君合专题研究报告

2020 年 5 月 8 日

跨境数据传输系列——跨国公司如何趟过“国家秘密”雷区

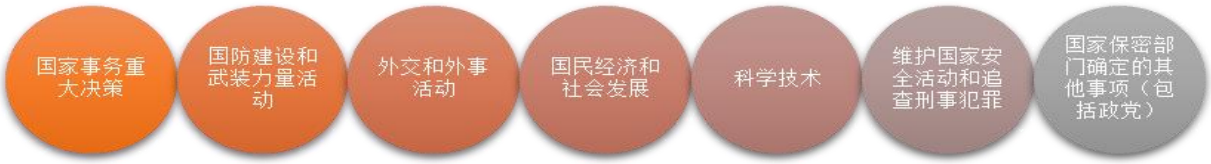
在中国进一步扩大对外开放的背景下，外国企业可以投资准入的行业领域不断延伸，跨国公司参与新能源汽车、无人驾驶、金融、医药行业的投融资案例显著增加。跨国公司在与政府部门、国有企业、特殊行业洽谈合作、业务开发、投融资贸易等过程中，均有可能接触含有国家秘密的信息，国家秘密合规问题不容忽视。近期，先后发生跨国公司外籍员工以及境外大学教授因涉嫌搜集涉及国家秘密的资料，被拘留、判处刑罚的案件，再次使业界认识到在商务活动中“国家秘密”的雷区看似远在天边，实则就在眼前。

本文拟通过对国家秘密的界定及识别、常见特殊行业的国家秘密范围整理、国家秘密的规制要求及法律责任的梳理，为跨国公司在华商务活动中的国家秘密合规提供参考，以期作为趟过雷区的探雷针。

一、国家秘密的界定、载体及识别

1、 国家秘密的界定

根据《保守国家秘密法》，“国家秘密”是指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。该规定对国家秘密作了较为宽泛的原则性界定，具体内涵及范围并不明确。因此，《保守国家秘密法》从损害程度及七个重点保护领域方面，对国家秘密的范围作了列举式定义。对于涉及国家安全和利益的下列领域及活动中的秘密事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密：



根据我们以往的实务经验，企业交易涉及国家秘密较多的领域主要集中在上述“国民经济和社会发展”。但是，上述范围举例仅细分到“国民经济”这一层面，对于经营不同行业的企业而言，很难据此判断其所在行业领域是否触及国家秘密，需要结合相应规章等规范性文件规定的国家秘密及具体范围（具体请看后述“二”）进一步核实。

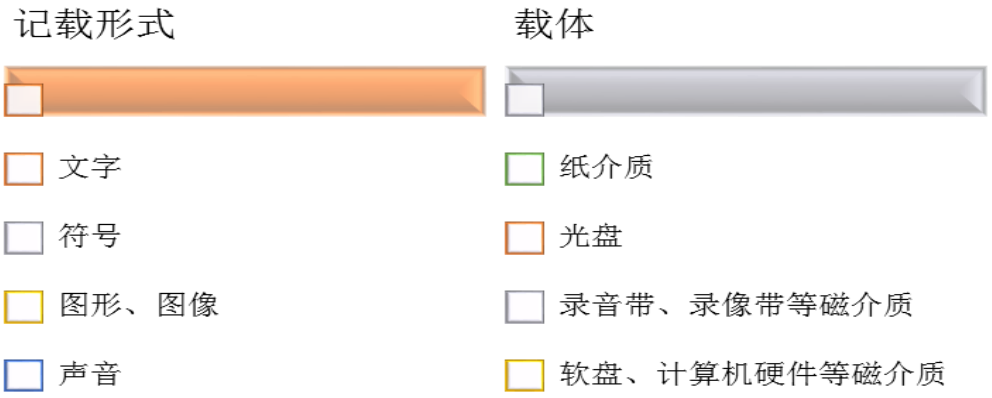
2、 国家秘密的分类及保密期限

基于秘密泄露后的损害程度，《保守国家秘密法》将国家秘密等级分为下述绝密、机密、秘密三级。相应地，《保守国家秘密法》根据密级程度的不同对保守国家秘密的保密期限做了区分。

国家秘密分类	界定	保密期限
绝密级	最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害。	一般不超过三十年
机密级	重要的国家秘密，泄露会使国家安全和利益遭受严重的损害。	一般不超过二十年
秘密级	一般的国家秘密，泄露会使国家安全和利益遭受损害。	一般不超过十年

