网络安全及数据合规动态（2020 年 1 月-6 月）：监管规则（下）

作者：傅鹏、赵卿梦、俞沁

本动态下篇涵盖 2020 年 1 月至 6 月细分领域下的个人信息与网络安全保护规则介绍，主要聚焦行业细分领域下的个人信息与网络安全保护规则，包括教育、电商、金融、工业等领域；也介绍了与网络安全审查有关的新规。

有关 App 场景下的个人信息保护规则以及综合性个人信息监管规则的简述，可参见我们动态的上篇：《海问·观察：网络安全及数据合规动态（2020 年 1 月-6 月）：监管规则（上）》。

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

- **监管规则目录**：

发布时间	规则名称	发布单位
教育领域		
2020.02	《2020 年教育信息化和网络安全工作要点》	国家教育部
金融领域		
2020.02	《个人金融信息保护技术规范》	中国人民银行
2020.05	《商业银行互联网贷款管理暂行办法》	中国银行保险监督管理委员会
电商领域		
2020.02	《电子商务信息公示管理办法（征求意见稿）》	商务部
工业数据保护		
2020.03	《工业数据分类分级指南（试行）》	工业和信息化部
人类遗传资源信息保护		
2020.04	《生物安全法（草案二次审议稿）》	全国人民代表大会常务委员会
网络安全保护领域		
2020.04	《网络数据安全标准体系建设指南（征求意见	国家工业和信息化部

发布时间	规则名称	发布单位
	稿）》	
2020.04	《网络安全审查办法》	国家互联网信息办公室、国家发展和改革委员会、工业和信息化部等 12 个部门
2020.04	《信息安全技术 网络安全等级保护定级指南（GB/T 22240-2020）》	国家市场监督管理总局、国家标准化管理委员会

一、 教育领域

(一) 《2020 年教育信息化和网络安全工作要点》

2020 年 2 月 26 日，国家教育部办公厅发布了《2020 年教育信息化和网络安全工作要点》（教科技厅[2020]1 号）（“**《工作要点》**”）。《工作要点》列举了在教育信息化与网络安全领域的 11 个主要工作方面和 32 项重点任务，其中，特别值得关注的是：

(1) 教育移动互联网应用[1]应当进行备案

与 2019 年 11 月，教育部办公厅发布的《教育移动互联网应用程序备案管理办法》（教技厅〔2019〕3 号）相同，《工作要点》中重申了分阶段推进教育移动互联网应用程序（“**教育类 APP**”）备案工作，并 2020 年 1 月 31 日前完成对现有教育类 APP 的备案工作。

根据教育部网站公布的数据，截至 2020 年 1 月 14 日已有 1928 家教育类 APP 完成了备案工作[2]，尚未完成备案工作的教育类 APP 企业应当高度重视并积极办理该项备案工作，严格遵守主管部门的业务合规要求。

(2) 主管部门将开展高等学校管理服务类教育移动互联网应用专项治理行动

2019 年 11 月，教育部网络安全和信息化领导小组办公室印发了《高等院校管理服务类教育移动互联网应用专项治理行动方案》（教技司〔2019〕265 号）（“**《高等院校服务 APP 专项治理》**”），要求提

高高等院校管理服务类教育移动互联网应用（“**高校服务类 APP**”）的网络安全保障，并指出将在 2020 年 1 月 31 日前完成对高校服务类 APP 的重点抽查工作。

《2020 年工作要点》进一步强调，将加强对于教育类 APP 的事中事后监管机制，重点治理强制使用收费、违规采集个人信息、呈现低俗信息等问题，并开展高校服务类 APP 专项治理行动。

二、 金融领域

(一) 《个人金融信息保护技术规范》

2020 年 2 月 13 日，中国人民银行发布了《个人金融信息保护技术规范》(JR/T0171-2020)（“**《金融信息规范》**”），从安全技术和安全管理两个方面规定了个人金融信息的收集、传输、存储、使用、删除、销毁等生命周期的安全防护要求，进一步明确了个人金融信息风险识别和把控重点。其中，特别值得关注的有：

