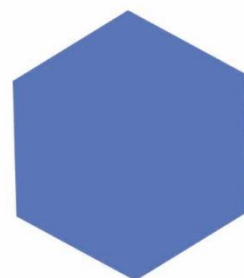


天衡法律通讯

2020第2期

T E N E T & P A R T N E R S

数据合规专刊



扫一扫
了解最新法律资讯

天衡动态

法规快讯

律师专栏

- 10 金融机构数据出境的监管进路
- 17 两岸个人信息识别机制探究
- 24 政府大数据运用中的法律合规问题研究

顾问：林楚雄
主编：林浩夫
责任编辑：周 玥

本期主题：数据安全合规

为您量身定做 的法律服务

信息技术与经济社会的交汇融合引发了数据迅猛增长，大数据正日益对全球生产、流通、分配、消费活动以及经济运行机制、社会生活方式和国家治理能力产生重要影响。党和政府已经深刻认识到数据的重要性，并将数据当作国家基础性战略资源对待。例如党的十九大报告指出“深化供给侧结构性改革要推动大数据和实体经济深度融合”；国务院通过下发《促进大数据发展行动纲要》、《政务信息资源目录编制指南（试行）》等纲领性文件，全面推进我国大数据发展和应用，数据时代已经悄然来临。

在党和政府的支持和推动下，我国大数据迎来了大发展和大繁荣的格局，目前，我国互联网、移动互联网用户规模居全球第一，拥有丰富的数据资源和应用市场优势，大数据部分关键技术研发取得突破，涌现出一批互联网创新企业和创新应用，例如阿里巴巴、百度、腾讯等。数据成为实体企业的重要资源，更是互联网企业生存的核心要素，数据即石油。然而，也正因为数据的价值凸显，数据黑灰产业不断滋生、数据泄露成为企业治理难题，甚至成为社会乱象，企业数据安全的合规设计亟需解决。天衡在此领域提供的专业服务内容主要包括：

非诉讼类产品

- 数据安全合规培训
- 隐私政策的合规设计
- 数据出境安全评估
- 特殊行业（金融机构、医疗机构等）数据安全合规诊断与设计

诉讼类产品

- 民商事数据纠纷
- 侵犯个人信息的刑事案件处理



若有进一步了解需求，欢迎向联系人提出咨询并索要相关材料。

联系人：李金招：0592-6304575 陈乙捷：0592-6304515 蒋晓焜：0592-2956982



01 天衡动态

天衡律师助力福建省首单可续期“疫情防控债”成功发行

近日，由福建天衡联合律师事务所提供专项法律服务的“厦门象屿集团有限公司公开发行 2020 年可续期公司债券（第一期）（疫情防控债）”成功发行，系福建省成功发行的首单可续期“疫情防控债”，本期债券发行规模合计人民币 16 亿元。

为积极响应防控疫情相关政策，打赢疫情狙击战，天衡律所指派许理想律师（合伙人）、潘舒原律师采用线上见证形式，对本次发行簿记建档过程进行见证并出具法律意见书，助力象屿集团成功发行本期债券。除本期债券外，疫情期间天衡律所许理想、陈珂两位合伙人为主的律师团队与客户、中介机构积极沟通，为多起债券发行项目提供了全流程法律服务，在非常时期助力企业拓宽融资渠道、降低融资成本。

近年来，天衡律所许理想、陈珂团队多次为厦门市国有企业提供债券发行项目法律服务，已涵盖公司债、企业债、中期票据、短期融资券、超短期融资券、ABS、CMBN 等多个品种债券。团队律师凭借在债权市场丰富的经验及严谨的工作态度赢得了广大客户的认可。

天衡泉州办公室合伙人杜鸣泉律师为泉州市挂牌、上市后备企业作“新冠肺炎”疫情下企业风控合规指引线上培训

2020 年 3 月 16 日，天衡泉州办公室合伙人杜鸣泉律师受泉州市金融监管局的邀请，通过线上直播的形式，为泉州市辖区内挂牌、上市后备企业的百余名负责人作“‘新冠肺炎’疫情下企业风控合规指引”培训。

为了帮助泉州市挂牌、上市后备企业为企业在“新冠肺炎”疫情期间尽快恢复正常生活经营活动，积极迎接《证券法》出台后的资本市场新时代，把握时间窗口尽快实施改制上市，泉州市金融监管局于近期举办“走进资本市场，全力复工复产”系列线上培训活动。杜鸣泉律师受邀参与首期培训，为辖区内挂牌、上市后备企业负责人作题为“‘新冠肺炎’疫情下企业风控合规指引”的培训讲座。



杜鸣泉律师从商务租赁、融资借贷、劳动用工、采购承揽四个版块，分析“新冠肺炎”这一突发公共卫生事件对企业各类合同履行可能产生的影响，并提出法律风险防控建议，为企业改制上市提供法律保障。

自“新冠肺炎”疫情发生以来，杜鸣泉律师所在律师团队通过编撰“新冠肺炎”疫情下企业合同履行指引手册、惠企政策汇编、线上直播培训等方式，积极主动为社会各阶层提供公益法律服务，从专业出发，为防疫工作贡献自己的力量。

新举措，履职责 ——厦门市思明区副区长、思明公安分局局长王嘉兴一行莅临天衡所调研指导

2020年3月25日，厦门市思明区副区长、思明公安分局局长王嘉兴率分局办公室副主任张劲嘉、分局法制队负责人许铭一行莅临福建天衡联合律师事务所对新时期法治社会治理新途径进行调研指导。天衡所党委书记王哲律师、党办主任温晓玲参加座谈。



王哲律师向王副区长等人介绍了天衡所的党建工作、党员律师业务开展情况，并共同参观了天衡荣誉室、党员律师调解室、党员活动室。

王副区长对天衡所的党建工作表示赞许并提出共建思路，双方就如何开展共建活动，推动建设人人有责、人人尽责、人人享有的社会治理共同体进行探讨。



王副区长指出，律师作为中国特色社会主义法律工作者应当发挥专业力量为建设法治社会、维护社会稳定做出更多贡献，希望思明分局和天衡所能进一步密切沟通，通过党建共建的形式，以派出所为载体共同推进社会治理，在促进矛盾纠纷多元调解机制方面做出新探索，为建设幸福思明做贡献。

王哲律师对王副区长就促进多元调解提出的举措表示赞同，下一步将加强与思明分局的密切联系，在党员律师深度参与派出所调解事务方面进行沟通探讨，充分引导党员律师发挥专业优势，积极主动服务基层群众，履行党员律师的社会责任。

助力外贸抗疫，本所陈川律师入选省商务厅外贸导师

疫情当前，为深化实施“助力万企成长”外贸辅导工作，继续发掘一批外贸经验丰富、讲授能力强、辅导效果佳的外贸导师充实外贸导师库资源，福建省商务厅组建第二批“福建外贸导师库”，从各机构选出了 22 名业务精通、政策熟悉、善于讲解的业务骨干聘任为“外贸实务导师”，我所陈川律师也在本次名单之列。

附件

第二批外贸实务导师名单

- | | |
|---------|--|
| 1. 郭伟耀 | 福建亚南电机有限公司 |
| 2. 林志萍 | 宁德师范学院 |
| 3. 张碧聪 | 武夷学院商学院国际贸易系 |
| 4. 林玲 | 中国建设银行福建省分行国际业务部 |
| 5. 陈晓声 | 中国建设银行福建省分行国际业务部 |
| 6. 赵慧英 | 中国建设银行福建省分行国际业务部 |
| 7. 周金铁 | 福建商学院国际经贸学院 |
| 8. 李宗皓 | 福建农林大学经济学院 |
| 9. 林本喜 | 福建农林大学经济学院 |
| 10. 梁丽萍 | 武夷学院商学院 |
| 11. 张梅 | 福建江夏学院 |
| 12. 赖慧文 | 福建江夏学院 |
| 13. 林必越 | 集美大学 |
| 14. 陈川 | 福建天衡联合律师事务所 |
| 15. 陈朝晖 | 中国国际经济贸易仲裁委员会福建分会、中国海事仲裁委员会福建分会、海峡两岸仲裁中心 |
| 16. 杨晨 | 北京金诚同达律师事务所 |
| 17. 肖静娟 | 冠达星股份有限公司 |
| 18. 曹毓前 | 漳州市九龙江集团有限公司 |

