作为直接依据来援引。故而虚拟财产、数据如何定义与界定、如何保护等问题，仍需要更加具体的法律规范予以填充。

1.2《电子商务法（征求意见稿）》

2013 年 12 月 7 日，全国人大常委会召开了《电子商务法》第一次起草组的会议，正式启动了《电子商务法》的立法进程。

2017 年 10 月 31 日，《电子商务法（草案）》第二次提交全国人大常委会审议，相较于一审稿，二审稿进一步体现了对电商平台义务的规范和对消费者权益的保护，在经营主体、信息安全、交易安全保障、打击假货、规范广告排名、交易规则公示、信用评价机制、知识产权保护、电子发票、先行赔付规则、物流快递服务、订单合同生效规定、维权机制等方面做了明确法律规定。[2]

1.2.1 个人信息

《电子商务法》中所指的“个人信息”是电子商务经营主体在电子商务活动中收集的姓名、身份证件号码、住址、联系方式、位置信息、银行卡信息、交易记录、支付记录、快递物流记录等能够单独或者与其他信息结合识别特定用户的信息。由此可见，《电子商务法》中所指的个人信息，相较于《网络安全法》中所指个人信息，更加具体。它结合了电子商务本身的特点，涵盖了网上交易的各个环节中可能涉及的个人信息，不仅包括个人住址、联系方式等常规信息，也包括支付过程中的银行卡、网络账户和配送过程中的物流记录等信息。

1.2.2 信息收集

《电子商务法（征求意见稿）》对于电子商务经营主体收集用户个人信息的过程作出了相关规定。

首先，电子商务经营主体收集用户个人信息应当遵循合法、正当、必要原则，事先向用户明示信息收集、处理和利用的规则，并征得用户的同意。

其次，电子商务经营主体不能采用非法交易、非法入侵、欺诈、胁迫等手段收集个人信息，如以拒绝为用户提供服务为由强迫用户同意其收集个人信息等。

最后，电子商务经营主体如果想要修改个人信息收集规则，应当取得用户的同意或向用户提供相应的救济方法。

1.2.3 信息利用

此次的《电子商务法》二次审议稿对个人信息的处理和利用也做出了规定。概括性的原则是：电子商务经营主

2.《独家 | 首部 < 电商法 > 草案二审出炉 电商中心专家为你划七大重点》，http://wemedia.ifeng.com/35847239/wemedia.shtml，于 2017 年 11 月 14 日最后一次访问。

体处理和利用用户个人信息，应当符合用户同意的处理利用规则，即当变更收集信息时约定的处理、利用的目的、方式和范围时，应当告知用户，并征得用户的明示同意。且一旦法定或者约定保存期限届满，就应当主动或者按照用户的请求停止处理、利用，或者删除、销毁相关个人信息。

与信息的收集相同，经营主体也不得以拒绝为用户提供服务为由强迫用户同意其收集个人信息；如果想要修改个人信息收集规则，应当取得用户的同意或向用户提供相应的救济方法。

1.2.4 信息管理

电子商务经营主体在保护、管理用户个人信息方面也负有义务。

一方面，应当建立健全内部控制制度和技术管理措施，防止信息泄露、丢失、毁损，确保电子商务数据信息安全。另一方面，在发生或者可能发生用户个人信息泄露、丢失、毁损时，也应当立即采取补救措施，及时告知用户，并向有关部门报告。

1.2.5 信息交换

电子商务经营主体交换共享电子商务数据信息的，应当对数据信息进行必要的处理，使之无法识别特定个人及其终端，并且无法复原。“经过处理无法识别特定个人且不能复原”这一匿名化标准为大数据流通和交易环节提供了法律依据。

1.2.6 用户权利

《电子商务法》在规定了电子商务经营主体的义务的同时，也对用户的权利作出了规定。

在信息查询方面，用户有权查询与本人有关的个人信息。电子商务经营主体收到用户查询请求的，应当在核实身份后及时提供查询结果。用户对错误信息提出更正补充请求的，电子商务经营主体应当及时更正补充。在个人信息处理利用方面，若电子商务经营主体的行为可能侵害自己合法权益，则用户有权请求中止相关行为。

1.3《测绘法》

地理信息安全也是最为重要的数据种类之一，近年来发生的对于个人轨迹的非法追踪以及境外组织的非法测绘等违法犯罪事件时有发生。《测绘法》的本次修订就显得非常必要。

宏观来看，本次修法中有关数据保护的条款主要涉及这两个方面：一是数据安全制度，二是个人信息保护。两者都是保护数据，一是针对地理信息本身，二是针对经过同意收集的个人信息。

本次修法新增的一项内容，即“卫星导航定位基准服务”。卫星导航定位基准站是国家重要的空间基础设施，是导航定位服务系统的重要组成部分，可以实现诸多民生领域的产品服务。在建设和运行维护卫星导航定位基准站时，相关企业应该格外注意对于“关键信息基础设施”的规定。同时，从事测绘活动的单位也应当建立安全保障措施、信息安全保密管理制度方可开展活动。

《测绘法》中另外涉及的是“互联网地图服务”，这是首次加入对于该种服务的监管措施。使用经依法审核批准的地图的前置行政审批包括：建立地图数据安全管理制度，采取安全保障措施。相关企业应重点关注此种安全管理制度该如何建设，以切实保障数据的安全。

此外，《测绘法》对于涉及国家秘密的地理信息规定了特别的制度，即要求进行登记和长期保存，达到可追溯管理。本法相对重要的是个人信息保护制度，这也是继《民法总则》、《网络安全法》等一系列法律出台后，将个人信息保护入法的又一典型。该规定适用于两个主体，一为地理信息生产和利用单位，二为互联网地图服务提供者。

1.4《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》

2017 年 5 月 10 日，最高人民法院、最高人民检察院联合发布《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》（简称“个人信息司法解释”），对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定。

1.4.1 对于“公民个人信息”的界定

根据个人信息司法解释，公民个人信息是指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身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。这一界定与《网络安全法》附则中的界定有所区别。

这一界定表明，在刑法的范畴内，对于公民个人信息的保护不单单局限在涉及隐私、可识别公民个人身份的类别。车辆档案、手机定位等反应公民活动情况的信息也在

被保护之列。理由在于，这些信息往往也具有商业价值，是值得《刑法》所保护的对象。

1.4.2 对于“提供公民个人信息”、“非法获取”的界定

根据个人信息司法解释，向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为《刑法》所规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于《刑法》第二百五十三条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。该司法解释还规定：违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法规定的“以其他方法非法获取公民个人信息”。

这一界定丰富了有关“提供公民个人信息”犯罪形态的规定。可见，通过互联网非法购买、交换、出售公民个人信息，构成侵犯公民个人信息罪。通过对“提供”与“非法获取”公民信息形态的扩大解释，强化了对公民个人信息的刑法保障。

1.4.3 其他

个人信息司法解释中还对该罪名的适用作出了一些具体化的规定。对于“情形严重”的界定，包括但不限于出售或者提供行踪轨迹信息，被他人用于犯罪的、非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的、违法所得五千元以上的等情形。对于“情形特别严重”的界定，包括但不限于造成被害人死亡、重伤、精神失常或者被绑架等严重后果的、造成重大经济损失或者恶劣社会影响的、利用非法购买、收受的公民个人信息获利五万元以上等情形。

另外，个人信息司法解释还规定了该罪名下单位犯罪的定罪量刑规则、个人信息数量计算规则、量刑规则等，均有利于依法惩治侵犯公民个人信息犯罪活动，保护公民个人信息安全和合法权益。

1.5《统计法实施条例》

《统计法实施条例》对于识别或者推断单个统计调查对象身份的确定以及使用途径都作出了细致的规定，这与《网络安全法》对于“个人信息”作出的定义是相对应的。《网络安全法》对于个人信息的解释是以“定义”加“列举”的方式，这种解释方法的涵盖范围就相当的广。而《统计法实施条例》对于“对象身份”的识别采取的是“标明”加“推断”，即最终的结论是：只要可以通过汇总资料推断出单个调查对象的身份，就可以看作是可识别。所以，本报告认为，两者所采取的解释方法本质上有异曲同工之处，均有一个类似兜底性质的条款去尽量的拓宽对于个人信息的保护范围，均将“可识别性”作为其根本的判断标准。

此外，该条例对于行政主体的权力进行了约束，对于可识别对象身份的信息进行严格管理，不得作为实施行政许可和行政处罚的依据，从而有效的保障了行政相对人的合法权益。

1.6《残疾人教育条例》

由于这部条例的着重点就是在于关注残疾人教育事业的发展，因此在条例中涉及网络安全或者个人信息保护的条文极为有限，仅为一款，下文将对该款（条例第二十条第三款）进行分析。

第二十条中只有第三款涉及到对于残疾人个人信息的保密义务。依照规定作出的评估结果属于残疾儿童、少年的隐私，仅可被用于对残疾儿童、少年实施教育、康复。教育行政部门、残疾人教育专家委员会、学校及其工作人员对在工作中了解的残疾儿童、少年评估结果及其他个人信息负有保密义务。