3、 国家秘密的记载形式与载体

根据《关于禁止邮寄或非法携运国家秘密文件、资料和其他物品出境的规定》、《中共中央保密委员会办公室、国家保密局关于国家秘密载体保密管理的规定》等规定，对国家秘密的记载形式及载体列举如下：



4、 企业应如何识别国家秘密

根据《保守国家秘密法》及《国家秘密定密管理暂行规定》，国家秘密标志形式为“密级★保密期限”、“密级★解密时间”或者“密级★解密条件”。涉及的机关、单位应根据承载国家秘密的以下载体类型，相应做出国家秘密标志。

- 对于纸介质和电子文件，国家秘密标志一般标注在封面左上角或者标题下方的显著位置（有国家标准的应当符合国家标准）；
- 对于光介质、电磁介质等国家秘密载体和属于国家秘密的设备、产品，应当标注在壳体及封面、外包装的显著位置。

建议企业在日常商务活动中，特别是与政府部门接洽、与特殊行业合作的过程中，及时留意并识别相关文件、载体是否含有上述国家秘密标志。例如，在项目中审阅到源自政府部门的纸质“红头文件”、某些光盘、产品、设备等介质的业务资料时，应着重留意载体的壳体、封面、外包装是否含有国家秘密相关标识。

在我们以往接触的案件中，也出现过部分国家秘密并未做出或者不宜做出标志，而只能通过书面形式通知知悉范围内的机关、单位或人员的情况。因此，外部企业无法通过外在形式识别其是否构成国家秘密。建议跨国公司参照下述特殊行业国家秘密的范围进行识别，并根据需要及时咨询外部专家律师协助识别。

二、特殊行业的国家秘密范围及投资贸易中的注意点

为便于从事特殊行业的企业在其经营管理活动中辨识并保护国家秘密，相关国家部门制定了一系列规章文件，对相应行业的国家秘密范围及

密级做出了更细化的列举式界定。以下以实务中比较常见的测绘、电力、医药、建筑行业及涉及国有资产的投融资为例，简要梳理各行业国家秘密的范围；并结合我们为客户处理以往交易案件时的经验，提示相关规定可能影响到的跨国公司投融资、贸易等交易项目。对于涉及其他特殊行业（例如金融、海洋、国土、军工等）的企业，需要研究相应领域的规章文件。

行业	该行业涉及国家秘密的部分特别规定	可能影响的交易项目/环节案例
测绘	（一）绝密级范围 1、公开或泄露会严重损害国家安全、领土主权、民族尊严的； 2、公开或泄露会导致严重外交纠纷的； 3、公开或泄露会严重威胁国防战略安全或削弱国家整体军事防御能力的。 （二）机密级范围 1、公开或泄露会对国家重要军事设施的安全造成严重威胁的； 2、公开或泄露会对国家安全警卫目标、设施的安全造成严重威胁的。 （三）秘密级范围 1、公开或泄露会使保护国家秘密的措施可靠性降低或者失效的； 2、公开或泄露会削弱国家局部军事防御能力和重要武器装备克敌效能的； 3、公开或泄露会对国家军事设施、重要工程安全造成威胁的。	自动驾驶项目收购、投融资
电力	（一）机密级事项 1、全国电力行业的年度、中长期计划和规划； 2、涉及国防、军工生产的发、供、用电规划、计划及统计数字； 3、全国电力设备的年度计划、中长期进口规划及转口电力设备和技术引进的内定方案、意向和对策； 4、国家电力工程对外招标的标底、评标情况，对外投标报价和标价计算依据，定标签约前的工程概算； 5、对外经济、科技合作的国别政策。 （二）秘密级事项 1、战备电力工程的人防系统和工程设防标准； 2、电力工业重大污染事故中的监测数据及危害程度； 3、承包国外电力工程的劳务项目投标保函； 4、电力工业科技发展的重点任务、关键科技内容。	光伏、电站、电厂等项目收购、投融资（包括为火力、水力、风力等电站、电厂提供节能增效解决方案而需要采集相关数据的项目）
建筑	（一）机密级事项 1、处于世界先进水平，且对国民经济具有重要影响的建材工业研究开发项目、计划； 2、为国家重点武器型号配套的建材军工新材料的有关规划、计划、研究试制项目的	房地产投资、并购项目（特别需留意建材与设备方面的计划、招投标信息