- 3 -



陈川律师为我所副主任兼国际商事海事与涉外部主任，本科毕业于北京大学、研究生毕业于厦门大学。执业前有十年从国企、外企到外贸企业的工作经验。2001 年执业至今处理过大量的国际贸易、海商海事、供应链金融、涉外纠纷案件。2017 年获得福建省律师协会授予的福建省优秀律师，2019 年入选司法部公布的全国千名涉外律师人才名单。此次陈川律师被聘任为“外贸导师”，将根据福建省商务厅的安排主要从外贸实务流程、外贸法律风险防控、客户洽谈技巧等各

方面为全省外经贸企业深入浅出地剖析外贸中的法律问题及风险防范。尤其针对本次疫情期间的特殊情形，陈川律师也将从企业的实际需求出发，系统全面地从法律层面对外经贸企业如何应对疫情风险等问题进行分析、献力献策。



02 法规快讯

法律

1. 电子商务法[2018.08.31 发布] [2019.01.01 实施]

第二十三条 电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。

第二十四条 电子商务经营者应当明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件。

电子商务经营者收到用户信息查询或者更正、删除的申请，应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的，电子商务经营者应当立即删除该用户的信息；依照法律、行政法规的规定或者双方约定保存的，依照其规定。

第二十五条 有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者应当提供。

有关主管部门应当采取必要措施保护电子商务经营者提供的信息的安全，并对其中的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第三十条 电子商务平台经营者应当采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动，有效应对网络安全事件，保障电子商务交易安全。

电子商务平台经营者应当制定网络安全事件应急预案，发生网络安全事件时，应当立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。

第三十一条 电子商务平台经营者应当记录、保存平台上发布的商品和服务信息、交易信息，并确保信息的完整性、保密性、可用性。商品和服务信息、交易信息保存时间自交易完成之日起不少于三年；法律、行政法规另有规定的，依照其规定。

2. 统计法[2009.06.27 发布] [2010.01.01 实施]

第三十九条 县级以上人民政府统计机构或者有关部门有下列行为之一的，对直接负责的主管人员和其他直接责任人员由任免机关或者监察机关依法给予处分：

（二）泄露统计调查对象的商业秘密、个人信息或者提供、泄露在统计调查中获得的能够识别或者推断单个统计调查对象身份的资料的；统计人员有前款所列行为之一的，依法给予处分。

3. 电子签名法[2019.04.23 发布] [2019.04.23 实施]

第二十四条 电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后五年。

司法解释

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[2017.05.08 发布] [2017.06.01 实施]

第三条 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，应当认定为刑法第二百五十三条之一规定的“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。

第四条 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，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第九条 网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

5. 检察机关办理侵犯公民个人信息案件指引[2018.11.09 发布][2018.11.09 实施]

根据《中华人民共和国刑法》第二百五十三条之一的规定，侵犯公民个人信息罪是指违反国家有关规定，向他人出售、提供公民个人信息，或者通过窃取等方法非法获取公民个人信息，情节严重的行为。结合《最高人民法院、最高人民检察院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》（法释〔2017〕10号），办理侵犯公民个人信息案件，应当特别注意以下问题：一是对“公民个人信息”的审查认定；二是对“违反国家有关规定”的审查认定；三是对“非法获取”的审查认定；四是对“情节严重”和“情节特别严重”的审查认定；五是对关联犯罪的审查认定。

6. 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[2014.08.21 发布][2014.10.10 实施]

为正确审理利用信息网络侵害人身权益民事纠纷案件，根据《中华人民共和国民事诉讼法》《中华人民共和国侵权责任法》《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》《中华人民共和国民事诉讼法》等法律的规定，结合审判实践，制定本规定。

7. 最高人民法院关于审理旅游纠纷案件适用法律若干问题的规定[2010.10.26 发布][2010.11.01 实施]

第九条 旅游经营者、旅游辅助服务者泄露旅游者个人信息或者未经旅游者同意公开其个人信息，旅游者请求其承担相应责任的，人民法院应予支持。

8. 关于办理利用信息网络实施黑恶势力犯罪刑事案件若干问题的意见[2019.07.23 发布][2019.10.21 实施]

为认真贯彻中央关于开展扫黑除恶专项斗争的部署要求，正确理解和适用最高人民法院、最高人民检察院、公安部、司法部《关于办理黑恶势力犯罪案件若干问题的指导意见》（法发〔2018〕1号，以下简称《指导意见》），根据刑法、刑事诉讼法、网络安全法及有关司法解释、规范性文件的规定，现对办理利用信息网络实施黑恶势力犯罪案件若干问题提出意见。

| 全国人大常委会的决定

9. 全国人大常委会关于加强网络信息保护的决定[2012.12.28 发布][2012.12.28 实施]

五、网络服务提供者应当加强对其用户发布的信息的管理，发现法律、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，保存有关记录，并向有关主管部门报告。

10. 全国人民代表大会常务委员会关于维护互联网安全的决定[2000.12.28 发布][2000.12.28 实施]

我国的互联网，在国家大力倡导和积极推动下，在经济建设和各项事业中得到日益广泛的应用，使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化，对于加快我国国民经济、科学技术的发展和社会服务信息化进程具有重要作用。同时，如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。为了兴利除弊，促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益，特作决定。

| 行政法规

11. 对外合作开采海洋石油资源条例 [2013.07.18 发布] [2013.07.18 实施]

第二十一条 为执行石油合同所取得的各项石油作业的数据、记录、样品、凭证和其他原始资料，其所有权属于中国海洋石油总公司。

前款数据、记录、样品、凭证和其他原始资料的使用和转让、赠与、交换、出售、公开发表以及运出、传送出中华人民共和国，都必须按照国家有关规定执行。

12. 畜禽遗传资源进出境和对外合作研究利用审批办法 [2008.08.28 发布] [2008.10.01 实施]

第二十条 我国的畜禽遗传资源信息，包括重要的畜禽遗传家系和特定地区遗传资源及其数据、资料、样本等，未经国务院畜牧兽医行政主管部门许可，任何单位或者个人不得向境外机构和个人转让。

13. 人类遗传资源管理暂行办法 [1998.06.10 发布] [1998.06.10 实施]

第十七条 我国境内的人类遗传资源信息，包括重要遗传家系和特定地区遗传资源及其数据、资料、样本等，我国研究开发机构享有专属持有权，未经许可，不得向其他单位转让。



03 律师专栏

金融机构数据出境的监管进路



蒋晓焜 律师助理

TMT 行业法律服务、私募股权与投资基金、
资本市场与金融、并购重组



李金招 合伙人、律师

TMT 行业法律服务、私募股权与投资基金、
资本市场与金融、并购重组

摘要：对于金融机构数据出境，中国人民银行建构了“原则禁止，以业务必需+客户同意+关联机构+保密为例外”的监管模式；网信办¹建构了“原则禁止，以经安全评估为例外”的监管模式。两个监管部门采用不同的监管模式凸显监管的思路不清晰、手段不具体、内容不明确。搭建金融机构数据出境的统一监管框架、制定金融机构数据合规识别指南以及做好金融机构数据合规内控，有助于解决金融机构数据出境的困局。