教育行政部门、残疾人教育专家委员会、以及学校，这些主体都具有网络运营者的身份。因此，该条例规定的教育行政部门、残疾人教育专家委员会、学校以及其他工作人员对残疾儿童的个人隐私应负的信息保密义务，可看作是《网络安全法》中个人信息保密义务在残疾人教育领域内作出的细化规定。

1.7 国家网信办有关互联网信息服务的管理规定

2017 年，国家互联网信息办公室在《网络安全法》实施的大背景下，出台了数个有关互联网信息服务的相关规定：《互联网群组信息服务管理规定（以下简称“群组规定”）、《互联网用户公众账号信息服务管理规定》（以下简称“公众账号规定”）、《互联网论坛社区服务管理规定》（以下简称“论坛社区规定”）、《互联网跟帖评论服务管理规定》（以下简称“跟帖评论规定”）和《互联网新闻信息服务管理规定》（以下简称“新闻规定”）。表二十七和表二十八是法规概览。

表二十七

法规名称	制定机关	通过时间	生效时间
《互联网新闻信息服务管理规定》	国家互联 网信息办公室	2017年5月2日	2017年6月1日
《互联网跟帖评论服务管理规定》		2017年8月25日	2017年10月1日
《互联网论坛社区服务管理规定》			
《互联网用户公众账号信息服务管理规定》		2017年9月7日	2017年10月8日
《互联网群组信息服务管理规定》			

这五部规定在编纂体例和具体条款上均有一定的相似性。可以认为，它们是《网络安全法》在互联网信息传播领域对主要的几种互联网产品和服务的具体细化。

表二十八

个人信息保护的规定	
《群组规定》	互联网群组信息服务提供者应当按照“后台实名、前台自愿”的原则，对互联网群组信息服务使用者 进行真实身份信息认证，用户不提供真实身份信息的，不得为其提供信息发布服务。 互联网群组信息服务提供者应当采取必要措施保护使用者个人信息安全，不得泄露、篡改、毁损， 不得非法出售或者非法向他人提供。
《公众账号规定》	互联网用户公众账号信息服务提供者应当采取必要措施保护使用者个人信息安全，不得泄露、篡改 、毁损，不得非法出售或者非法向他人提供。
《论坛社区规定》	互联网论坛社区服务提供者应当按照“后台实名、前台自愿”的原则，要求用户通过真实身份信息认 证后注册账号，并对版块发起者和管理者实施真实身份信息备案、定期核验等。用户不提供真实身份 信息的，互联网论坛社区服务提供者不得为其提供信息发布服务。 互联网论坛社区服务提供者应当保护用户身份信息，不得泄露、篡改、毁损，不得非法出售或者非 法向他人提供。
《跟帖评论规定》	（一）按照“后台实名、前台自愿”原则，对注册用户进行真实身份信息认证，不得向未认证真实身 份信息的用户提供跟帖评论服务。 （二）建立健全用户信息保护制度，收集、使用用户个人信息应当遵循合法、正当、必要的原则， 公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。
《新闻规定》	互联网新闻信息服务提供者为用户提供互联网新闻信息传播平台服务，应当按照《中华人民共和国 网络安全法》的规定，要求用户提供真实身份信息。用户不提供真实身份信息的，互联网新闻信息服 务提供者不得为其提供相关服务。 互联网新闻信息服务提供者对用户身份信息和日志信息负有保密的义务，不得泄露、篡改、毁损， 不得出售或非法向他人提供。

可见，信息服务提供者保障用户个人信息安全的举措基本相同。具体来说，就是各规定中的“实名制”和收集其他个人信息的要求。然而，“实名制”在网络安全的大背景下可以说是一把双刃剑，一方面，它使得任何网络安全威胁的出现都可以尽快得到解决，因此在这个层面上，相关规定出现在《网络安全法》第三章“网络运行安全”；但是另一方面，“实名制”或多或少也产生了用户个人隐私信息泄露的风险，这同样关乎网络信息安全，值得保护，因此相关的规制被规定在了第四章“网络信息安全”。国家网信办在起草上述规定时也注意到了这个问题，将其共同规定在了同一条款中进行规制。可见，国家网信办对于网络运行安全与信息安全两者都予以了高度重视。

通观五部规定，在互联网信息服务当中，对于个人信息收集规则的规定均包括“后台实名、前台自愿”。相关上位法依据规定在《网络安全法》第二十四条。从某种意义上来说，今后在互联网信息服务当中，不应当再允许“游客”这一身份存在。网信办的五部规定中的规定和上位法的表述基本一致，且在这基础上又创立了“前台自愿”的规则，也为个人信息的保护又增添了一道屏障。

1.8《信息安全技术 个人信息去标识化指南》（征求意见稿）

该标准描述了个人信息去标识化的目标和原则，提出了去标识化过程和管理措施。《网络安全法》中设专章“网络信息安全”，竭力保护个人信息安全，提出了网络经营者应当建立健全用户信息保护制度。而本标准就是其中采取的一种重要的技术措施，以保护个人信息。从技术层面来讲，本标准主要是为微数据提供具体的个人信息去标识化指导，针对相关标识符进行删除或变换等技术处理，避免攻击者根据这些属性直接识别或者结合其它信息识别出原始个人信息主体。

1.9《信息安全技术 个人信息安全规范》

《信息安全技术 个人信息安全规范》（以下简称为“安全规范”）作为国家推荐标准，于 2017 年 12 月 29 日发布，自 2018 年 5 月 1 日正式施行。它“针对个人信息面临的安全问题，规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益”。

个人信息控制者，指有权决定个人信息处理目的、方式等的组织或个人。“安全规范”主要从以下方面规范了个人信息控制者在信息处理环节中的相关行为：

1.9.1 确定个人信息安全基本原则

安全规范规中规定，个人信息控制者开展个人信息处理活动，应遵循表二十九中的基本原则。

表二十九

原则	解释
权责一致原则	对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任
目的明确原则	具有合法、正当、必要、明确的个人信息处理目的
选择同意原则	向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意
最少够用原则	除与个人信息主体另有约定外，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息
公开透明原则	以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督
确保安全原则	具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性
主体参与原则	向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法

1.9.2 个人信息收集的要求

安全规范要求信息控制者收集个人信息时，需要符合合法性、最小化、授权同意的要求。具体要求见表三十。

表三十

要求	含义
收集个人信息合法性要求	a）不得欺诈、诱骗、强迫个人信息主体提供其个人信息； b）不得隐瞒产品或服务所具有的收集个人信息的功能； c）不得从非法渠道获取个人信息； d）不得收集法律法规明令禁止收集的个人信息
收集个人信息最小化要求	a）收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现； b）自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率； c）间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量
收集个人信息时授权同意	收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则（例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等），并获得个人信息主体的授权同意

1.9.3 附件

为了提高个人信息控制者遵守安全规范的可操作性，安全规范的附录中提供了参考资料与模板，让企业能够在实践中顺利履行相应义务，包括：

隐私政策模板：包括收集、使用个人信息的目的以及目的所涵盖的各个业务功能，例如，将个人信息用于推送商业广告，或用于形成直接用户画像及其用途等。此模板可以帮助企业制定合规的隐私政策。

功能界面模板：安全规范提供了个人信息控制者向个人信息主体就个人敏感信息的收集、使用以及个人信息的共享、转让、公开披露等事项征求授权同意的实现方法。个人信息控制者可参考安全规范附录中的功能界面模板设计功能界面，保障个人信息主体能充分行使其选择同意的权利。

个人信息、个人敏感信息示例：该附件主要通过举例说明的方式，对“个人信息”和“个人敏感信息”的判定提供帮助，供个人信息控制者知悉所收集的个人信息所述类别。

2. 违法违规信息管理

网络运营者不仅对其自己做出的行为负有义务，对其平台上的用户发布的信息也负有管理义务。网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

2.1 网信办有关互联网信息服务的管理规定

在 2017 年，国家网信办针对互联网信息服务，颁布了一系列的规定（表三十一），涉及互联网信息服务的方方面面。

表三十一

违法违规信息管理的规定	
《群组规定》	互联网群组信息服务提供者和使用者不得利用互联网群组传播法律法规和国家有关规定禁止的信息内容。
《公众账号规定》	互联网用户公众账号信息服务使用者不得通过公众账号发布法律法规和国家有关规定禁止的信息内容。 互联网用户公众账号信息服务提供者应加强对本平台公众账号的监测管理，发现有发布、传播违法信息的，应当立即采取消除等处置措施，防止传播扩散，保存有关记录，并向有关主管部门报告。
《论坛社区规定》	互联网论坛社区服务提供者不得利用互联网论坛社区服务发布、传播法律法规和国家有关规定禁止的信息。 互联网论坛社区服务提供者应当加强对其用户发布信息的管理，发现含有法律法规和国家有关规定禁止的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并及时向国家或者地方互联网信息办公室报告。
《跟帖评论规定》	对新闻信息提供跟帖评论服务的，应当建立先审后发制度； 提供“弹幕”方式跟帖评论服务的，应当在同一平台和页面同时提供与之对应的静态版信息内容。 跟帖评论服务提供者对发布违反法律法规和国家有关规定的信息内容的，应当及时采取警示、拒绝发布、删除信息、限制功能、暂停更新直至关闭账号等措施，并保存相关记录。
《新闻规定》	互联网新闻信息服务提供者和用户不得制作、复制、发布、传播法律、行政法规禁止的信息内容。 互联网新闻信息服务提供者提供服务过程中发现含有违反本规的内容的，应当依法立即停止传输该信息、采取消除等处置措施，保存有关记录，并向有关主管部门报告。