(1) 《金融信息规范》监管对象较为宽泛

《金融信息规范》适用于国家金融管理部门监督管理的持牌金融机构，以及个人金融信息处理的相关机构。相较于中国人民银行此前发布的涉及个人金融信息保护的规范文件，《金融信息规范》将为持牌金融机构提供业务支持而涉及个人金融信息数据处理的相关机构（如大数据分析公司等）纳入监管范围。

(2) 《金融信息规范》中个人金融信息范围的扩大

在《金融信息规范》中，“个人金融信息”指金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息，包括账户信息、鉴别信息、金融交易信息、个人身份信息等七大类信息，范围相对宽泛。相较于中国人民银行在 2011 年 1 月发布的《中国人民银行关于银行业

金融机构做好个人金融信息保护工作的通知》[3]，增加了“鉴别信息”的概念，即用于验证主体是否具有访问或使用权限的信息，包括但不限于银行卡密码、预付卡支付密码；个人金融信息主体登录密码、账户查询密码、交易密码；卡片验证码（CVN 和 CVN2）、动态口令、短信验证码、密码提示问题答案等。

(3) 个人金融信息类别

《金融信息规范》根据个人金融信息遭遇到未经授权的查看或变更后的可能影响，将个人金融信息分成敏感程度由高到低的 C3、C2、C1 三个类别，具体如下：

类别	范围	未经授权查看或变更的可能后果	代表性信息举例
C3	用户鉴别信息	会对个人金融信息主体的信息安全与财产安全造成**严重危害**	• 银行卡磁道数据（或芯片） • 账户登录密码、交易密码、查询密码 • 用于用户鉴别的个人生物识别等
C2	可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息	会对个人金融信息主体的信息安全与财产安全造成**一定危害**	• 用户鉴别辅助信息 • 支付账户、**手机号码**及等效信息 • 账户登录用户名 • 用于金融产品与服务的关键信息（如交易流水）等
C1	机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息	**可能**会对个人金融信息主体的信息安全与财产安全造成**一定影响**	• 账户开立时间、开户机构 • 基于账户信息产生的支付标记信息 • C2 和 C3 类别信息中未包含的其他个人信息

(4) 个人金融信息安全技术和安全管理要求

《金融信息规范》对个人金融信息提出了覆盖数据全生命周期保护的，贯穿收集、传输、存储、使用、删除、销毁等环节的安全技术和安全管理要求。其中，特别值得注意的有：

(i) 在对个人金融信息主体各类信息进行获取和记录的过程中，《金融信息规范》要求金融业机构不得委托或授权无金融业相关资质的机构收集 C3、C2 类别信息。即，企业不得委托或授权无金融业相关资质的机构收集包括手机号在内的个人金融信息，这对金融业机构数据服务外包环节提出较高的整改与合规要求；

(ii) 就个人金融信息在终端设备、信息系统内或信息系统间传递的过程，《金融信息规范》要求金融业机构在个人金融数据传输前及传输时注重信息安全的技术保护，如：

(a) 对通过公共网络传输的 C2、C3 类别信息使用加密通道或进行数据加密；

(b) 传输个人金融信息前，通信双方应通过有效技术手段进行身份鉴别和认证；

(iii) 就个人金融信息处于终端设备、信息系统内的保存的过程，《金融信息规范》要求金融业机构不得留存非本机构的 C3 类别信息，除非获得个人金融信息主体及账户管理机构的授权、C3 类别个人金融信息应进行加密存储。

此外，由于《金融信息规范》要求受理终端、个人终端及客户端应用软件不得留存支付敏感信息及个人生物识别信息的样本数据，金融业机构应当及时展开对其手机 APP、支持人脸识别取款的 ATM 机等收集的支付敏感信息与个人生物识别信息的终端的自查工作，并尽快完成相关留存信息（如有）的清除；