关键字：金融机构、数据出境、数据监管

金融机构的数据涉及个人财产信息、账户信息、信用信息、交易信息、身份信息等诸多敏感内容，²一旦发生泄露，影响的主体多，波及面广，后果不堪设想。因此保密义务一直以来都是金融机构的古老传统，例如，银行业等金融机构一直被要求不得泄露客户的身份信息、账户信息及交易信息等。³

然而，经济的全球化带来了金融机构数据的全球化流动。据悉，截至 2019 年 4 月，共有来自 54 个国家和地区的 215 家外国银行在华设立了 41 家外国银行法人、115 家外国银行的分行和 153 家代表处，外资银行的营业机构已经达到 982 家。⁴而随着我国改革开放力度的不断加大，外资金金融机构的数量还将持续增长。规模庞大的外资金金融机构在与外国关联机构保持信息交流的过程中，必然会涉及数据出境问题。因此，如何处理好数据出境问题，值得引起重视。

一、金融机构数据出境的监管模式梳理

当前，我国金融机构数据出境的监管模式上主要由中国人民银行和网信办各自监管。其中，中国人民银行采用“原则禁

¹ 本文的网信办指国家互联网信息办公室。

² 参见《关于银行业金融机构做好个人信息保护工作的通知》第 1 条。

³ 例如《个人存款账户实名制规定》第 8 条规定：“金融机构及其工作人员负有为个人存款账户的情况保守秘密的责任。”《人民币银行结算账户管理办法》第 9 条规定：“银行应依法为存款人的银行结算账户信息保密。”《反洗钱法》第 5 条规定：“对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密。”《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》第 3 条规定：“金融机构应当按照安全、准确、完整、保密的原则。”

⁴ 中国产业经济信息网：215 家外资银行已进驻中国 这些外资行收成如何？参见：<http://www.cinic.org.cn/hy/cj/535541.html>，2019.06. 最近一次访问：2019 年 7 月 2 日。

止，以业务必需+客户同意+关联机构+保密为例外”的监管模式；网信办采用“原则禁止，以经安全评估为例外”的监管模式。

（一）“原则禁止，以业务必需+客户同意+关联机构+保密为例外”的监管模式

2011年，中国人民银行发布《关于银行业金融机构做好个人金融信息保护工作的通知》（银发[2011]17号）（以下简称“17号文”），其中第6条规定“在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息”。17号文首次提出了金融机构对个人金融信息的存储、处理和分析原则上禁止出境，例外情形允许出境。但对于何种“例外情形”可以允许其出境，17号文仅规定“除法律法规及中国人民银行另有规定”，并未详细说明。

然而，未明确“例外情形”始终不利于实务中外资金融机构的数据出境。因此，在17号文出台后的4个月后，中国人民银行上海分行紧急发布《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》（上海银发〔2011〕110号）（以下简称“110号文”）。110号文指出17号文所称的“例外情形”包括“为客户办理业务所必需，且经客户书面授权或同意，境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。银行业金融机构应当保证其境外总行、母行或分行、子行为所获得的个人金融信息保密”。⁵110号文在17号文的基础上，规定在满足“业务必需+客户同意+关联机构+保密”四要件的基础上，允许金融机构数据出境。

由于110号文是上海分行发布的规范性文件，并不具有拘束全国的法律效力。为推广上海市的做法，2016年中国人民银行发布《金融消费者权益保护实施办法》（银发〔2016〕314号）（以下简称“314号文”），肯定了110号文的做法。关于金融机构数据出境的规定详见下表一：

表1：110号文和314号文关于金融机构数据出境对比表

	110号文	314号文
效力范围	上海地区	全国
内容	第4条规定：17号文第6条规定：“除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。”为客户 办理业务 所必需，且经客户书面授权或同意， 境内银行业金融机构 向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。 银行业金融机构应当保证其境外总行、母行或分行、子行为所获得的个人金融信息保密。	第33条规定：在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。 境内金融机构为处理跨境业务 且经当事人授权，向境外机构（含总公司、母公司或者分公司、子公司及其他为完成该业务所必需的关联机构）传输境内收集的相关个人金融信息的，应当符合法律、行政法规和相关监管部门的规定， 并通过签订协议、现场核查等有效措施，要求境外机构为所获得的个人金融信息保密。

资料来源：笔者自行制作。

上表可以看出，对于“例外情形”，314号文在肯定110号文的基础上也做了修改和完善。例如，扩大了监管对象的范围，将原来的“银行业金融机构”扩大为“金融机构”⁶，将原本的“境外总行、母行或分行、子行”扩大为“完成业务所必需的关联机构”；同时，将原先“办理业务”改为“处理跨境业务”，使得概念更加准确；此外，对于保密要件，314号在110号文的基础上，还规定金融机构必须签订协议或者现场核查，使得保密措施更具现实操作性。314号文发布之后，中国人民银行对金融机构数据出境的监管模式正式定为“原则禁止，以业务必需+客户同意+关联机构+保密为例外”。

⁵ 参见《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》第4条。

⁶ 《中国人民银行金融消费者权益保护实施办法》第2条规定：“在中华人民共和国境内依法设立的为金融消费者提供金融产品和服务的银行业金融机构，提供跨市场、跨行业交叉性金融产品和服务的其他金融机构以及非银行支付机构（本办法统称金融机构）适用本办法。”

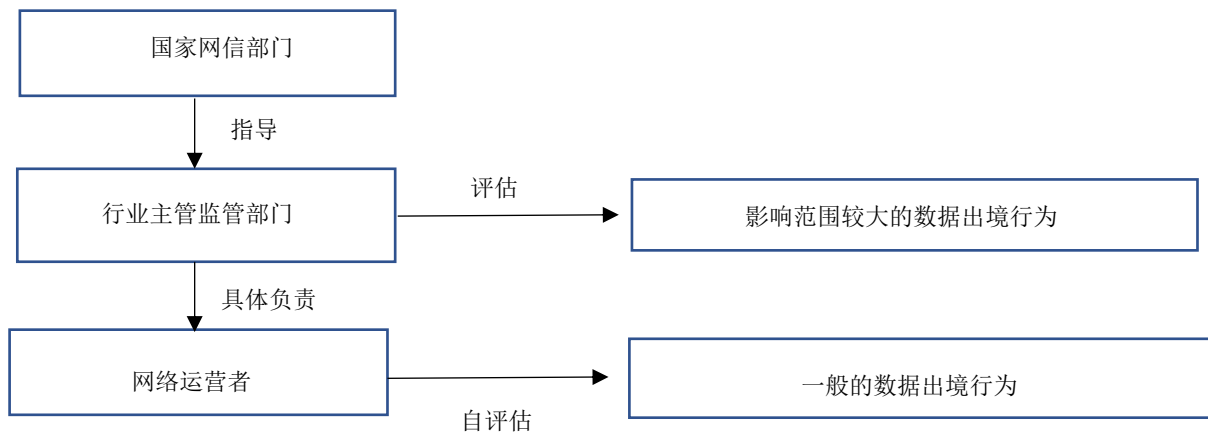
（二）“原则禁止，以经安全评估为例外”的监管模式

网信办对于金融机构数据出境的监管模式与中国人民银行的监管模式具有显著区别。《网络安全法》第 37 条规定：“关键信息基础设施⁷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。”可以看出，网信办对于数据出境的监管主要采用“原则禁止，以经安全评估为例外”的监管模式。

对于“例外情形”中如何做好“安全评估”，网信办发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》和《个人信息出境安全评估办法（征求意见稿）》对此做了不同规定。