	内容； 3、建材工业重大项目技术引进和设备进口计划，涉外谈判中内定的方案、标底和对策。 （二）秘密级事项 1、未经公布的全国建材工业发展战略和中、长期规划、计划、固定资产年度投资计划； 2、处于世界先进水平的建材工业技术的研究方法及内容； 3、建材工业出口和利用外资的发展战略及有关政策； 4、建材军工新材料研究、试制及产品定货计划； 5、未经公布的国家统管的建材产品的价格政策和调价方案。	等）
医药卫生	（一）机密级事项 1、泄露会对国家医学科学研究和国家公共卫生安全造成严重损害的； 2、泄露会对国家声誉和公民权益造成严重损害，对省级以上行政区域社会安定造成严重影响的； 3、泄露会对国际卫生交往工作造成严重损害的； 4、泄露会对国家卫生信息安全造成严重损害的。 ➢ 机密级事项（举例） - 卫生部指定的病原微生物菌（毒）种保藏机构保藏的一类高致病性病原微生物菌（毒）种及样本总体数据和保存情况（包括数量、地点和方式等）。 - 通过特殊渠道获得的医学重要成果的技术内容及其来源。 （二）秘密级事项 1、泄露会对国家医学科学研究和国家公共卫生安全造成损害的； 2、泄露会对国家声誉和公民权益造成损害，对部分地区社会安定造成影响的； 3、泄露会对国际卫生交往工作造成损害的； 4、泄露会对国家卫生信息安全造成损害的。 ➢ 秘密级事项（举例） - 卫生部指定的病原微生物菌（毒）种保藏机构保藏的二类高致病性病原微生物菌（毒）种及样本总体数据和保存情况（包括数量、地点和方式等）。 - 地市级卫生行政部门统计的引产数。	医药行业并购、投融资项目（涉及中医药行业时应特别注意）

国有资产	（一）绝密级事项 1、报送党中央、国务院的有关国有资产管理工作重大问题的请示、报告和重要文件、资料； 2、国有资产管理工作中，涉及特殊部门的境外国有资产管理情况及其相关的文件和资料。 （二）机密级事项 1、重大国有资产流失案件的查处材料； 2、尚未对外公布的国有资产全国汇总数据资料； 3、尚未对外公布的境外企业、机构的基本情况及统计资料。 （三）秘密级事项 1、尚未出台的企业国有资产管理体制改革政策及办法； 2、国有资产流失的检举查处材料； 3、国有资产产权纠纷案件处理过程中，产权纠纷调处委员会的讨论意见、调查取证材料； 4、国有企业股份制改造中涉及企业的效益预测、股票发行价格的有关资料及股份公司国有股权转让审核期间的有关文件、资料； 5、各部门、各省、自治区、直辖市尚未对外公布的国有资产统计汇总资料； 6、尚未对外公布的国家投资企业效绩考核资料和文件。	对国有企业投融资、参与国有企业混改等涉及国有资产的各类项目

跨国公司如果从事上述特殊行业，或者在投资贸易过程中与该等行业、国有企业、政府部门存在有较多交集的，均有可能接触到属于国家秘密范围的信息，需要格外注意识别并谨慎应对。

此外，根据相关法规规章的规定，某些领域的信息虽然不属于国家秘密的范围，但是企业应作为内部事项管理，不得擅自扩散。跨国公司应注意避免接触和扩散此类信息。以电力工业为例，电力企业不得扩散的内部事项包括但不限于以下内容。

- 全国电力工业科技发展的主要技术和装备政策、各专业（水电、火电、核电、电网）科技发展的战略和目标；
- 全国电力建设布局的规划、计划和统计资料；
- 全国电力工业技术改造规划；
- 全国电力系统计算机应用规划、管理信息系统总体方案；
- 电力建设项目的区域环境规划及专题资料；
- 尚未出台的全国电、热力价格调整方案。

三、国家秘密处理行为的规制要求

1、 关于国家秘密及其载体的禁止行为

根据《保守国家秘密法》，对于国家秘密禁止以下行为：

- 非法复制、记录、存储国家秘密；
- 在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密；
- 在私人交往和通信中涉及国家秘密。