(iv) 就对个人金融信息的展示、共享和转让、公开披露、委托处理、加工处理等操作的过程，《金融信息规范》要求金融业机构：

(a) 在委托第三方机构处理个人金融信息时，不得委托其处理 C3 类别信息以及 C2 类别信息中的用户鉴别辅助信息；

(b) 在必需的信息展示环节，采取适当的模糊化（指通过隐藏或截取局部信息令个人金融信息无法完整显示）、不可逆（指无法通过样本信息倒推真实信息的方法）等脱敏处理，具体而言包括：

•对通过各类业务界面（如计算机屏幕、自助终端、交易凭条等）或后台管理和业务支撑系统展示的个人金融信息，采取信息屏蔽等处理措施；

•用户处于未登录状态时，有关系统不展示与个人金融信息主体相关的 C3 信息；

•用户处于已登录状态时，有关系统不明文展示 C3 类别信息（银行卡有效期除外）等;

(v) 在共享与转让个人金融信息时：

(a) 不应共享、转让 C3 类别信息以及 C2 类别信息中的用户鉴别辅助信息，共享转让其他个人金融信息需要告知并获得信息主体的同意，但经去标识化处理、确保数据接收方无法重新识别信息主体的除外。

(b) 因收购、兼并、重组、破产等情况导致金融业机构主体变更而需进行个人金融信息共享、转让时，金融业机构应将该变更情况以逐一传达或公告的方式通知个人金融信息主体，且承接后的个人

信息控制者应继续履行原定责任和义务，并在变更个人信息使用目的时，重新取得个人信息主体的明示同意。

(c) 如因业务需要，可向境外机构提供在中国境内提供金融产品或服务过程中收集和产生的个人金融信息。但是，与此前《中国人民银行金融消费者权益保护实施办法》中的限定相同，目前前述个人金融信息仅能提供给境内机构的境外关联机构如其总公司、母公司或分公司、子公司及其他未完成其业务所必需的关联机构;

(vi) 就对个人金融信息的不可被检索、访问的处理过程，《金融信息规范》要求金融业机构积极响应个人金融信息主体删除其个人金融信息的请求；

(vii)就对个人金融信息进行清除使其不可恢复的过程，《金融信息规范》要求:

(a) 如金融业机构因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（含外包服务机构与外部合作机构）处理的，在委托关系解除时（或外包服务终止后），受委托者应按照金融业机构的要求销毁其处理的个人金融信息；

(b) 金融业机构应建立外包服务机构与外部合作机构管理制度，该制度应包括通过协议或合同的方式，约束外包服务机构与外部服务机构不应留存 C2、C3 类别信息。

(二) 《商业银行互联网贷款管理暂行办法（征求意见稿）》

中国银行保险监督管理委员会于 2020 年 5 月 9 日发布了《商业银行互联网贷款管理暂行办法（征求意见稿）》（“**《网络贷款办法》**”），对商业银行的互联网贷款业务经营行为作出规范。其中，特别值得关注的是《网络贷款办法》设立专门章节，对商业银行业务开展中的风险数据管理作出了规定：

(1) 明确风险数据的范围

风险数据是指商业银行在对借款人进行身份确认，以及贷款风险识别、分析、评价、监测、预警和处置等环节收集、使用的各类内外部数据。

(2) 要求商业银行确认外部风险数据来源合法合规

商业银行如果需要从外部合作机构获取借款人风险数据，应当至少包含借款人姓名、身份证号、联系电话、银行账户等基本信息，且通过适当方式确认合作机构的数据来源合法合规、真实有效，并已获得数据主体本人的明确授权。

(3) 要求风险数据收集和使用遵循合法、必要、有效的原则

不得违反法律法规和借贷双方约定，不得将风险数据用于从事与贷款业务无关或有损借款人合法利益的活动，不得向第三方提供借款人风险数据。

(4) 要求商业银行采取风险数据安全保管措施

商业银行应当建立风险数据安全管理的策略与标准，采取有效技术措施，保障借款人风险数据在采集、传输、存储、处理和销毁过程中的安全，防范数据泄漏、丢失或被篡改的风险。

三、 电商领域：《电子商务信息公示管理办法（征求意见稿）》

2020 年 2 月 12 日，商务部发布了《电子商务信息公示管理办法（征求意见稿）》（“**《电商信息公示办法》**”），对《电子商务法》中提出的电子商务经营者信息公示义务进一步作出了细化规定[4]。