《个人信息和重要数据出境安全评估办法（征求意见稿）》规定数据出境安全评估应遵循公正、客观、有效的原则⁸，国家网信部门统筹协调安全评估工作，指导行业主管或监管部门做好工作；⁹行业主管或监管部门负责具体的评估工作，评估时长为 60 个工作日；¹⁰网络运营者在数据出境前应做好自评估工作。但对于影响范围较大的数据出境行为，例如数据量超过 1000GB 等情形，网络运营者应报请行业主管或监管部门评估。¹¹同时，对于可能影响国家安全、损害社会公共利益等行为，数据不得出境。¹²综上所述，安全评估的具体流程详见下图：

图 1：安全评估的具体流程图



资料来源：笔者自行制作。

《个人信息出境安全评估办法（征求意见稿）》规定的安全评估方式又不同于《个人信息和重要数据出境安全评估办法（征求意见稿）》。《个人信息出境安全评估办法（征求意见稿）》规定数据出境的主管评估部门为省级网信部门，省级网信部门的审核时长为 15 个工作日。¹³网络运营者申报材料包括申报书、网络运营者与接收者签订的合同、风险评估报告和其他材料。该征求意见稿主要对合同的内容做了详细规定，¹⁴侧重以规范网络运营者与境外接收者合同内容的方式，来落实对数据出境的监管。实际上，该种监管手段借鉴了欧盟数据出境监管所采用的标准合同文本形式，¹⁵我国监管部门有尝试将发达国家运行成熟的监管模式引入本土，以实现其本土化移植的趋势。审核时长为 15 个工作日。¹⁶网络运营者申报材料包括申报书、网络

⁷ 《网络安全法》第 31 条规定“……金融……等关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。同时《关键信息基础设施安全保护条例（征求意见稿）》第 18 条规定关键信息基础设施的范围包括金融行业。

⁸ 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 3 条规定。

⁹ 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 5 条规定。

¹⁰ 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 6 条、10 条规定。

¹¹ 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 7 条、第 9 条规定。

¹² 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 11 条规定。

¹³ 参见《个人信息出境安全评估办法（征求意见稿）》第 3 条、第 5 条规定。

¹⁴ 参见《个人信息出境安全评估办法（征求意见稿）》第 4 条、第 13-17 条规定。

¹⁵ 张舵. 跨境数据流动的法律规制问题研究[D]. 北京: 对外经贸大学. 2018. 69-78.

¹⁶ 参见《个人信息出境安全评估办法（征求意见稿）》第 3 条、第 5 条规定。

运营者与接收者签订的合同、风险评估报告和其他材料。该号征求意见稿主要对合同的内容做了详细规定，¹⁷侧重以规范网络运营者与境外接收者合同内容的方式，来落实对数据出境的监管。实际上，该种监管手段借鉴了欧盟数据出境监管所采用的标准合同文本形式，¹⁸我国监管部门有尝试将发达国家运行成熟的监管模式引入本土，以实现其本土化移植的趋势。审核时长为 15 个工作日。¹⁹网络运营者申报材料包括申报书、网络运营者与接收者签订的合同、风险评估报告和其他材料。该号征求意见稿主要对合同的内容做了详细规定，²⁰侧重以规范网络运营者与境外接收者合同内容的方式，来落实对数据出境的监管。实际上，该种监管手段借鉴了欧盟数据出境监管所采用的标准合同文本形式，²¹我国监管部门有尝试将发达国家运行成熟的监管模式引入本土，以实现其本土化移植的趋势。

二、金融机构数据出境的监管困境

虽然我国监管部门对金融机构数据出境作出一定的规制，但观察上述两种不同的监管模式可以发现，监管部门对金融机构数据出境存在着监管思路不清晰、监管手段不具体、监管内容不明确等问题。

（一）监管思路不清晰，双头监管问题突出

根据法律适用原则，特别法优于一般法，新法优于旧法，新的一般法与旧的特别法不一致时应酌情决定如何适用。中央人民银行建立的监管制度本属于金融行业的数据安全特别法，但因其出台的文件均早于网信办出台的文件，因此属于旧法；网信办建立的监管制度虽然属于一般法范围，但其属于新法。因而二者之间何者优先适用并不明确。²²在适用情况不明确的情况下，两个监管部门出于不同的监管思路，采用了不同的监管模式，两种监管模式如何适用成为实践中的难题。在监管思路不清晰的情况下，双头监管下难免出现扯皮、推卸责任亦或争相监管的问题。

同时，网信办内部的监管思路也并不清晰。在《网络安全法》第 37 条确定建立“原则禁止，以经安全评估为例外”的监管模式后。对于如何进行“安全评估”，网信办在 2017 年 4 月发布《个人信息和重要数据出境安全评估办法（征求意见稿）》后，时隔 2 年，又重新发布《个人信息出境安全评估办法（征求意见稿）》，这两份征求意见稿规定的内容截然不同。例如，2017 年征求意见稿规定网信部门负责指导安全评估工作，2019 年征求意见稿规定网信部门直接负责安全评估；2017 年征求意见稿规定安全评估的时长为 60 个工作日，2019 年征求意见稿一下子将其缩短至 15 个工作日；2017 年征求意见稿主要规定安全评估的操作流程，2019 年征求意见稿主要规定网络运营者需提交的内容要求。两份征求意见稿时隔两年之久，规定的内容截然不同，足见网信办的监管思路并不清晰。

此外，中国人民银行的监管思路也不清晰。根据上文所述，314 号文虽然对 110 号文做了修改和完善，但仍有较多问题并未理清。例如，314 号文虽然肯定了“例外情形”的监管模式要满足“业务必需+客户同意+关联机构+保密”四要件。但该四要件说是唯一的“例外情形”还是“例外情形”中的一种，314 号文并未说明。同时，对于该“例外情形”的合法性，314 号文和 110 号文皆含糊其辞，110 号文采用“可不认为违规”的说辞，314 号文采用“应符合相关规定”的说辞，两份文件都未正面确认其合法性。可见，在中国人民银行内部，对于如何监管金融机构数据出境的思路也有待理清。

（二）监管手段不具体，缺乏可操作性

中国人民银行和网信办的监管模式在监管手段上是否具有足够的可操作性，也存在诸多可供商讨的地方。

在中国人民银行监管方面，314 号文虽然建构了监管模式，但其只是在理论上所作的建构，对于如何落地实施并未建立可操作化的指引。比如，对于“例外情形”的审核，如何确定审批主体，是由中国人民银行省级分行审批还是让金融机构自评估，没有规定；同时，对于“当事人授权”是否需要适用统一的格式合同，以及通过“签订协议”落实的保密措施，该协议内

¹⁷ 参见《个人信息出境安全评估办法（征求意见稿）》第 4 条、第 13-17 条规定。

¹⁸ 张舵. 跨境数据流动的法律规制问题研究[D]. 北京: 对外经贸大学. 2018. 69-78.

¹⁹ 参见《个人信息出境安全评估办法（征求意见稿）》第 3 条、第 5 条规定。

²⁰ 参见《个人信息出境安全评估办法（征求意见稿）》第 4 条、第 13-17 条规定。

²¹ 张舵. 跨境数据流动的法律规制问题研究[D]. 北京: 对外经贸大学. 2018. 69-78.