同时，对于纸质资料、光盘、录像带软件等纸质、光盘、磁介质的国家秘密载体，禁止以下行为：

- 非法获取、持有国家秘密载体；
- 买卖、转送或者私自销毁国家秘密载体；
- 通过普通邮政、快递等无保密措施的渠道传递国家秘密载体；
- 邮寄、托运国家秘密载体出境；
- 未经有关主管部门批准，携带、传递国家秘密载体出境。

2、 使用互联网、计算机信息系统时的注意点

在大数据时代，互联网、计算机系统是企业不可或缺的信息传输、处理手段。《计算机信息系统保密管理暂行规定》、《计算机信息系统国际联网保密管理规定》从计算机系统、网络安全角度，对涉及国家秘密信息的采集、存储、处理、传递、使用和销毁方面作出各种规制。跨国公司在通过互联网、计算机系统处理特殊行业的敏感信息时，除了应谨慎识别国家秘密标志之外，还应注意以下信息处理事宜。

- 对于通过计算机信息系统打印输出的涉密文件，应当按相应密级的文件进行管理；
- 涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行物理隔离等；
- 不得擅自卸载、修改涉密信息系统的安全技术程序、管理程序；
- 退出使用的涉密计算机、涉密存储设备应进行安全技术处理，不得未经处理实施赠送、出售、丢弃或者改作其他用途的行为。

3、 国家秘密的出境禁止及例外

(1) 国家秘密载体的出境许可制度

如上所述，国家秘密及其载体原则上禁止跨境传输或出境。在确有必要出境的情况下，依法办理出境许可手续后方可出境。

根据《关于禁止邮寄或非法携运国家秘密文件、资料和其他物品出境的规定》的相关规定，属于国家秘密的文件、资料和其他物品出境，须由外交信使（含临时信使）或国家保密局核准的单位和人员携运；目的地不通外交信使或外交信使难以携运的，需自行携运机密级、秘密级国家秘密文件、资料和其他物品出境的，应当向有关保密工作部门或保密工作机构申办《国家秘密载体出境许可证》；相关人员在出境时应当主动向海关申报，海关凭《国家秘密载体出境许可证》验放。

(2) 技术秘密出口的分类及许可要求

企业在对外技术合作过程中，有可能涉及到将有关科学技术的国家秘密出口到境外，此时应注意国家科技部有关技术秘密出口的规制要求。根据《国家秘密技术出口审查规定》，绝密级国家秘密技术禁止出口；机密级国家秘密技术，由申请单位按行政隶属关系经省、自治区、直辖市、计划单列市或国务院各部委、直属机构的科技保密管理机构审查同意后，报科学技术部审批；秘密级国家秘密技术，由申请单位按行政隶属关系上报省、自治区、直辖市、计划单列市或国务院各部委、直属机构的科技保密管理机构审批，报科学技术部备案。

需要注意的是，企业在办理国家秘密技术出口时，必须依照上述规定先行办理保密审查手续，获批准后，按有关规定履行技术出口许可手续，方可与外方进行实质性洽谈。此外，在交易文件设计上，技术出口经营者应当在技术出口合同中规定保密条款，要求技术的受让方承担保密义务，必要时，应对受让方使用技术的范围和方式加以限定。

四、侵害国家秘密的法律责任

根据《保守国家秘密法》、《保守国家秘密法实施条例》、《泄密案件查处办法》以及《刑法》等的相关规定，侵害国家秘密面临以下行政责任、刑事责任：

行政责任	➢ 常见行为场景 • 在泄密案件查处工作中，企业事业单位及其工作人员拒不配合，弄虚作假，隐匿、销毁证据，以其他方式逃避、妨碍案件查处的； • 涉密信息系统未按照规定进行检测评估和审查而投入使用的。
	➢ 常见处罚内容 • 由主管部门对企事业单位予以处罚，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； • 责令改正、停止涉密业务； • 限制出境等。
刑事责任	➢ 常见行为场景 • 擅自拍摄属于国家秘密的政府机关红头文件（例如，国家部委尚未公布的金融行业调整政策等）并通过微信群转发； • 应境外网友要求，搜集境内部队军用机场飞机、跑道、军船、港口等军事设施文件资料、拍摄照片，通过 QQ、互联网等传送至境外； • 向境外朋友传输参与的国家重点实验室项目资料、国防科工信息。 • 向境外传输、泄露专案犯罪嫌疑人的关押地点、嫌疑人照片。
	➢ 可能涉及的刑事犯罪 • 为境外窃取、刺探、收买、非法提供国家秘密、情报罪 • 非法获取国家秘密罪 • 非法持有国家绝密、机密文件、资料、物品罪 • 故意/过失泄露国家秘密罪 • 故意/过失泄露军事秘密罪 • 间谍罪