值得关注的是，除对《电子商务法》规定的公示义务进行细化外，《电商信息公示办法》还专门规定了非法获取公示电子商务信息数据和非法篡改与使

用公示电子商务信息数据行为及相应的法律责任，加强了对公示电子商务信息数据的保护力度，具体如下：

(1) 非法获取信息数据的行为与法律责任

《电商信息公示办法》强调，任何自然人、法人或者其他组织不得通过数据抓取等技术手段不正当地获取公示的电子商务信息。根据该文件，仅有“不正当”的获取行为才应当承担法律责任，但未就“不正当”的具体情形进行说明。

参照《数据安全管理办法（征求意见稿）》规定，“不正当”的运用技术手段可以指，妨碍网站正常运行的自动化收集网站数据的行为[5]。举例而言，自然人、法人或者其他组织采用数据抓取等技术手段收集流量超过网站日均流量三分之一，且在网站要求其停止此类访问收集行为而拒不停止的，可能被认定为该自然人、法人或者其他组织通过数据抓取等技术手段不正当地获取了公示的电子商务信息。

(2) 篡改和非法使用信息数据的行为与法律责任

《电商信息公示办法》明确禁止篡改和非法使用公示的电子商务信息的行为，由于经公示的电子商务信息数据很容易被外界获取，并被他人非法的修改、编辑和利用，从而导致被公示的电子商务信息失去其真实性和完整性。因此，《电商信息公示办法》明确了对公示信息的保护，体现了对打击篡改和非法使用公示电子商务信息数据的侵权行为的决心。

四、 工业数据保护：《工业数据分类分级指南（试行）》

2020 年 3 月 4 日，工业和信息化部办公厅发布了《工业数据分类分级指南（试行）》（“**《分级指南》**”）以促进工业数据的使用、流动与共享。该指南所指工业数据是工业领域产品和服务全生命周期产生和应用的数据，包括但不限于工业企业在研发设计、生产制造、经营管理、运维服务等环节中

生成和使用的数据，以及工业互联网平台企业在设备接入、平台运行、工业APP 应用等过程中生成和使用的数据。

根据《分级指南》，企业在业务开展过程中产生的工业数据可以根据其遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益等带来的潜在影响，分为三个级别，具体分类情况以及管理要求如下：

(1) 工业数据遭篡改、破坏、泄露或非法利用后，将造成以下影响的，应当被界定为三级数据：

(i) 将引发特大安全事故、特大环境事件、特大经济损失的；或

(ii) 将对国家的安全和经济情况、社会和公众利益、行业发展产生严重影响的。

管理上，企业针对三级数据采取的防护措施，应能抵御来自国家级敌对组织的大规模恶意攻击。且三级数据原则上不共享，确需共享的应严格控制知悉范围。

(2) 工业数据遭篡改、破坏、泄露或非法利用后，将造成以下影响的，应当被界定为二级数据：

(i) 将引发较大安全事故、较大环境事件、较大经济损失的；或

(ii) 引发的级联效应明显，如涉及多个行业、区域或者行业内多个企业，或影响持续时间长或被非法利用的数据量较大。

管理上，企业针对二级数据采取的防护措施，应能抵御大规模、较强恶意攻击。二级数据只对确需获取该级数据的授权机构及相关人员开放，在做好数据管理的前提下，企业可以适当共享二级数据。