除了《群组规定》以外，其他四项规定都有涉及“先审后发”、“实时巡查”、“监测”、“立即”、“及时”等字样，也即，相关的监管部门是有权力实时监测后四种互联网信息服务的，即公众账号、论坛社区、新闻信息、跟贴评论。

本报告提醒，应当注意一下每部规定当中特殊的规定和新建的制度，如《群组规定》中的分级分类管理制度、信用等级管理体系和唯一群组识别编码等；《公众账号规定》中的公众账号数据库和分级分类管理制度等；《跟帖评论规定》中的新闻评论先审后发制度、反垃圾信息管理系统、用户分级管理制度、用户信用评估制度等；《新闻规定》中的许可制度、总编辑负总责制度，将主管部门由“国务院新闻办公室”调整为“国家互联网信息办公室”等。另外，《新闻规定》中对于法律责任的设置相较其他四部更为丰富，但是其也存在指引性规范指向《网络安全法》，因此，其他四部规定如果对于责任的设置模糊不清的话，可参照《网络安全法》中的规定。

第十三章
其他法律法规

虽然“网络运行安全”与“网络信息安全”相关的法律法规已高度覆盖“网络安全”的内涵，但是仍然有部分法律法规的补充对于网络运营者履行网络安全义务有积极意义。本章将介绍除网络运行安全与信息安全外，网络运营者在网络运行、数据收集过程中需要注意的法律规范。

1. 反不正当竞争法

新修订的《反不正当竞争法》，于 2018 年 1 月 1 日起开始施行。此次修订是这部法律自 1993 年实施以来二十四年的首次修订。对比原《反不正当竞争法》，修订后的版本针对互联网领域的迅速发展，增加了有关互联网不正当竞争行为的条款，主要规定了经营者不得利用技术手段在互联网领域从事影响用户选择、干扰其他经营者正常经营的行为，同时在第十二条列举了相关应予禁止的行为：

（一）未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转；

（二）误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务；

（三）恶意对其他经营者合法提供的网络产品或者服务实施不兼容；

（四）其他妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。

可以看出，这些列举的不正当竞争行为均需通过专业的计算机和网络技术行使，且直接侵害其他经营者与消费者的权益。

第一项的行为可见于最高人民法院发布的第 45 号指导案例“北京百度网讯科技有限公司诉青岛奥商网络技术有限公司等不正当竞争纠纷案”。案件中，三被告利用网通的互联网接入网络服务，在百度公司网站的搜索结果页面强行增加广告，损害了百度公司的商誉和经济效益，违背了诚实信用原则，构成不正当竞争。

第二项和第三项行为可见于“北京奇虎科技有限公司、奇智软件（北京）有限公司与腾讯科技（深圳）有限公司、深圳市腾讯计算机系统有限公司不正当竞争纠纷案”。在本案诉至法院之前，双方之间就采取诸如互不兼容的措施，进一步加剧了纠纷和矛盾。最终法院认定，奇虎公司针对腾讯公司拥有的 QQ 软件专门开发了扣扣保镖，该软件鼓励和诱导用户删除 QQ 软件中的增值业务插件、屏蔽客户广告，破坏了合法运行的 QQ 软件及其服务的安全性、完整性，使腾讯公司丧失合法增值业务的交易机会及广告、游戏等收入，偏离了安全软件的技术目的和经营目的，且主观上具有恶意，构成不正当竞争。

此前，针对互联网不正当竞争行为，法院进行判断时多会援引原《反不正当竞争法》第二条的基本原则，即该行为是否符合诚实信用原则及公认的商业道德和商业惯例。修订后第十二条的增加，将为司法机关裁判互联网不正当竞争行为列举更为明确的法律规则，使得相关的审判更有指向性和针对性。

2. 互联网信息内容管理行政执法程序规定

《互联网信息内容管理行政执法程序规定》（简称“执法程序规定”）是一部专门的程序性部门规章。

“执法程序规定”的目的是规范和保障互联网信息内容管理部门依法履行职责，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益。值得一提的是，执法程序规定的上位法依据中还提到了《行政处罚法》。网信办相关负责人在答记者问过程中也提到了该规定“确保互联网信息内容管理部门依法正确实施行政处罚”的意义。

根据《行政处罚法》，国务院部、委员会制定的规章可以在法律、行政法规规定的给予行政处罚的行为、种类和幅度的范围内作出具体规定。尚未制定法律、行政法规的，前款规定的国务院部、委员会制定的规章，对违反行政管理秩序的行为，可以设定警告或者一定数量罚款的行政处罚。罚款的限额由国务院规定。因此，我们应当注意到一部部门规章能够设定的行政处罚的边界。

“执法程序规定”主要包括表三十二中的五个方面。

表三十二

内容	具体要求
确定执法主体和范围	国家和地方互联网信息办公室实施行政执法，对违反有关互联网信息内容管理法律法规规章的行为实施 行政处罚，适用本《程序规定》
建立执法督查制度	国家和地方互联网信息内容管理部门建立行政执法督查制度，上级互联网信息内容管理部门对下级互联 网信息内容管理部门实施的行政执法进行督查
加强执法体系建设	国家和地方互联网信息内容管理部门要建立健全执法人员培训、考试考核、资格管理和持证上岗制度， 明确执法证由国家互联网信息内容管理部门统一制定、核发，或授权省、自治区、直辖市互联网信息内容 管理部门核发
以行政执法办案为主线，明 确执法程序	全面规范了管辖、立案、调查取证、听证、约谈、决定、执行等各环节的具体程序要求
规定常用文书格式范本	国家互联网信息内容管理部门制定执法文书格式范本，并在附件中列明了立案审批表、案件处理意见报告、行政处罚决定书等 17个常用文书格式范本

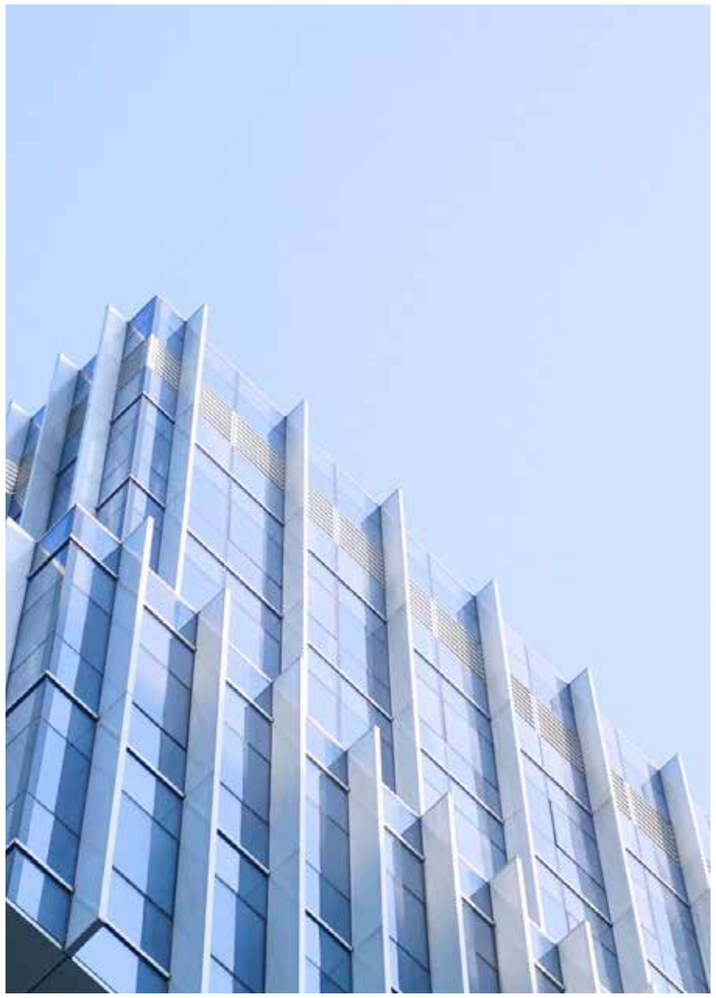
“执法程序规定”涉及内外监管两个方面。“内部监管”涉及上级对下级的执法督查、相关执法人员的培训和资格管理。“外部监管”即以行政执法办案为主线的执法程序，具体环节主要包括：管辖；立案；调查取证；听证、约谈；处罚决定、送达；执行与结案。

在管辖方面，“执法程序规定”对互联网信息内容违法行为的管辖进行了明确的规定，具体包括地域管辖、级别管辖、移送管辖、指定管辖和管辖权的转移等。

除此之外，从立案到结案的整个执法程序，流程如表三十三所示。

表三十三

阶段	相关规定	涉及的重要文书
立案	立案条件与期限、办案人员的回避	《案件来源登记表》 《立案审批表》
调查取证	调查取证要求、保密义务、取证类别、先行登记保存与处理决 定、调查终结与撰写报告	《案件处理意见报告》
听证、约谈	适用听证范 围【吊销互联网新闻信息服务许可 证、较大数额罚款 等】、听证时限要求、约谈	《举行听证通知书》 《听证笔录》 《执法约谈笔录》
处罚决定、送达	陈述申辩权、复杂重大案件的集体讨论、行政处罚决定的作出与送达	《行政处罚意见告知书》 《行政处罚决定书》
执行与结案	当事人履行义务与复议诉讼权利、强制执行	《行政处罚强制执行申请书》 《行政处罚结案报告》