²² 冯坚坚、袁立志: 银行业金融数据出境的监管框架与脉络。参见: <http://www.jinciwei.cn/e598790.html>, 最近一次访问: 2019 年 7 月 3 日。

容如何规定，是否也需要统一的标准合同文本，均没有规定；再比如，314号文规定“其他为完成该业务所必需的关联机构”，如何确定此处的“关联机构”，怎么理解“完成业务所必需”，同样没有说明。

在网信办监管层面，征求意见稿虽然对“安全评估”的操作流程作出规定，但该方案是否能贯彻实施，同样值得怀疑。例如，2019年征求意见稿规定所有网络运营者都需上报所在地省级网信部门审核评估，网信部门需在15个工作日内完成安全评估工作。同时，发生较大数据安全事件、数据泄露安全事件时也需要上报省级网信部门。这意味着省级网信部门要在极短的时间内完成繁重的审查工作。同时，2019年征求意见还规定网络运营者需要提交申报书、合同、风险分析报告及其他材料，这些材料涉及技术安全、法律、金融、风控等多学科交叉知识，网信部门的工作人员是否有能力作出准确的审核意见，值得怀疑。

（三）监管内容不明确，存在模糊地带

监管部门对金融机构数据出境不仅存在监管思路、监管手段上的问题，在监管的内容上，也存在模糊地带。首先，网信办对于金融机构数据出境并未设置专门的条款进行规制。《网络安全法》所规范的数据出境监管对象是关键信息基础设施，金融机构只是作为关键信息基础设施的一部分受其监管。²³其次，中国人民银行也并未设置专法、甚至也无设置专章规范金融机构的数据出境。314号文只在第33条对金融机构数据出境作出规定。过于粗糙的法律规范极易产生大量的不确定性法律概念，从而使得数据出境监管存在诸多模糊地带。

拿最核心的“数据出境”概念来说，如果金融数据未转移存储至本国以外的地方，但能被境外的机构、组织和个人访问查看，是否属于“数据出境”？向在本国境内，但不属于本国司法管辖的主体提供个人金融信息，是否属于“数据出境”？还有，不在本国收集的个人金融信息，但途经本国出境，是否属于“数据出境”？同理，314号文规定金融数据的储存、分析和处理需要监管，那么金融数据向境外机构共享是否需要受到监管？须知，数据共享不同于数据处理，共享是指双方同时分别对数据拥有独立控制权，此时，境内机构仍然控制数据的所有权，那么，这时候数据算出境了吗？由此可见，监管部门对监管的内容未作精细化地处理，以致于数据监管的内容不明确，存在灰色地带。

三、金融机构数据出境监管困局的应对措施

根据上文可以看出，由于数据出境存在双头监管的现状，加之监管的思路、手段、内容均未清晰，以致于金融机构数据出境监管存在困境。笔者认为，通过搭建数据出境的统一监管框架、制定金融机构数据合规的识别指南，建立金融数据合规的内控制度，有助于解决金融机构数据出境的困境。

（一）搭建数据出境的统一监管框架

中国人民银行和网信办虽然对金融机构数据出境的监管思路有所不同，但其并非不可调和。其实，两个监管部门都坚持“原则上禁止数据出境”，只是在例外情况双方所采取的措施不同。然而，仔细研究两机关对于“例外情形”的规定会发现，倘若将中国人民银行所谓的“以业务必需+客户同意+关联机构+保密”的四要件审查机制，视为一种另类的“安全评估”审查机制，就会发现两个监管部门之间并非势如水火，相反，两者之间反而可以相互协作，共同监管。

根据上面的思路分析，笔者思考的统一监管框架的策略为：将网信办的“安全评估”机制引入中国人民银行对金融机构数据出境的场景中，规定网信办负责统筹协调金融机构数据出境的安全评估工作，指导中国人民银行各地市省级分行（行业主管）组织开展金融数据安全检查工作。而中国人民银行各地市省级分行负责金融数据出境的具体评估工作，具体的评估方法包括审查金融数据出境是否为业务必需，是否得到客户同意，接收方是否为金融机构的境外关联机构，是否有以合同的形式规定保密义务的条款（即原本的四要件审核机制）。从而在监管主体上、监管理念上、监管手段上打通监管机构之间先前存在的矛盾。

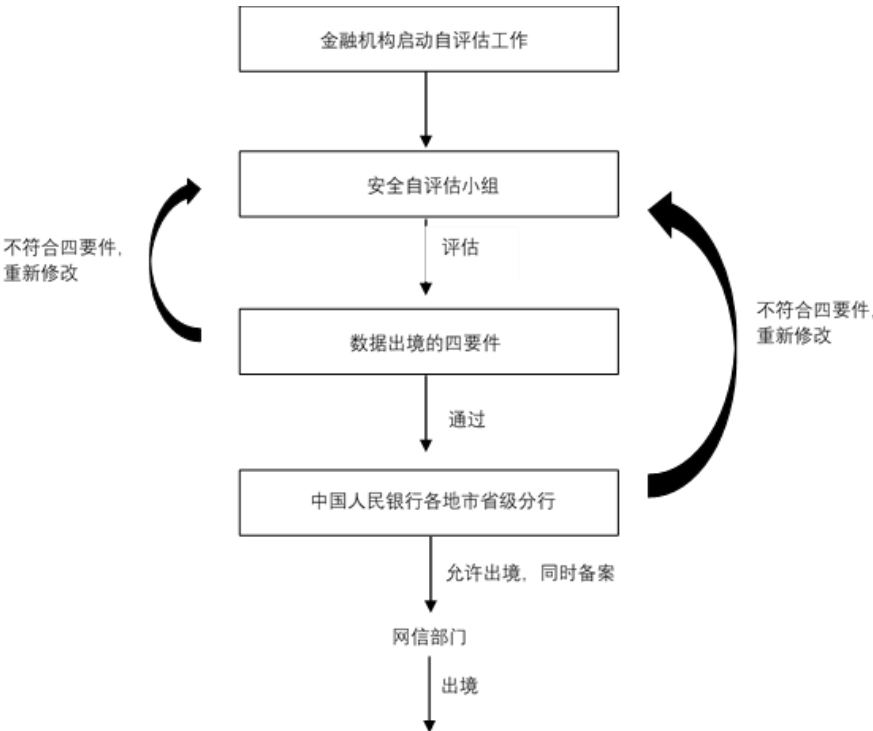
²³ 参见《网络安全法》第37条。

同时，如果将所有监管重任压在中国人民银行各地市省级分行头上，在各地市省级分行分身乏术的情况下，极有可能采取提高数据出境审核门槛的方式以减少案件受理量，或者以形式审查对金融机构数据出境进行从宽审查，以上几种方式均不利于保证数据出境的监管质量。为有效落实监管框架的可操作性，笔者认为金融机构在上报前，须完成自评估工作，以此减轻审批机关的工作量。金融机构数据出境的统一监管框架流程图如下图 2 所示：

（二）制订金融机构数据合规的识别指南

如同上文所述，由于金融机构数据出境的监管模式存在大量不确定性法律概念，由此导致监管内容存在诸多模糊地带。通过立法模式消弭不确定性法律概念是解决问题的重要方式，然而由于金融机构的数据出境只是众多数据出境中的一种类型，如果各个行业都采用立法模式规范各自行业的数据出境行为，将消耗巨大的司法成本。同时，立法耗时长，效率低，也难以及时处理实务中层出不穷的新问题。

图 2：金融机构数据出境的统一监管框架流程图



资料来源：笔者自行制作

因此，笔者建议，对于金融机构数据出境的不确定性法律概念，可以采用制定金融机构数据出境识别指南的方式解决问题。具体来说，中国人民银行和网信办可以共同研究、制订金融机构数据出境识别指南，也可以委托下属的事业单位或者相对应的技术部门研究制订。此外，金融机构数据出境的识别指南还可以以推荐性标准，甚至强制性标准的形式制定。实际上，对于数据的合规问题，近年来，国家质量监督检验检疫总局和国家标准化管理委员会已经联合发布了多号推荐性标准文件，例如《信息安全技术 数据出境安全评估指南》（征求意见稿）、《信息安全技术 个人信息安全规范》、《信息安全技术 网络安全等级保护》等。因此，对于数据出境的识别指南，以推荐性文件的形式发布也不失为可行的举措之一。