(3) 工业数据遭篡改、破坏、泄露或非法利用后，将造成以下影响的，应当被界定为一级数据：

(i) 对工业控制系统、设备、平台等的影响较小；或

(ii) 给企业造成负面影响、直接经济损失较小，数据恢复或消除负面影响所需付出的代价较小；或

(iii) 受影响的用户和企业数量较少、区域范围较小、持续时间较短。

管理上，企业针对一级数据采取的防护措施，应能抵御一般恶意攻击，且在做好数据管理的前提下企业可以适当共享一级数据。

五、 人类遗传资源信息保护：《生物安全法（草案二次审议稿）》

《生物安全法（草案二次审议稿）》（“**《生物安全法》**”）于 2020 年 4 月 30 日在中国人大网公布并向公众公开征求意见至 2020 年 6 月 13 日。该文件对疫情防控、生物技术研发与应用、人类遗传资源与生物资源安全管理以及防范生物入境和生物武器威胁等生物安全领域进行了规定。其中，《生物安全法》延续了《人类遗传资源管理条例》（“**《遗传资源条例》**”）中的相关规定，核心内容如下：

(1) 与《遗传资源条例》相同，《生物安全法》规定采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，不得危害公众健康、国家安全和社会公共利益。

(2) 采集我国重要遗传家系、特定地区人类遗传资源或者采集国务院科学技术主管部门规定的种类、数量的人类遗传资源；保藏我国人类遗传资源；利用我国人类遗传资源开展国际科学研究合作；将我国人类遗传资源材料运送、邮寄、携带出境的行为需要经国务院科学技术主管部门批准。

但是，上述规定也有两个例外情况：第一，以临床诊疗、教学、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等为目的采集、保藏人类遗传资源及开展的相关活动不需要取得批准；第二，为了取得相关药品和医疗器械在我国上市许可，在临床试验机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源出境的，不需要批准；但是，在开展临床试验前应对将拟使用的人类遗传资源种类、数量及其用途向国务院科学技术主管部门备案。

(3) 境外组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源；境外组织、个人及其设立或者实际控制的机构获取和利用我国生物资源，应当依法取得有关部门的批准。

(4) 将我国人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院科学技术主管部门事先报告并提交信息备份；可能影响公众健康、国家安全和社会公共利益的，还应当通过国务院科学技术主管部门的安全审查。

(5) 利用我国人类遗传资源和生物资源开展国际科学研究合作，应当保证中方单位及其研究人员全过程、实质性地参与研究，依法分享相关权益。利用我国生物资源开展国际科学研究合作，应当依法取得有关部门的批准。

简评：

人类遗传资源的跨境传输（其中往往也可能涉及个人信息的跨境传输）引发了广泛的关注，也产生了直接相关的行政处罚案例。该领域的企业有必要对业务过程中涉及人类遗传资源跨境传输的部分进行梳理，提前准备以更好地满足相关的批准或备案程序。

六、 网络安全保护领域

(一) 《网络数据安全标准体系建设指南（征求意见稿）》

工业和信息化部于 2020 年 4 月 10 日发布了《网络数据安全标准体系建设指南（征求意见稿）》（“**《数据建设指南》**”），该指南为电信和互联网行业网络数据安全搭建了整体框架，提出了网络数据安全的重点领域。特别值得关注的是：

(1) 重点领域的范围：包括 5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等领域。

(2) 车联网领域：车联网安全覆盖车内、车与车、车与路、车与人、车与服务平台的全方位连接和数据交互过程，数据安全和隐私保护贯穿于车联网的各个环节。车联网领域的网络数据安全标准主要包括车联网云平台数据安全、V2X 通信数据安全、智能网联汽车数据安全、车联网移动 App 数据安全等。

我们之前就车联网业务的主要构成，及外资进入中国车联网市场的主要交易结构进行分析，可参见我们的文章：

“海问车联网法律评论（一）：旧江湖的新隐喻--TSP 服务市场的格局与监管”

“海问车联网法律评论（二）：域外玩家的本土布局--外资进入 TSP 服务领域路径浅析”

(3) 物联网领域：物联网安全涵盖物联网的感知层、传输层、应用层，涉及服务端安全、终端安全和通信网络安全等方面，数据安全贯穿于其中的各个环节。物联网领域的网络数据安全标准主要包括物联网云端数据安全保护、物联网管理系统数据安全保护、物联网终端数据安全保护等。