第五部分
数据合规指引

2018 年可以被视为中国企业开展数据合规的关键之年。《网络安全法》的正式实施为数据合规奠定了基础，公众对于数据保护的意识不断提升，企业保护自身数据安全、保护用户个人隐私的能力已经成为了企业的核心竞争力之一。

然而，现阶段企业在数据合规方面的工作仍面临一定的不确定性，主要出于两方面的原因：一方面，《网络安全法》的诸多实施细则、技术标准尚在征求意见阶段。2017 年底发布的《全国人大常委会检查组关于一法一决定实施情况的报告》指出：“作为网络安全管理方面的基础性法律，网络安全法不少内容还只是原则性规定，真正‘落地’还有赖于配套制度的完善。”另一方面，报告也认为：“网络安全监管‘九龙治水’现象仍然存在，权责不清、各自为战、执法推诿、效率低下等问题尚未有效解决，法律赋予网信部门的统筹协调职能履行不够顺畅。”这些客观存在的问题均为企业的数据保护工作带来了不确定性，更加需要企业慎重对待数据合规问题。

因此，企业的数据合规就成为了一项必要却难以实施的工作。从 2017 年下半年开始，企业因未履行数据保护或网络安全义务而被相关部门给予行政处罚的案件不断增多，可见不少企业在数据合规方面的工作亟需进一步加强。

本报告调研问卷结果也反映出大量企业数据合规的意识明显欠缺，对于自己所需要承担的义务缺少系统的认识。

本报告认为，数据合规工作与其他合规事项相似，均与风险管理息息相关，因此可以从“主动防御”与“危机应对”两个角度进行。由于数据一经泄露就再也难以被控制，所造成的损害已经形成，因此主动防御的工作更为重要。而对于危机应对，其作为事后补救措施，也不应被忽视。本报告建议，企业应当在了解自身情况与外部风险的前提下，尽快着手制定并实行数据合规工作。

因此，报告本部分将针对数据合规工作中所面对的重点问题，提供切实可行的指引，帮助企业的数据合规工作。

第十四章
主动合规

1. 身份识别

由于不同的主体需要承担不同的义务，因此，企业自身主体地位的识别成为数据合规的第一步。《网络安全法》规定的主体主要包括：网络运营者，关键信息基础设施运营者，网络产品、服务提供者。以上三个主体并不是非此即彼的关系，有时会出现某一主体既是网络运营者，又是关键信息基础设施运营者的情况，还可能出现某一主体同时是网络产品、服务提供者的情况。

网络运营者是《网络安全法》中最为基础的概念，包括网络的所有者、管理者和网络服务提供者。这一概念极为宽泛，甚至局域网和工业控制系统的运营者都可以成为网络运营者。因此，几乎所有企业都可能被纳入《网络安全法》下网络运营者的范畴内。

尽管《网络安全法》提出了“关键信息基础设施运营者”的概念，《关键信息基础设施安全保护条例（征求意见稿）》也指出，五大类行业应被认定为关键信息基础设施运营者，但是关键信息基础设施运营者的范围仍没有得到清晰的界定。据《全国人大常委会检查组关于一法一决定实施情况的报告》所披露的数据，截止到 2017 年底，“目前全行业共确定关键网络设施和重要信息系统 11590 个”。另外，在 2016 年，国家互联网信息办公室（以下简称“国家网信办”）等部门组织开展了关键信息基础设施摸底排查工作，对 1.1 万个重要信息系统安全运行状况进行抽查和技术检测，完成了对金融、能源、通信、交通、广电、教育、医疗、社保等多个重点行业的网络安全风险评估。根据以上公开信息可以推断，若企业属于关键信息基础设施的运营者，目前应当已经收到相关通知。但值得注意的是，关键信息基础设施的名录并非一成不变，而是会根据实际情况进行不断调整。因此，本报告建议，相关企业需及时关注企业内外网络安全环境的变化。

网络产品、服务提供者是指通过信息网络向公众提供网络产品或信息服务的机构。该主体的范围也相对较宽，互联网企业大都属于该概念的范畴。根据国家网信办制定的《网络产品和服务安全审查办法（试行）》，如果网络产品、服务关系国家安全，则该产品（服务）应当经过网络安全审查。

2. 数据审计

2.1 数据

本报告认为，除了明确自身的主体地位，企业还应当对自己经营过程中涉及的各类数据有充分的了解。“维护网络数据的完整性、保密性和可用性”是《网络安全法》基本原则之一，我国法律规定了多种不同类型的数据（表十四），也分别对应不同的保护义务。

在《网络安全法》中，“个人信息”是最为重要也是最为敏感的一类数据，在对个人信息进行收集、储存、使用、共享时需要有专门设计的流程以与普通数据区别对待。

对于其他一些数据类型，也需要有特殊的管理规则，比如“重要数据”的概念。不同行业中的重要数据不尽相同，某些数据在一些行业里面可能属于重要数据，但在另一行业可能就无法被纳入重要数据的范畴，所以，本报告建议，企业需要根据自身所处的行业，判断哪些数据是法律意义上的重要数据。

除上述数据外，国家秘密、商业秘密、员工的个人信息以及需要面向公众进行开放的数据都需分类进行管理。

表三十四

数据类型	界定	法律依据
个人信息	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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等	《网络安全法》 《信息安全技术 个人信息安全规范》
个人敏感信息	一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康收到损害或歧视性待遇的个人信息。	《信息安全技术 个人信息安全规范》
重要数据	相关组织、机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据，经政府信息公开渠道合法公开的，不再属于重要数据）	《信息安全技术数据出境安全评估指南》（征求意见稿）
商业秘密	不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息	《反不正当竞争法》
国家秘密	国家秘密是关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。	《保守国家秘密法》

2.2 网络布局 (Network Mapping)

企业还需要对自己网络布局状况进行盘点，包括明晰存储数据的地理位置情况与网络系统部署情况两方面。

2.2.1 明晰存储数据的地理位置情况

《网络安全法》第三十七条规定了关键信息基础设施运营者的个人信息和重要数据境内存储义务和跨境传输安全评估义务。于此，本报告建议，企业需要明确以下要点：

第一，自身是否为关键信息基础设施运营者；

第二，收集和产生个人信息和重要数据的时点是否处于在中国大陆地区运营过程中，如是，则上述数据应在中国大陆境内存储；

第三，仅在业务需要的前提下，并经过安全评估尚可跨境传输至境外。

国家网信办在 2017 年 4 月 11 日发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》第二条中将上述义务的履行主体从“关键信息基础设施运营者”扩大为“网络运营者”。因该办法尚在征求意见阶段且层级效力较低，目前关于上述义务的履行主体仍应以《网络安全法》的规定为准。值得注意的是，2018 年 2 月 28 日起美国苹果公司旗下 iCloud 云服务在中国大陆境内的运营和服务已转由中国互联网服务公司云上贵州大数据产业发展有限公司提供，此举被认为是履行境内存储义务的典型。

2.2.2 明晰网络系统部署情况

本报告建议，企业应当主动了解自身所涉及的网络系统分布状况，是否存在多套相互独立的网络系统，以及企业内部除互联网外的局域网、工业控制系统的部署情况。

工业和信息化部针对工业控制系统，专门制订了《工业控制系统信息安全事件应急管理工作指南》、《工业控制系统信息安全防护指南》等文件，提出了多项安全要求。对于具有工业控制系统的企业，应当建立工控安全应急值守机制，实行领导带班、专人值守工作制度，做好工控安全风险、威胁、事件信息日常监测和报告工作；在应急响应状态下，实行“7×24”小时值守，加强信息监测、收集与研判，做好信息跟踪报告；在应急处置结束、系统恢复运行后，相关工业企业要尽快消除事件造成的不良影响，做好事件的分析总结工作，应在三十天内以书面形式报工业和信息化部等。

3. 合同保护措施

3.1 数据相关条款的审查

数据在企业的对外合作中扮演着重要的角色，在企业的对外合作中会有大量内容围绕数据的利用与共享，因此，本报告认为，关于数据有关合同条款的审查同样至关重要。比如企业在并购、收购时对交易对象的数据利用是否合法，企业开发的手机 App 从手机调用数据的范围，企业委托第三方对员工进行背景调查时个人信息的收集、存储，大量的数据有关条款需要法务部门与外部律师谨慎对待。

本报告认为，企业除了履行《网络安全法》等相关法律法规规定的义务之外，还可以通过自行订立合同中的数据条款，约定合同多方对于数据使用的规则，以实现数据保护。随着数据价值的提升，数据成为了企业之间合作的重要资源。围绕着数据资源，在 2017 年涌现出了大量争议。比如，本报告第三部分“案例与争议”部分讨论的几个典型案例：新浪微博与脉脉之间围绕着微博数据的授权使用对簿公堂，菜鸟网络与顺丰丰巢围绕数据接口开放的争议让部分快递业务陷入瘫痪，华为与微信也因为用户个人信息的利用产生争议。