（三）建立金融数据合规的内控制度

对于金融机构的数据出境问题，笔者认为外部的监管有助于控制数据泄露的风险，但是最根本的控制方法在于金融机构要做好内部的风险控制。

例如，金融机构应当建立健全内部控制制度，对于易发生个人金融信息泄露的环节进行充分排查，强化网络数据安全全

流程管理，及时整改消除重大数据泄露、滥用等安全隐患，明确规定各部门、各岗位和人员的管理责任，加强个人金融信息管理的权限设置，形成相互监督、相互制约的管理机制。

同时，金融机构还应该完善金融数据安全管理制度设计，加快建立金融数据分类分级保护、金融数据安全风险评估、金融数据安全事件通报处置、金融数据对外提供使用报告等制度，完善信息安全技术防范措施，确保个人金融信息在收集、传输、保存、使用等环节不被泄露。

四、结 语

金融机构数据出境虽然只是众多行业领域数据出境的一种，但由于金融数据涉及个人财产、个人交易等敏感信息，庞大的金融数据一旦出境，对国家经济安全、社会公共利益均会产生极大的冲击和影响。因此，对于金融机构数据出境进行监管是必要之举，不容置疑。然而目前由于监管部门对于如何做好金融机构数据出境的思路并不清晰，以致于出现多头监管、双类监管思路、不同的监管手段等监管错位的种种问题。解决监管的问题本质在于理清监管思路，搭建统一的监管框架，以保障数据保护和促进数据流动。由于金融数据出境监管问题纷繁复杂，本文权属抛砖引玉，希望后期有更多实务界和理论界的专家学者能做更深入的研究。

参考文献：

- [1] 个人信息保护课题组. 个人信息保护国际比较研究[M]. 北京：中国金融出版社，2017 年。
- [2] 弓永钦. 跨境电子商务中的个人信息保护问题研究[D]. 北京：对外经贸大学. 2016.
- [3] 胡慧凯. 个人信息跨境流动的法律问题研究[D]. 上海：华东政法大学. 2016.
- [4] 【德】库勒. 杨会水等译. 欧洲数据保护法：公司遵守与管制[M]. 北京：法律出版社，2008 年。
- [5] 杨雪. 欧盟法中的个人数据保护问题研究——以欧盟跨境流动数据的保护为核心[D]. 北京：外交学院. 2017.
- [6] 周汉华. 个人信息保护前沿问题研究[M]. 北京：法律出版社，2008 年。
- [7] 张舵. 跨境数据流动的法律规制问题研究[D]. 北京：对外经贸大学. 2018.
- [8] 中国产业经济信息网：215 家外资银行已进驻中国, 这些外资行收成如何？
<http://www.cinic.org.cn/hy/cj/535541.html>. 2019. 06. 最近一次访问：2019 年 7 月 2 日
- [9] 全国人民代表大会常务委员会：《反洗钱法》。
- [10] 全国人民代表大会常务委员会：《网络安全法》。
- [11] 国务院：《个人存款账户实名制规定》。
- [12] 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》。
- [13] 中国人民银行：《人民币银行结算账户管理办法》。
- [14] 中国人民银行：《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》。
- [15] 国家互联网信息办公室：《个人信息和重要数据出境安全评估办法（征求意见稿）》。
- [16] 国家互联网信息办公室：《个人信息出境安全评估办法（征求意见稿）》。
- [17] 工业和信息化部：《电信和互联网行业提升网络数据安全保护能力专项行动方案》。
- [18] 中国人民银行上海分行：《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》。

两岸个人信息识别机制探究



蒋晓焜 律师助理

TMT 行业法律服务、私募股权与投资基金、
资本市场与金融、并购重组



李金招 合伙人、律师

TMT 行业法律服务、私募股权与投资基金、
资本市场与金融、并购重组

摘要：两岸个人信息¹识别机制包括形式和实质两要件。在形式要件上，大陆“识别+关联”的方式比台湾地区“直接识别+间接识别”的方式范围更广；在实质要件上，台湾地区“告知+多种许可渠道”的方式比大陆“告知+用户同意”的方式更具可行性。大陆的个人信息识别范围看似广泛，实际处处受限，延伸“用户同意”的内容，消减“用户同意”的强效力约束，打破“用户同意”的框架壁垒，有助于大陆个人信息识别机制的落地实施。

关键字：个人信息、识别机制、用户同意

在法律层面上，只有明确了个人信息的定义，才能开展后续信息收集、使用、处理、共享等法律行为。因此，识别个人信息是法律活动的开始，也是法律活动的前提和基础。大陆和台湾地区在个人信息收集、处理等发展流变中建构了各自的个人信息识别机制。笔者认为，通过对比两岸个人信息识别机制的异同，有利于大陆看到自身个人信息识别机制的不足，以此加以借鉴吸收。

一、台湾地区个人信息识别机制的发展流变

台湾地区个人信息识别机制随着台湾地区“个人信息保护法”的发展而逐渐形成，台湾地区对个人信息保护的立法，经历了从“电脑处理个人信息保护法”到“个人信息保护法”的演变。²在发展流变过程中，台湾地区个人信息识别机制的形式要件经历了从“直接识别”到“直接识别+间接识别”的演变过程；台湾地区个人信息识别机制的实质要件经历了从“多种许可渠道”到“告知+多种许可渠道”的演变历程。

（一）形式要件：从“直接识别”到“直接识别+间接识别”

1995 年，台湾地区发布“电脑处理个人信息保护法”，³其中规定个人信息是指“自然人之姓名、出生年月日、身分证统

¹ 本文所提及“个人信息”，在台湾地区，无论是立法还是学者讨论，都采用“个人资料”“个人资讯”的用语。为行文需要，本文统一使用“个人信息”的说法。

² 个人信息保护课题组. 个人信息保护国际比较研究[M]. 北京：中国金融出版社，2017 年. 385.

³ 台湾地区称其为“电脑处理个人资料保护法”。为统一称呼，本文将其称为“电脑处理个人信息保护法”。

一编号、特征、指纹、婚姻、家庭、教育、职业、健康、病历、财务情况、社会活动及其他足资识别该个人之数据”。⁴该条文列举了常见的个人信息，比如姓名、身份证、指纹等信息，同时在最后规定“其他足资识别该个人之数据”都归为个人信息，从而奠定了个人信息在形式上“直接识别”的判断标准。

但是，由于“直接识别”只能对显而易见的信息作出规定，有些信息虽未指名道姓，但一经揭露仍足以识别为某一特定人，对个人隐私仍会造成伤害。⁵因此，2010年台湾地区“个人信息保护法”⁶规定个人信息，是指“自然人之姓名、出生年月日、国民身分证统一编号、护照号码、特征、指纹、婚姻、家庭、教育、职业、病历、医疗、基因、性生活、健康检查、犯罪前科、联络方式、财务情况、社会活动及其他得以直接或间接方式识别该个人之数据。”⁷该规定将识别方式由原来的“直接识别”变为“以直接或间接方式识别该个人之数据”，从而建构“直接识别+间接识别”的形式要件模式。台湾地区个人信息识别机制形式要件的演变详见下表1：

表1：台湾地区识别机制形式要件变化表

“电脑处理个人信息保护法”	“个人信息保护法”	备注
个人信息：指自然人之姓名、出生年月日、身分证统一编号、特征、指纹、婚姻、家庭、教育、职业、健康、病历、财务情况、社会活动及其他足资识别该个人之数据。	个人信息：指自然人之姓名、出生年月日、国民身分证统一编号、护照号码、特征、指纹、婚姻、家庭、教育、职业、病历、医疗、基因、性生活、健康检查、犯罪前科、联络方式、财务情况、社会活动及其他得以直接或间接方式识别该个人之数据。	“个人信息保护法”在“电脑处理个人信息保护法”的基础上，增加了“护照号码、医疗、基因、性生活、健康检查、犯罪前科、联络方式”，并将识别方式改为“以直接或间接方式识别”。