我们在以往的案件也注意到，即使企业本身没有泄露国家秘密，但如果在泄密案件查处工作中拒不配合、妨碍案件查处的，仍有可能被追究法律责任。万一发生涉及国家秘密的案件时，建议企业聘请外部专家对调查程序、对应方式等方面提供意见与协助，以免产生不必要的额外风险。

五、跨国公司在华业务活动中的保密合规要点

综上所述，尽管在测绘、电力、医药、建筑、金融等特殊行业存在国家秘密的范围规定，但整体而言，相关界定仍不明确，且国家安全部门对于国家秘密的判定拥有较大的自主裁量权。我们在相关实务中也注意到，企业往往很难自行判断接触的信息是否构成国家秘密，在经营过程中仍面临国家秘密的合规风险。

1、 跨境数据传输场景及审核注意点

跨国公司在华商务活动过程中，面临较多向境外传输数据的场景，根据我们为客户提供相关服务的经验，在实务中比较常见的有以下场景。

- 因 FCPA 调查案件向美国司法部或证券交易委员会及境外律所传输调查信息；
- 因在华外商投资企业的商业贿赂调查案件向境外母公司传输和汇报调查信息；
- 因在华外商投资企业的反舞弊调查向境外母公司传输和汇报调查信息；

- 因境外诉讼和仲裁向境外机构或者律师事务所传输证据材料；
- 就敏感领域的业务合作，需要国内公司提供相关信息给境外公司进行分析研究提供解决方案的。

在以上场景中，对于有可能涉及国家秘密的文件，我们通常建议跨国公司保持保守、谨慎的态度，在跨境数据传输前首先在外部专家的协助下对材料进行筛查、识别，如果经筛查发现相关资料可能含有国家秘密，一般应通过特殊加工（Redaction）等措施进行排除，防止这些信息被传输至境外带来不必要的风险。根据我们以往的相关经验，在筛查过程中，除应注意前文第一、二部分所列举的特殊行业国家秘密之外，对下列文件也应谨慎操作。

- 国家机关或者行业协会下发的任何文件（可能已经明确标明国家秘密的密级，也可能没有标明密级）；
- 各种政府、行业协会内参等明确标识只限于特定领域人员可以阅读的资料；
- 各种涉及已经进入刑事诉讼程序的信息；
- 各种涉及政治、经济、国家政策层面敏感的且未被公开的信息。

2、 公司内部管理及员工培训

鉴于涉及国家秘密案件的法律责任重且社会影响巨大，可能会对跨国公司的声誉及在华业务开展造成极为不利的影响，跨国公司在其日常经营管理过程中，应通过内部法务合规部门或者外聘专家加强对员工的国家秘密合规培训。万一发生涉及国家秘密事件时，应及时与专业律师咨询，尽量降低和管控相关法律风险。基于我们以往的相关实务经验，跨国公司应就以下事项对员工进行合规培训：

- 培训有关国家秘密的标志、标识、以及本行业可能涉及国家秘密的信息范围，要求员工在业务过程中提高警惕；
- 员工在特殊敏感行业的业务洽谈、投资合作以及拜访政府部门等业务过程中，如果接触到政府部门的红头文件等可能涉及国家秘密文件的信息，建议不要轻易触碰（包括翻阅、摘抄、复制、拍照）等行为，应第一时间向公司法务合规部门报告。
- 及时制定或修订公司关于文档管理等内部规章制度，禁止员工在微信群、未加密系统传输、发送敏感信息。
- 加强员工培训教育，特别是对于公司的外籍员工或者母公司派驻员工，告知其在出差、考察研究、私人旅游过程中，应避免随意拍摄涉及军用、国防设施、重要国家机关等驻地及其规划图，同时避免将相关信息擅自传输到境外。
- 因从事公司业务或者个人行为导致被相关部门以涉及国家秘密为由查处的，应立即向公司法务合规部门报告。

杨锦文　合伙人　电话：86 10 8553 7608　邮箱地址：yangjw@junhe.com
高　健　律　师　电话：86 10 8519 1359　邮箱地址：gaojian@junhe.com
陈嘉怡　律　师　电话：86 21 2208 6011　邮箱地址：chenjiayi@junhe.com