本报告建议，企业还应当在涉及数据的合同中加入专门条款。当企业委托第三方来处理个人信息，或者为第三方收集个人信息时，需要在合同中让第三方承担同样的个人信息保护义务，以确保个人信息的保护，并且约定企业对第三方损害个人信息的行为免责。企业还可以对第三方个人信息保护情况的审计进行约定，以确保企业有权对第三方的数据保护情况进行审查。对于从第三方获取个人信息的情形，企业应在合同中要求第三方说明个人信息的来源，并对来源合法性进行确认。

3.2 网络产品和服务采购合同审查

《网络安全法》要求“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”（第三十五条）。尽管该义务仅针对关键信息基础设施运营者，但对于非关键信息基础设施运营者的企业来说，对采购网络产品和服务的合同加以检视也尤为必要。

因为产品（服务）的漏洞会不断出现，一些在采购时达到安全标准的产品（服务）可能会在投入使用后被发现存在漏洞。2018 年 1 月，安全人员发现了两个 CPU 漏洞，分别被命名为 Meltdown（熔断）和 Spectre（幽灵）。Meltdown 影响范围包括 1995 年之后的几乎所有 Intel CPU 型号；而 Specture 则能够影响几乎所有来自 Intel 和 AMD 的 CPU 型号，以及 ARM 旗下的一些 CPU 型号。事件发生后，Intel、微软、Google、苹果在内的多家公司纷纷针对这一漏洞做出了反应，并发布了相关声明。

漏洞层出不穷，也防不胜防，企业在采购网络产品（服务）时，并不是一次性的“一锤子买卖”，而是在整个产品（服务）周期中都需要技术支持的解决方案，所以，本报告建议，企业需要留意网络产品（服务）提供者对产品安全义务的承诺，即在产品出现漏洞或面临新的外部风险时，网络产品（服务）提供者是否需要承担立即就产品（服务）升级或采取安全措施。在合同中，需要网络产品（服务）提供者约定在发现漏洞后，告知的方式、期限，补救措施的部署方式，以及未履行该义务的违约责任。如果未对此进行约定，那么企业无法就网络产品（服务）提供者隐瞒漏洞的行为追究违约责任，相应的损失只能由企业自己承担。

4. 个人信息保护

在 2018 年初，支付宝因为在年度账单首页中嵌入一行“我同意《芝麻服务协议》”的小字，并且帮用户预先选择好了“同意”而引起争议，因协议条款涉及“你允许芝麻信用收集你的信息”等敏感内容。该行为经报道引起争议后，支付宝迅速将该行字及其所链接的协议从年度账单首页中撤下。国家互联网信息办公室网络安全协调局也就此事约谈了支付宝（中国）网络技术有限公司、芝麻信用管理有限公司的有关负责人。根据《网络安全法》的规定，企业运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。具体而言，需要在收集时明确获得用户的授权，用户需要有“同意”的意思表示。

用户协议是企业最为重要的数据相关合同，会涉及到个人信息的收集、存储、利用、共享，是行政部门的监管

重点，也是最容易引发公众事件的环节。如本报告第三部分“案例和争议”中提到的新浪微博诉脉脉案，法院在判决书中频繁援引了新浪微博《开发者协议》《微博服务使用协议》《微博个人信息保护政策》与《脉脉服务协议》，可见隐私条款的重要性。

随着《网络安全法》的正式施行与《信息安全技术 个人信息安全规范》（GB/T 35273–2007）的颁布，个人信息的合规已经成为企业经营过程中一个不可回避的问题。本报告提示，任何单位都应当对收集的个人信息严格保密，并建立健全用户信息保护制度。

对个人信息的保护是一个法律问题，也是一个商业问题，完善的个人信息保护措施可以增强企业的竞争力。近年来“经规划的隐私”（Privacy by Design）的理念被越来越多的企业接受。具体到获取“同意”的领域，不仅需要一份符合法律要求的协议文本，还需要确保用户的“同意”真实有效。这不只是一个法律问题，还是一个产品设计问题，需要确保“同意”的流程符合法律要求。

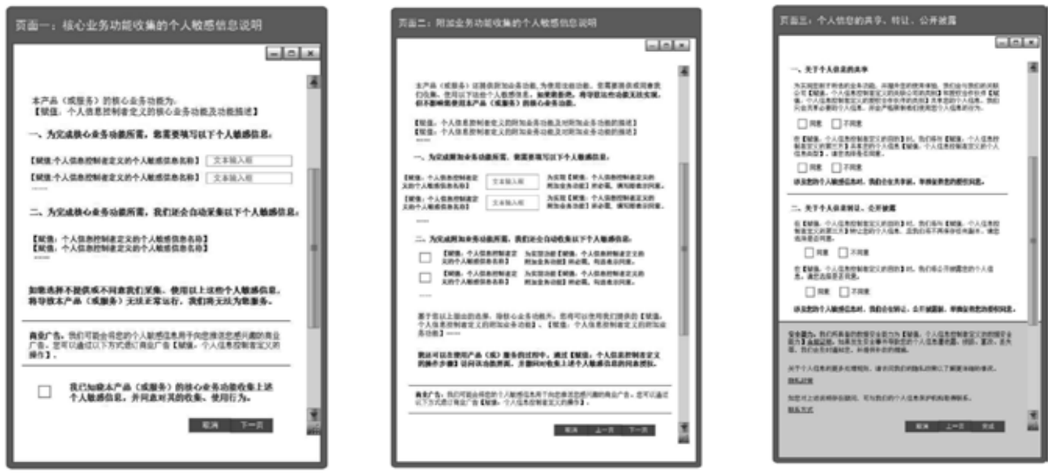
通过用户协议收集用户个人信息的，应在进行收集之前，如产品安装时，或用户首次使用产品（服务）时，或用户注册时，向用户展示收集个人信息的目的、种类等内容，并征得用户的明确同意，在需要用户勾选“确认”或“已知晓”有关收集、利用信息时，不应默认进行勾选，需要用户有点击行为。并且，企业应当提供“隐私政策”页面的链接，确保用户可以访问完整的文本。而本报告调研结果显示，仅有不到半数企业在收集用户个人信息时要求用户“点击同意”，有超过四成的企业并不清楚自己是如何获取用户的“同意”的。

本报告建议，在内容上，企业不仅需要做到明示收集、使用个人信息的规则，还需要为用户提供更多授权选择，提供个人信息的关闭授权和在线注销的功能。另外，企业还有必要修改隐私条款中语焉不详、晦涩难懂、避重就轻的文本，让隐私条款更规范、更清晰、责任更明确，使其独立成文，内容全面，重点突出。根据企业业务类型的不同，所涉及到的隐私政策也不尽相同。一旦涉及到第三方对所收集个人信息的利用，问题也会更加复杂。比如，对用户基因信息的收集一旦与精准保险、健康等方面利用关联起来，则会具有高度的敏感性；同时，可能需要对第三方公司的股东背景进行调查。因此，本报告认为，对个人信息的隐私政策的设计需要针对具体情况具体分析。

此外，法律要求企业不得泄露、篡改、毁损其收集的个人信息，一旦发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，及时告知用户并向有关主管部门报告。可能涉及犯罪的，如黑客入侵窃取个人信息，企业还应主动向公安机关报案。

5. 重要数据保护

重要数据是数据合规最为重要的对象之一。根据《重要数据识别指南》[1]，重要数据是指相关组织、机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：



图十二 用户个人信息收集功能界面（《信息安全技术 个人信息安全规范》）

a) 危害国家安全、国防利益，破坏国际关系；

b) 损害国家财产、社会公共利益和个人合法利益；

c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d) 影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；

e) 干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f) 危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；

g) 影响或危害国家经济秩序和金融安全；

h) 可分析出国家秘密或敏感信息；

i) 影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。

重要数据的概念非常宽泛，且不同行业（领域）的重要数据范畴都不相同。一些数据在能源领域属于重要数据，但在通信行业可能就不属于重要数据。因此，对于重要数据的判断，各行业的主管部门具有相当的话语权。

根据《网络安全法》的要求，企业对于重要数据的保护应当采取备份和加密等措施，法务部门需要确保这些措施符合法律要求，并且能够在需要时将采取的措施作为相关证据进行提供。

除此以外，关键信息基础设施运营者应将其在中国境内运营所收集的重要数据在中国境内进行存储，需要出境时，必须要先按照国家网信部门会同国务院有关部门制定的办法进行安全评估。因此，一旦企业被认定为关键信息基础设施运营者，需要明晰自己所涉的哪些数据属于重要数据，并做好重要数据境内存储的工作。

6. 制度设立

6.1 安全防护

企业开展网络安全防护工作，虽然很多内容需要技术部门、安全部门来完成，但法务部门与外部律师的角色同样不可或缺。本报告认为，法务部门与外部律师不仅需要确保有关电子数据在法庭上或面对政府调查时是合法有效的电子证据，更需要承担引导企业技术部门、安全部门开展的责任，确保技术部门、安全部门开展的安全防护工作符合《网络安全法》的要求。