资料来源：笔者自行制作。

（二）实质要件：从“多种许可渠道”到“告知+多种许可渠道”

形式要件是指只要符合识别标准，原则上都可归为个人信息的范畴。然而，有些个人信息即使符合个人信息范畴之列，但由于不符合收集个人信息的规范要求，仍无法搜集，笔者将该种要件称为识别机制的实质要件。

1995年，台湾地区“电脑处理个人信息保护法”规定“公务机关”收集个人信息应符合“……一、于法令规定职掌必要范围内者。二、经当事人书面同意者。三、对当事人权益无侵害之虞者”，⁸“非公务机关”收集个人信息应符合“……一、经当事人书面同意者。二、与当事人有契约或类似契约之关系而对当事人权益无侵害之虞者。三、已公开之资料且无害于当事人之重大利益者。四、为学术研究而有必要且无害于当事人之重大利益者。五、依本法第3条第7款第2目有关之法规及其他法律有特别规定者”。⁹可以看出，当时无论是公务机关还是非公务机关，只要满足“多种许可渠道”中的一种，则符合个人信息收集的“实质要件”。

2010年，台湾地区在“电脑处理个人信息保护法”的基础上制定了“个人信息保护法”，该法在上述“多种许可渠道”的基础上规定“公务机关或非公务机关依第十五条或第十九条规定向当事人搜集个人信息时，应明确告知当事人下列事项”。¹⁰从而将原先的“多种许可渠道”的实质要件延伸为“告知+多种许可渠道”，明确了个人信息识别机制的实质要件在于首先要先行“告知”，在“告知”的基础上，还要符合“多种许可渠道”，此种个人信息才属于真正意义上可以被采用的个人信息。

⁴ 参见台湾地区“电脑处理个人信息保护法”第3条第1款规定。

⁵ 参见台湾地区“立法院”第7届第1会期第2次会议议案关系文书。

⁶ 台湾地区称其为“个人资料保护法”。为统一称呼，本文将其称为“个人信息保护法”。

⁷ 参见台湾地区“个人信息保护法”第2条第1款规定。

⁸ 参见台湾地区“电脑处理个人信息保护法”第7条规定。

⁹ 参见台湾地区“电脑处理个人信息保护法”第18条规定。

¹⁰ 参见台湾地区“个人信息保护法”第8条规定。

二、大陆个人信息识别机制的发展流变

大陆个人信息的识别机制不同于台湾地区个人信息的识别机制。在形式要件上，大陆经历了从“直接识别”到“识别”再到“识别+关联”的经过，在实质要件上，大陆则一直以“告知+用户同意”作为采用个人信息的标准。

（一）形式要件：从“直接识别”到“识别”再到“识别+关联”

迄今为止，大陆并没有专门规范个人信息的法律，因此对个人信息识别机制的规定大多散落在各种规范性文件之中。其中，2012年全国人民代表大会常务委员会发布《关于加强网络信息保护的決定》，其中规定“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”，¹¹该《決定》从法律位阶上确定了个人信息“直接识别”的判断标准。

同时，“直接识别”的判断标准使得个人信息的范围变得异常狭窄，有些重要的个人信息都被排除在外，不利于监管。因此2016年发布的《网络安全法》规定个人信息是指“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”，¹²从而将判定标准拓宽为“直接识别+间接识别”，使得个人信息的界定范围扩大。

虽然《网络安全法》扩大了个人信息的识别范围，然而随着科技时代的到来，人民的上网记录、软件使用记录、用户日志的价值越来越受到重视，然而此种信息不符合现行的个人信息的范畴，无法被监管。基于此种现状，最高院、最高检在2017年发布《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》，其中规定公民个人信息是指“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。”¹³《信息安全技术 个人信息安全规范》进一步解释，判定某项信息是否属于个人信息，应考虑两个路径：一是识别，即从信息到个人；二是关联，即从个人到信息。¹⁴从而将个人信息识别机制确定为“识别+关联”的判断标准。大陆个人信息识别机制形式要件的演变详见下图1：

图1：大陆个人信息识别机制形式要件演变图



资料来源：笔者自行制作。

（二）实质要件：告知+用户同意

对于识别机制的实质要件，大陆从始至终一直采用的是“告知+用户同意”的唯一标准。也即，在信息采集者告知之后，如果未经用户同意，任何人、任何机构都不允许采用用户的个人信息。

2011年，工信部发布《规范互联网信息服务市场秩序若干规定》，其中规定“互联网信息服务提供者经用户同意收集用户个人信息的，应当明确告知用户收集和处理用户个人信息的方式、内容和用途”，¹⁵首次提及个人信息的采集必须明确告知用

¹¹ 参见全国人民代表大会常务委员会《关于加强网络信息保护的決定》第1条规定。

¹² 参见《网络安全法》第76条第5项规定。

¹³ 参见《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》第1条规定。

¹⁴ 参见《信息安全技术 个人信息安全规范》附录A规定。

¹⁵ 参见《规范互联网信息服务市场秩序若干规定》第11条规定。

户，并经过用户同意。2012 年人大常委会发布《关于加强网络信息保护的決定》再次重申“网络服务提供者和其他企业事业单位在业务活动中采集公民个人电子信息，应当遵循……，明示收集、使用信息的目的、方式和范围，并经被收集者同意”，¹⁶一个“并”字体现了“同意”是充分必要条件，是必须经历的程序。此后，无论是《消费者权益保护法》、《网络安全法》还是其他规范性文件，均把“告知+用户同意”当作采集个人信息必经的环节。是以，大陆个人信息识别机制的实质要件一直贯彻执行“告知+用户同意”的判断标准。

三、两岸个人信息识别机制的比较

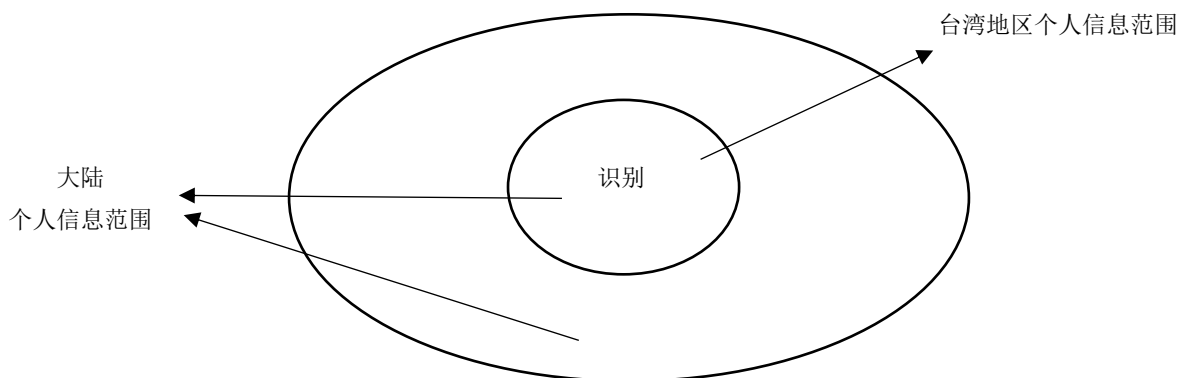
从两岸个人信息识别机制的发展流变可以看出，在形式要件上，大陆“识别+关联”的方式比台湾地区“直接识别+间接识别”的方式范围更广；在实质要件上，台湾地区“告知+多种许可渠道”的方式比大陆“告知+用户同意”的方式更具可行性。