(4) 大数据领域：大数据安全覆盖数据全生命周期管理各环节，涵盖对大数据平台运行安全功能保障及以数据为对象进行资产管理等。大数据领域的网络数据安全标准主要包括大数据平台安全、大数据资产管理等。

(5) 人工智能领域：人工智能安全覆盖个人信息安全、算法安全、数据安全、网络安全等。人工智能领域的网络数据安全标准主要包括人工智能平台数据安全、人工智能终端个人信息保护等。

简评：

对强调的上述领域，可预期形成未来一段时间的立法及行业标准制定重点。事实上，由于上述领域的商业应用丰富、活跃，对数据进行利用的场景多样、复杂，所以这些领域在过去一段时间已经颁布了一些规定及国家标准。

但该等规定和国家标准偏重于在政策方向性方面进行指导和把控。由于这些领域的数据应用及数据安全越来越重要，所以也可期在未来一段时间有一系列更为细化、具有指导性的规定颁布。

(二) 《网络安全审查办法》

国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部等 12 个部门于 2020 年 4 月 27 日联合发布了《网络安全审查办法》（“**2020 年审查办法**”），该办法于 2020 年 6 月 1 日起正式施行。对关键信息基础设施运营者（“**CII 运营者**”）采购网络产品和服务的网络安全审查范围、审查程序和审查要素等作出了规定。其中，特别值得关注的是：

(1) 审查对象：CII 运营者采购网络产品和服务，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或可能影响国家安全的，应当进行网络安全审查。

一方面，根据《网络安全法》规定，CII 运营者是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施的运营者；国家互联网信息办公室就 2020 年审查办法相关问题答记者问时指出，电信、广播电视、

能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当考虑申报网络安全审查。

另一方面，并非 CII 运营者采购的所有网络产品和服务都需要进行网络安全审查。根据 2020 年审查办法，属于审查范围的网络产品和服务主要指核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务；同时，也规定了“其他对关键信息基础设施安全有重要影响的网络产品和服务”作为兜底。

(2) 审查的启动和流程：2020 年审查办法规定两种启动方式，第一种是由 CII 运营者预判后主动向网络安全审查办公室（“**审查办公室**”）申报；另一种是网络安全审查工作机制成员单位（“**成员单位**”）认为影响或可能影响国家安全的网络产品和服务，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，进行审查。

主体	流程	期限（工作日）
成员单位	如为成员单位启动，则需报中央网络安全和信息化委员会批准	N/A
CII 运营者	提交申报材料	N/A
审查办公室	接收申报材料，确定是否需要安全审查	10
审查办公室	如认定需要审查，则应书面通知 CII 运营者，形成初步审查意见，并征求各相关部门意见	30+15
成员单位及相关关键信息基础设施保护工作部门（“**相关单位**”）	接收初步审查意见，作出书面回复意见	15
审查办公室与相关单位	意见一致的情况下，由审查办公室将审查结论通知 CII 运营者； 意见不一致情况下按照特别审查程序处理	N/A

(3) CII 运营者与网络产品和服务的供应商之间的采购合同的关注点：根据 2020 年审查办法规定，CII 运营者应当通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便

利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。

(三) 《信息安全技术 网络安全等级保护定级指南（GB/T 22240-2020）》

国家市场监督管理总局和国家标准化管理委员会于 2020 年 4 月 28 日联合发布了《信息安全技术 网络安全等级保护定级指南（GB/T 22240-2020）》（“**2020 年定级指南**”），该指南将于 2020 年 11 月 1 日正式施行，规定了网络运营者开展非涉及国家秘密的安全保护的等级保护对象、定级方法和定级流程。相较于公安部于 2017 年 5 月 8 日发布的《信息安全技术 网络安全等级保护定级指南（GA/T 1389-2017）》（“**2017 年定级指南**”）在定级对象、定级要求和定级认定方面作出了修订。其中，特别值得关注的是：