等级保护制度是中国网络安全保护的基础。早在 1994 年，《计算机信息系统安全保护条例》首次明确提出计算机信息系统实行安全等级保护。2004 年，公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室联合制订了《关于信息安全等级保护工作的实施意见》，根据信息及信息系统的重要程度和危害程度将信息和信息系统的安全保护等级划分为五级：自主保护级、指导保护级、监督保护级、强制保护级、专控保护级。2017 年，《网络安全法》的正式实施将等级保护制度从行政法规上升到了法律层面，同时关于等级保护的一系列国家标准也正在修订中，保护对象也将进一步扩展。

本报告调研结果（图一）显示，没有如实履行该项义务的受访企业占比 31.02%。在 2017 年，也出现了一批因企事业单位未履行等级保护义务而被行政处罚的案件。在这些案件中，大多是在单位网站被黑客入侵后，网警部门发现被入侵的网络系统未进行等级保护测评，而对单位及单位网络安全主管人员进行约谈或处罚。截至 2017 年 12 月，中国已累计受理备案 14 万个信息系统，其中三级以上重要信息系统 1.7 万个，基本涵盖了所有关键信息基础设施。同时，有关部门对纳入等级保护的信息系统开展常态化检查，近年来累计发现整改各类安全漏洞近 40 万个。

信息系统定级工作应按照“自主定级、专家评审、主管部门审批、公安机关审核”的原则进行。定级工作的主要内容包括：确定定级对象、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核，具体可按照《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字〔2007〕861 号）的要求进行。各信息系统运营使用单位和主管部门是信息安全等级保护的责任主体，根据所属信息系统的重要程度和遭到破坏后的危害程度，确定信息系统的安全保护等级。同时，按照所定等级，依照相应等级的管理规范和技术标准，建设信息安全保护设施，建立安全制度，落实安全责任，对信息系统进行保护。

本报告提示，在等级保护工作中，信息系统运营使用单位和主管部门应按照“谁主管谁负责，谁运营谁负责”

1.《信息安全技术 数据出境安全评估指南（征求意见稿）》附录 A。

的原则开展工作，并接受信息安全监管部门对开展等级保护工作的监管。运营使用单位和主管部门是信息系统安全的第一责任人，对所属信息系统安全负有直接责任；公安、保密、密码部门对运营使用单位和主管部门开展等级保护工作进行监督、检查、指导，对重要信息系统安全负监管责任。由于重要信息系统的安全运行不仅影响本行业、本单位的生产和工作秩序，也会影响国家安全、社会稳定、公共利益，因此本报告认为，国家必然要对重要信息系统的安全进行监管。

6.1.1 初步确定安全保护等级

具体的等级确定，由等级测评机构对非涉及国家秘密信息系统安全等级保护状况进行检测评估。而根据《信息安全等级保护管理办法》的规定，如果涉及涉密信息系统，则应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

安全保护等级的确定一般由两个定级要素所决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。测评机构也是依照此最终确定安全保护等级。所谓等级保护对象受到破坏时所侵害的客体主要包括以下三个方面：

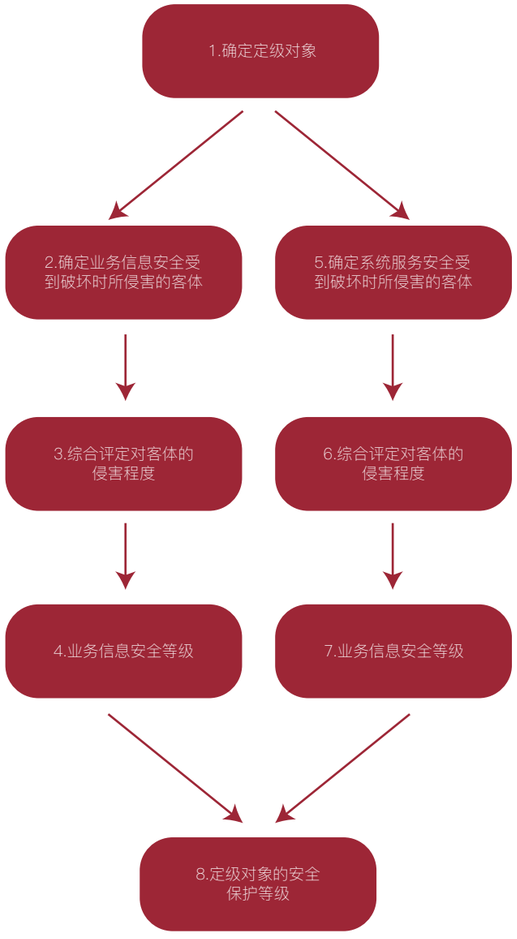
- 公民、法人和其他组织的合法权益；
- 社会秩序、公共利益；
- 国家安全。

所谓对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。等级保护对象受到破坏后对客体造成侵害的程度有三种：一是造成一般损害；二是造成严重损害；三是造成特别严重损害。

本报告提醒，信息系统安全包括了业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的信息系统安全保护等级称为业务信息安全等级。从系统服务安全角度反映的信息系统安全保护等级称系统服务安全等级。所以，确定安全保护等级应分别从业务信息和系统服务两方面的安全来评定。而在各自的评定中，前述两个定级要素也应分别衡量。流程如图十三所示。[2]

前述两个定级要素的不同组合对应着不同的安全保护等级，根据表三十五即可确定相应的等级。

图十三



2. 信息系统定级与备案工作介绍，http://www.djbh.net/webdev/web/SafeProductAction.do?p=getBzgfZxbz&id=8a8182565deefd0d015e6e9b37630067，2018 年 2 月 1 日最后访问。

表三十五

业务信息安全/系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

最后，安全保护等级由业务信息安全保护等级和系统服务安全保护等级孰高者来评定。在等级确定后可开始起草定级报告。

另外，在定级过程中，如是单位自建的信息系统（与上级单位无关），则由单位自主定级；如是跨省或者全国统一联网运行的信息系统，可以由主管部门统一确定安全保护等级。其中：由各行业统一规划、统一建设、统一确定安全保护策略的全国联网系统，应由行业主管部门统一对下属各级系统分别确定等级；由各行业统一规划、分级建设、全国联网的信息系统，应由部、省、地市分别确定系统等级，但各行业主管部门应对该系统提出定级意见，避免出现同类系统下级定级比上级高的现象。对于该类系统的等级，下级确定后需报上级主管部门审批。

6.1.2 专家评审和主管部门审批

初步确定信息系统安全保护等级后，为了保证定级合理、准确，可以聘请专家进行评审，并出具专家评审意见。

对于单位自建的信息系统（与上级单位无关），在等级确定后，是否报上级主管部门审批，由各行业自行决定。信息系统运营使用单位参考专家定级评审意见，最终确定信息系统等级，形成《定级报告》。如果专家评审意见与运营使用单位意见不一致时，则由运营使用单位自主决定系统等级。

对于信息系统运营使用单位有上级主管部门的，应当经上级主管部门对安全保护等级进行审核批准。主管部门一般是指行业的上级主管部门或监管部门。如果是跨地域联网运营使用的信息系统，则必须由其上级主管部门审批，确保同类系统或分支系统在各地域分别定级的一致性。

6.1.3 公安机关备案

公安机关在收到信息系统运营使用单位备案材料后，会对信息系统定级的准确性进行审核。公安机关的审核是定级工作的最后一道防线，应予高度重视，严格把关。信息系统定级基本准确的，公安机关颁发由公安部统一监制的《信息系统安全等级保护备案证明》。对于定级不准的，公安机关应向备案单位发整改通知，并建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。备案单位仍然坚持原定等级的，公安机关可以受理其备案，但应当书面告知其承担由此引发的责任和后果，经上级公安机关同意后，同时通报备案单位上级主管部门。具体的备案要求可参照《信息安全等级保护备案实施细则》（公信安〔2007〕1360 号）中的规定。

6.2 数据本地化存储与跨境传输

数据已经成为国际贸易中最为重要的资源之一，数字跨境流动也逐步成为国际贸易规则中的重要议题。根据本报告第一章调研数据表十一显示，有接近 20% 的受访企业选择将数据存储在中国大陆以外的区域，还有 22.22% 的受访企业并不清楚自己数据存储的地理位置。

随着《网络安全法》的正式施行，中国数据跨境流动的基本规则逐渐形成：关键信息基础设施运营者在中国境内收集的个人信息与重要数据出境，需要先经过安全评估。但该条款的具体实施还有诸多不明朗之处，如“关键信息基础设施运营者”的范围、“中国境内”的界定、“重要数据”的概念、安全评估的程序都还有待有关部门进行更清楚的界定。

故 2017 年 4 月 11 日，国家互联网信息办公室发布了关于《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称为《评估办法》）公开征求意见的通知。《评估办法》对《网络安全法》的数据出境相关规定予以细化，为有跨境数据转移需求的企业提供了操作指引。

根据《评估办法》，数据出境安全评估相关的细化规定如表三十六所示，可供企业参考。

表三十六

项目	具体事项
数据出境安全评估工作的监管机构	国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估。 行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。
数据出境安全评估的重点评估内容	（一）数据出境的必要性； （二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等； （三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等； （四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等； （五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险； （六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险； （七）其他需要评估的重要事项。
网络运营者应报请行业主管或监管部门组织安全评估的情形	（一）含有或累计含有 50 万人以上的个人信息； （二）数据量超过 1000GB； （三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等； （四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息； （五）关键信息基础设施运营者向境外提供个人信息和重要数据； （六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。
数据不得出境的情形	（一）个人信息出境未经个人信息主体同意，或可能侵害个人利益 （二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益； （三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

此外，2017 年 5 月 27 日，全国信息安全标准化技术委员会发布了《信息安全技术数据出境安全评估指南（草案）》。相较前文所述的《评估办法》，《评估指南》的特点在于进一步将安全评估的流程予以补充与细化，为需要进行数据出境的企业提供更加详细的指导。《评估指南》关于数据出境安全评估的流程如表三十七。

表三十七

步骤	具体事项
自评估启动	网络运营者需要启动自评估的情形为： a）产品或服务涉及向境外机构、组织或个人提供数据的； b）已完成数据出境安全评估的产品或业务所涉及的数据出境，在目的、范围、类型、数量等方面发生较大变化、数据接收方变更或发生重大安全事件的
制定数据出境计划	网络运营者应首先制定数据出境计划，计划的内容包括但不限于： a) 数据出境目的、范围、类型、规模； b) 涉及的信息系统； c) 中转国家和地区（如存在）； d) 数据接收方及其所在的国家或地区的基本情况； e) 安全控制措施等
相关部门评估数据出境计划的合法正当和风险可控	数据出境安全评估首先评估数据出境计划的合法性和正当性；数据出境活动不具有合法性和正当性，不得出境。在此基础上再评估数据出境计划是否风险可控，有效避免数据出境及再转移后被泄露、损毁、篡改、滥用等风险

本报告认为，评估数据出境计划的要点在于“合法正当”与“风险可控”。对于该要点的具体内涵，《评估指南》进行了细化，见表三十八。

表三十八

原则	具体要求
合法正当	数据出境的合法性包括： 1）不属于法律法规明令禁止的； 2）符合我国政府与其他国家、地区签署的关于数据出境条约、协议的； 3）个人信息主体已授权同意的，危及公民生命财产安全的紧急情况除外； 4）不属于国家网信部门、公安部门、安全部门等有关部门依法认定不能出境的
	数据出境的正当性包括： 1）网络运营者在合法的经营范围内从事正常业务活动所必需的； 2）履行合同义务所必需的； 3）履行我国法律义务要求的； 4）司法协助需要的； 5）其他维护网络空间主权和国家安全、社会公共利益、保护公民合法利益需要的
风险可控	评估数据出境计划的风险可控，应综合考虑出境数据的属性和数据出境发生安全事件的可能性。 数据属性的参考因素为： 1）个人信息的属性，包括数量、范围、类型、 2）重要数据的属性，包括数量、范围、类型和技术处理情况等 数据出境发生安全事件的可能性的参考因素为： 1）发送方数据出境的技术和管理能力； 2）数据接收方的安全保护能力、采取的措施； 3）数据接收方所在国家或区域的政治法律环境

综上所述，《评估办法》与《评估指南》均对数据出境安全评估进行了细化规定。因此，需要企业密切注意数据出境领域实施细则与国家标准的制定情况，并保持与行业主管或监管部门进行有效的沟通。参照《个人信息和重要数据出境评估办法（征求意见稿）》及有关国家标准，对企业数据出境情况先行摸底排查，以便在正式细则通过后有效应对。

6.3 关键信息基础设施保护

《网络安全法》明确了关键信息基础设施安全保护中各方实体的义务和责任，推动责权清晰的管理体系建设。根据《全国人大常委会检查组关于一法一决定实施情况的报告》，截至 2017 年底，中国共确定关键网络设施和重要信息系统 11590 个。

在《关键信息基础设施安全保护条例（征求意见稿）》中，提出了五大类行业应被认定为关键信息基础设施运营者。但这并不意味着五大类行业的网络设施和信息系统也落入了关键信息基础设施的范畴之内。判断标准可参照《网络安全法》对关键信息基础设施的界定，即“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益”。

《网络安全法》对关键信息基础设施保护设定了较为明确的义务，见表三十九。

表三十九

分类	义务	责任
等级保护	（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任； （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施； （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月； （四）采取数据分类、重要数据备份和加密等措施； （五）法律、行政法规规定的其他义务	责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款
“三同步”	建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用	责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款
安全保护	（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查； （二）定期对从业人员进行网络安全教育、技术培训和技能考核； （三）对重要系统和数据库进行容灾备份； （四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务	
采购	采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任	

数据出境	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定	责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款
评估	应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门	

2017 年 9 月上旬至 10 月中旬，中国信息安全测评中心随机选取 120 个关键信息基础设施（60 个门户网站和 60 个业务系统），并进行了远程渗透测试和漏洞扫描。该中心出具的报告显示，本次远程测试的 120 个关键信息基础设施中，共存在 30 个安全漏洞，包括高危漏洞 13 个。许多单位没有依照法律规定留存网络日志，这可能导致发生网络安全事件时无法及时进行追溯和处置；有的单位从未对重要信息系统进行风险评估，对可能面临的网络安全态势缺乏认知。许多单位的内网和专网安全建设没有引起足够重视，个别单位对内网系统未部署任何安全防护设施，长期不进行漏洞扫描，存在重大网络安全隐患。

关键信息基础设施的建设和保护关乎国家安全、国计民生、公共利益，因此法律赋予其特定的义务，在网络安全技术上对其也有特殊的要求和标准。因而，企业面临法律和技术上的双重挑战。在义务履行的过程中，企业如果尚有未臻明确的问题，建议向专业法律人士咨询，以获取专业的法律意见。

第十五章 数据危机处理

面对网络安全风险，事前预防固然重要，但网络安全事件并不能够完全的避免，爆发之后的危机处理也同样重要。

数据危机的类型多种多样，不仅包括黑客攻击导致的数据泄露、网络瘫痪，还包括违反《网络安全法》而被有关部门约谈、处罚，甚至包括在企业并购、融资、上市过程中数据尽职调查中所发现数据安全事件（隐患）而影响企业正常运营的情形。本报告第一章调研数据表二显示，有近 1/3 的企业曾遭遇过威胁网络安全的事件，其中曾感染计算机病毒的企业占比 15.74%，曾遭遇网络瘫痪、发生数据泄漏的企业均占 6% 以上。

数据的高度流动性让数据危机的影响不会局限在一地，具有跨地域、跨国界的特点，企业可能需要同时面对多国政府的调查。除此以外，数据危机的爆发具有突发性，爆发前通常是毫无征兆。目前绝大多数企业在数据危机处理及应对机制的建立还处于空白，一旦危机爆发，企业面临政府部门高压的调查与严厉的外部舆论环境往往会不知所措。因此，本报告认为，企业有必要具备时刻待命的跨区域、跨部门的数据危机处理的能力，在数据危机爆发后，将损害结果控制在最低。

危机处理一般可以分为预警、评估和决策、响应、经验总结四个阶段。

1. 预警

1.1 通过新闻报道以及外界舆论感知态势

新闻报道以及外界舆论是法务人员以及外部律师的重要信息渠道。如通过国家或地方行政部门对其他企业所作出的行政处罚以及约谈等行为，企业可以感知其所在行业的现状，以及自身的法律困境。

在 2018 年年初，万豪酒店由于将港澳台地区和西藏表述为“国家”而被上海市网信办紧急约谈。其他企业应当据此自查其平台或 APP 等是否具有该项违法信息。若企业能够及时感知态势并作相应调整，即可在很大程度上避免不必要的行政处罚或约谈。但是在“万豪事件”发生后，仍有部分企业缺乏对信息的感知敏感度以及执行力而被予以行政处罚。比如，Zara 网站等运营主体就因未对上述违法信息作及时整改，而被上海市网信办发出《互联网站整改通知书》责令整改。“百万赢家”APP 也是基于上述同样的原因，将“港台”地区表述为国家，而被北京市网信办约谈。此类事件层出不穷。本报告建议，法务人员以及律师应当保持对相关信息渠道的密切关注以及高敏锐度，对约谈事件以及相关新闻等迅速做出反应，及时针对执法重点进行排除。

1.2 主动了解新近法律法规，进行自查自纠

本报告建议，企业的法务人员、技术人员、管理层以及外部律师都应主动了解新近法律法规，以及时发现企业内部存在的薄弱环节。网络信息安全事件一旦发生，需要多部门联动才可解决，因此需要多部门、多类人员的共同参与。与此同时，该类人员应当密切关注立法动态，结合《网络安全法》有关的配套规定，进行自查自纠。

比如，对于互联网新闻信息服务单位，应密切关注与之相关的法律法规动态，如《互联网新闻信息服务管理规定》、《互联网信息服务管理办法》及《互联网新闻信息服务单位约谈工作规定》等。对于相关法律法规的征求意见稿，亦应主动了解以察趋势。

2. 评估和决策

2.1 评估网络安全事件的类别

评估网络安全事件的类别，有利于企业对不同起因的网络安全事件采取相应措施。网络安全事件的起因，在《信息技术安全技术・信息安全事件管理第 1 部分：事件管理原理》的附录中有相应的例举与划分，包括遭受攻击产生的网络安全事件与因信息收集而产生的网络安全事件，表四十将对这两类事件进行详述。