(1) 定级对象的范围：即哪些主体需要进行定级并承担安全责任。相较于 2017 年定级指南，2020 年定级指南增加了云计算系统、数据资源，删去了宽泛的其他信息系统的表述，将基础信息网络修改为通信网络设施，对象从信息网络变更为网络设施。

变更后的定级对象包括：

(i) 信息系统：云计算平台/系统、物联网、工业控制系统、采用移动互联技术的系统；
(ii) 通信网络设施；
(iii) 数据资源。

(2) 定级对象的分别定级要求：

(i) 云计算平台/系统：2020 年定级指南要求不同服务模式项下的云计算平台/系统要划分为不同的对象进行定级。例如云服务提供者在对外提供 SaaS、PaaS 和 IaaS 时，应就各个服务模式分别进行定级；

(ii) 工业控制系统：工业控制系统主要包括现场采集 / 执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集 / 执行、现场控制和过程控制等要素需作为一个整体对象定级，各要素不单独定级；生产管理要素宜单独定级；

(iii) 数据资源：数据资源可独立定级；当安全责任主体不同时，大数据应独立定级；当安全责任主体相同时，大数据、大数据平台 / 系统宜作为一个整体对象定级。

(3) 确定等级时受侵害的客体的认定：受侵害的客体即受法律保护的、等级保护对象受到破坏时所侵害的社会关系，包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。相较于 2017 年定级指南，2020 年定级指南主要修订如下：

(i) 国家安全方面增加了国家海洋权益和国家社会主义经纪秩序和文化实力；
(ii) 社会秩序方面增加了企事业单位、社会团体生产秩序、医疗卫生秩序、公共交通秩序和人民群众生活的情况。

简评：

2020 年定级指南新增/强调了云计算、工业控制系统、物联网等系统的等保要求，是对 2017 年定级指南及之前一系列等保规定的拓展和细化。

随着《中华人民共和国网络安全法》明确对等保制度进行加强管理，近年来主管机关对等保定级/测评的实践要求和执法先例有所落实和趋紧。企业有必要根据 2020 年定级指南，对自身控制的信息系统进行梳理评定，特别对云计算、工业控制系统、物联网等系统予以关注，考虑是否需要分别定级。

后记：

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

《海问观察：网络安全及数据合规动态》（2019 年 9 月上半月）
《海问观察：网络安全及数据合规动态》（2019 年 9 月下半月-10 月上半月）
《海问观察：网络安全及数据合规动态》（2019 年 10 月下半月-11 月）
《海问观察：网络安全及数据合规动态》（2019 年 12 月）
《海问观察：网络安全及数据合规动态》（2020 年 1 月-6 月）：监管规则（上）

---

[1] 根据《教育移动互联网应用程序备案管理办法》第二条，教育移动应用是以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的互联网移动应用程序。

[2] 参见教育部网站关于已备案教育移动应用的公告信息（截至 2020 年 1 月 14 日发布三期）：http://www.moe.gov.cn/jyb_xxgk/s5743/s5744/202001/t20200120_416151.html；http://www.moe.gov.cn/jyb_xxgk/s5743/s5744/202001/t20200102_414289.html；http://www.moe.gov.cn/jyb_xwfb/s5147/201912/t20191220_412908.html。

[3] 根据《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第一条，一、本通知所称个人金融信息，是指银行业金融机构在开展业务时，或通过接入中国人民银行征信系统、支付系统以及其他系统获取、加工和保存的以下个人信息：（一）个人身份信息；（二）个人财产信息；（三）个人账户信息；（四）个人信用信息；（五）个人金融交易信息；（六）衍生信息；（七）其他个人信息。

[4] 根据《电子商务法》第十五条，电子商务经营者应当在其首页显著位置，持续公示营业执照信息、与其经营业务有关的行政许可信息、属于依照本法第十条规定的不需要办理市场主体登记情形等信息，或者上述信息的链接标识。

前款规定的信息发生变更的，电子商务经营者应当及时更新公示信息。

[5] 根据《数据安全管理办法（征求意见稿）》第十六条，网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。