表四十

因遭受攻击产生的网络安全事件		
攻击类型	**定义**	**案例**
拒绝服务	主要指人为、自然因素导致系统、服务或网络失败，不能按其预期能力持续运行	例如操作员的错误配置或应用软件的不兼容、操作人员违反物理安全规定或是由于环境条件，造成设备的失窃或故意损坏和破坏等
未授权访问	这类事件包括在实际未授权的情况下尝试访问或误用系统、服务或网络	试图提升对资源或信息的访问特权，以致超出一个用户或管理员已经合法所拥有的行为
恶意软件	一个程序或一个程序的部分被插入另外一个程序中，意在修改原来的行为，通常进行恶意活动	诸如盗用信息和身份、破坏信息和资源、拒绝服务，发送垃圾邮件等。恶意软件攻击可分为五类：病毒、蠕虫、特洛伊木马、移动代码和混合攻击
滥用	用户违背组织信息系统安全策略造成的	网络用户下载并安装黑客工具；利用企业电子邮件发送垃圾邮件或推广个人业务；利用公司资源建立未经授权的网站或进行“挖矿”
因信息收集产生的网络安全事件		
通常情况下，信息收集类事件涉及第三方（攻击者）对网络运营者的平台或网站等目标进行识别并进行了解。在某些情况下，技术型的信息收集可能会导致未授权访问，例如，攻击者在搜索目标脆弱性时还会试图获得未授权访问；非技术型的信息收集事件会造成直接或间接的信息泄露或篡改以及电子化存储的知识产权被窃盗等后果		

通过识别网络安全事件的起因与类别，有利于企业迅速反应拟定对策，知悉事件的严重性，为应对措施的采取、事件的对外报告提供合理依据。

2.2 拟定网络安全事件采取的应对措施

在确定网络安全事件起因和类别后，企业应该拟定相应的应对措施，用于后续的响应工作以解决风险、及时止损。对于应对措施的拟定与应对人员的安排，本报告建议，可以从以下方面予以考量：

第一，确定采取应对措施的人员，并通过评估、决策和对行动人员的安排，分配信息安全事件管理活动的责任；

第二，为每一个通知到的人员提供正式规程使其遵从，包括评审和修改报告，评估损害和通知相关人员；

第三，根据事件的性质与严重性对人员采取不同的手段，有需要的话，也可以以事件响应小组的形式确定分工与合作，提高解决安全事件的效率。

3. 响应

在对安全事件进行评估和决策之后，企业应当采取行动进行响应。

3.1 固定证据

网络安全事件发生之后，企业及其主管人员可能会招致企业内部的问责，主管机关的惩罚甚至诉讼，因此保留和固定相关证据至关重要。本报告建议，在这个过程中，尤其要注意电子数据的保存并且确保其存储安全。

根据最高人民法院、最高人民检察院和公安部联合发布的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》，电子数据是案件发生过程中形成的，以

数字化形式存储、处理、传输的，能够证明案件事实的数据。电子数据在固定、提取和保全的过程中都有其特殊性。

从网络数据安全的角度出发，本报告建议，如果电子数据涉及个人信息和重要数据，首先应确保其存储的介质安全并实时监管；其次，如要对外披露，对于上述敏感数据可先行进行脱敏处理。所谓脱敏处理，即“移除不应披露信息的过程”，具体方法可参见国家标准 ISO/IEC 27038《数字脱敏规范》。

3.2 报告与通知

《网络安全法》要求，企业在发现其网络产品、服务存在安全缺陷、漏洞等风险或在(可能)发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络信息安全事件一旦发生，发现者应立即将情况上报给网络安全负责人，使其能够确定事态的性质与严重程度，部署下一步的行动方案。网络安全负责人应当在第一时间汇报给管理层以及技术部门，并启动事件响应小组。事件响应小组是由企业中具备适当技能并且可信的成员所组成的团队，并负责事件的处理，可以包括企业管理层、安全技术人员、法务、公共关系人员、外部律师等。具体事件及处理方式见表四十一。

表四十一

主体	事件	处理
网络产品、服务提供者	网络产品、服务存在安全缺陷、漏洞等风险	立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
网络运营者	在发生或者可能发生个人信息泄露、毁损、丢失的情况时	
电信业务经营者、互联网信息服务提供者	保管的用户个人信息发生或者可能发生泄露、毁损、丢失的	立即采取补救措施
	造成或者可能造成严重后果的	立即向准予其许可或者备案的电信管理机构报告，配合相关部门进行的调查处理
个人信息管理者	发现个人信息遭到泄漏、丢失、篡改后，及时采取应对措施	防止事件影响进一步扩大，并及时告知受影响的个人信息主体
	发生重大事件的	及时向个人信息保护管理部门通报
互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织	发现从事危害计算机信息网络安全的活动	应当保留有关原始记录，并在24小时内向当地公安机关

根据《信息安全技术 个人信息安全规范》(GB/T 35273–2017) 的要求，在发生个人信息安全事件后，企业应按《国家网络安全事件应急预案》的有关规定及时上报，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；并且需要将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息，告知内容应包括但不限于：安全事件的内容和影响、已采取或将要采取的处置措施、个人信息主体自主防范和降低风险的建议、针对个人信息主体提供的补救措施、个人信息保护负责人和个人信息保护工作机构的联系方式。

事件响应小组应当对网络信息安全事件的法律风险进行判断，包括但不限于：是否需要向有关部门进行报告，如果需要，需向哪些有关部门进行报告；是否需要向用户告知，如果需要，如何向用户进行告知；是否需要向公安部门报案，如果需要，则需固定哪些证据等。具体事项见表四十二。

表四十二

序号	安全事件告知事项
1	事件响应小组应针对安全事件制定详细的告知方案，包括但不限于：告知的对象、时机、发布方、内容、方式
2	事件响应小组告知内容应包括但不限于： a）安全事件的内容和影响； b）已采取或将要采取的处置措施； c）个人信息主体自主防范和降低风险的建议； d）针对个人信息主体提供的补救措施； e）个人信息安全部门或专员的联系方式
3	事件响应小组应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体，难以逐一告知个人信息主体时，应采取合理、有效的方式发布公告
4	事件响应小组根据国家有关规定，公开披露安全事件相关情况

3.3 解决事件

在采取行动之前，要视安全事件的发展态势来决定采取行动的时点。有的可能需要即时采取行动解决事件，但如果事态发生了不可控的转变，则可能需要进一步评估和决策，以改变行动方案。在解决事件的过程中，需要全过程跟踪和记录，以便后续分析。

本报告建议，如果安全事件波及的范围较大，则合作和共享信息是一个有益的方法。2017 年 5 月，WannaCry (永恒之蓝)勒索蠕虫病毒爆发，影响遍及全球近百国家，我国许多高校和多家能源企业、政府机构也“中招”，重要数据损坏严重，并被病毒制造者勒索高额赎金以解密恢复文件。在此期间，新闻媒体对事件进行跟踪报道，提醒用户安装相关漏洞补丁。安全公司推出相关的免疫工具。针对关键的信息网络系统，政府和主管机关也及时介入。全社会通力合作，最大程度地恢复瘫痪网络，保护数据安全。因此，企业面临网络信息安全事件，也应视情况采取合作和共享信息的方式，及时止损，与外部单位合力解决问题。

在事件确定解决并恢复之后，应当及时披露相关细节和信息，并开展后续分析。根据此前事件的性质和严重性，尚需对事件和涉及的相关人员进行后续调查，对调查结果形成总结报告。

4. 经验总结

在数据安全事件解决之后，则进入总结阶段：汲取经验教训、形成一个熟悉的应对模式，以便再次发生类似事件时，可以顺利流畅地应对，减少反应时间，最大程度上减少乃至避免损失。

总体而言，此阶段就是对事件和涉及的相关人员进行后续调查，明确事件发生的原因，发展的过程，并对调查结果形成总结报告，依此制作企业的数据安全事件管理计划。之后将有关数据储存在专门的信息安全数据库中，以便随时展开研究。

具体而言，本报告认为，对于后续调查，应关注以下几个方面：

（一）对于事件发生的原因，企业应该找出数据安全保护的薄弱环节，评审和改进自身的数据安全控制措施，不断升级保护策略；

（二）对于事件发展的过程，企业应当明确何时是最及时的应对时间，哪个阶段造成的损失最大，哪个环节是最关键的环节，并对这些研究结果进行记录；

（三）对于在应对事件过程中所采取的措施，企业应当明确哪些措施最有必要，哪些行动最为及时，事先拟定的应对措施存在哪些问题，以便及时升级和改进类似事件的应对方法；

（四）在全部流程结束后，对于经验总结环节本身，企业也应当再次审视，评价此总结过程是否有所遗漏，下次如何可以更好地进行总结和记录。

最后，在明确了这些方面以后，企业应当将总结的结果告知其相关部门和人员，并将内容妥善保存，在企业内部充分学习，并依此改进企业的数据安全保护措施，不断更新企业的数据安全事件管理计划。本报告要强调的是，数据安全事件的管理和应对也应当是不断更新和迭代的，随着时间的推移定期审视和改进应对计划，才能更好地应对瞬息万变的网络安全态势，保护好企业的数据资产。