（一）形式要件：大陆比台湾地区范围更广

大陆和台湾地区对于个人信息的定义范围在实务发展中均呈现逐步扩大的趋势。例如台湾地区从“直接识别”到“直接识别+间接识别”，而所谓的“间接识别”是指“保有该资料之公务或非公务机关仅以该数据不能直接识别，须与其他数据对照、组合、链接等，始能识别该特定之个人”。¹⁷因此可以看出，台湾地区对个人信息的范围界定既包括指名道姓的信息，也包括通过信息间对照、组合、链接可以识别的信息。比如单纯根据工号无法定位到个人，但如果结合工号所在的公司，则可以查询到个人，那么“工号”和“公司信息”就属于个人信息。

大陆在台湾地区“直接识别+间接识别”的判断基准上更进一步拓宽了个人信息的范围，大陆的识别机制不仅认为从信息本身的特殊性识别出特定自然人的信息属于个人信息，同时它还认为从已知特定自然人，则由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话信息、人格浏览记录等）也属于个人信息。¹⁸从而将个人信息的定义范围界定为单独或者与其他信息结合识别自然人身份，或者反映特定自然人活动情况的各种信息。两岸关于个人信息范围界定的对比图详见下图：

图 2：两岸个人信息范围对比图



资料来源：笔者自行制作。

从上图可以看出，大陆的个人信息比台湾地区范围更广。大陆这种模式的选择实际上来源于司法实践的总结提升。近些年来，随着科学技术的爆发性发展，很多涉及利用技术采集个人信息的法律问题开始凸显。例如，网页浏览器，例如 360 安全浏览器 5.0 正式版软件会收集并上传用户计算机中安装应用程序的情况；¹⁹cookie 技术会追踪用户在计算机上浏览的信息，

¹⁶ 参见《关于加强网络信息保护的決定》第 2 条规定。

¹⁷ 参见台湾地区“个人信息保护法施行细则”第 3 条规定。

¹⁸ 参见《信息安全技术 个人信息安全规范》附录 A 规定。

¹⁹ 参见浙江省杭州市中级人民法院(2014)浙杭民终字第 1813 号。

进而向用户精准推销广告。²⁰浏览器或者 cookie 收集用户在电脑上留存的信息如果以“识别”说来判断的话，虽然此类信息反映了网络用户的网络活动轨迹和上网偏好，具有隐私属性，但这种信息一旦与网络用户身份相分离，便无法确定具体的信息归属主体，因此不属于个人信息范畴。可见，“识别”说无法解决随着科学技术的发展而产生的新问题，因此在司法实践的基础上，大陆对识别机制的形式要件做了拓展，最终将“关联”说纳入界定标准。

（二）实质要件：台湾地区比大陆更加畅通可行

台湾地区对于个人信息采集的实质要件主要采用“告知+多种许可渠道”的方式，其中，在多种许可渠道的采集上，台湾地区又将个人信息分为一般信息和特种信息，对于不同信息采用不同许可渠道。台湾地区对于不同信息所采用的许可渠道方式详见下表：²¹

表 2：一般信息与特种信息采集许可渠道表

	一般信息 ²²	特种信息 ²³
许可渠道	一、法律明文规定。 二、与当事人有契约或类似契约之关系。 三、当事人自行公开或其他已合法公开之个人信息。 四、学术研究机构基于公共利益为统计或学术研究而有必要，且资料经过提供者处理后或搜集者依其揭露方式无从识别特定之当事人。 五、经当事人书面同意。 六、与公共利益有关。 七、个人信息取自于一般可得之来源。但当事人对该数据之禁止处理或利用，显有更值得保护之重大利益者，不在此限。	一、法律明文规定。 二、公务机关执行法定职务或非公务机关履行法定义务必要范围内，且事前或事后有适当安全维护措施。 三、当事人自行公开或其他已合法公开之个人信息。 四、公务机关或学术研究机构基于医疗、卫生或犯罪预防之目的，为统计或学术研究而有必要，且资料经过提供者处理后或经搜集者依其揭露方式无从识别特定之当事人。 五、为协助公务机关执行法定职务或非公务机关履行法定义务必要范围内，且事前或事后有适当安全维护措施。 六、经当事人书面同意。但逾越特定目的之必要范围或其他法律另有限制不得仅依当事人书面同意搜集、处理或利用，或其同意违反其意愿者，不在此限。

资料来源：笔者自行制作。

从上表可以看出，台湾地区的“用户书面同意”只是采集个人信息诸多许可渠道中的一种，台湾地区关于个人信息的采集还可以“法律明文规定”“当事人自行公开或其他已合法公开”等许可渠道进行采集。对比台湾地区在实质要件上的宽松机制，大陆的实质要件异常严格，规定只能在“用户同意”的前提下才能采集个人信息。因此，虽然大陆识别机制的形式要件看似放宽了个人信息的范围，然而，只要用户不同意信息被收集，面对异常宽泛的个人信息，信息采集者也无法采集任何的个人信息。

大陆“用户同意”的识别机制实际上会造成很多实务中的问题，例如，对于犯罪嫌疑人来说，公安机关出于社会安全的考虑，需要调查犯罪嫌疑人的信息，但如果需要经过犯罪嫌疑人的同意才能采集信息，这在实务中如何操作？法院审判中须调取病例、医疗等个人信息，如果也需要经过当事人明确同意，恐怕也将会影响案件的真实性；再比如卫生局要进行传染病的个人追踪管理、社区巡视检查，警察为了维护治安要定期查访，甚至有些职业不允许特定人员具有某些消极资格，例如食

²⁰ 参见江苏省南京市中级人民法院(2014)宁民终字第 5028 号。

²¹ 本文此处所说的个人信息采集的许可渠道仅指非公务机关对个人信息采集的许可渠道，不包括公务机关对个人信息采取的许可渠道。

²² 参见台湾地区“个人信息保护法”第 19 条规定。

²³ 参见台湾地区“个人信息保护法”第 6 条规定。

品卫生行业的从业人员不得患有传染类疾病，如果上述各类事项都需要经过当事人同意的话，很多行为将窒碍难行。可见，台湾地区开通多种采集信息的“许可渠道”比大陆以单一的“同意”作为准入门槛在实务中更有贯彻落实的可行性。

四、大陆个人信息识别机制困局的应对方法

根据上文可以看出，大陆的识别机制虽然在形式要件上放开了个人信息的识别范围，但是由于采集信息的门槛过高，使得形式要件成为水中月、镜中花，无法被贯彻实施。笔者认为，针对大陆个人信息识别机制的困局，可以通过延伸“用户同意”概念的内涵，消减“用户同意”的强约束效力，打破“用户同意”框架的约束，以此贯彻落实个人信息识别机制在实践中的运用。

（一）延伸“用户同意”概念的内涵

《网络安全法》等法律位阶性质的文件仅规定“须经用户同意”。但对于用户如何“同意”并未做细致规定。因此可以将“用户同意”视为不确定法律概念，在实务中可以通过对该概念意涵的延伸，从而降低个人信息采集的门槛。例如我们可以将“同意”的意涵尽可能延伸为类似“默示同意”“明示同意”等新的概念。所谓的“默示同意”是指对于用户不是特别重要的一般信息，只要履行告知义务，可以替用户勾选“同意”的按钮，甚至只要用户浏览了告知须知，就算用户已经同意；所谓的“明示同意”是指重要的敏感信息，都需要经过用户主动性的授权同意。

实际上，有些规范性文件已经开始在尝试以这种方式突破上位法的约束了。例如，《信息安全技术 个人信息安全规范》就延伸了上位法“同意”的内涵。该规范性文件将个人信息分为一般信息和敏感信息，对于一般信息只需要“授权同意”，对于敏感信息则需要“明示同意”。²⁴，其中，所谓的“授权同意”“如果现实中大量的场景做达不到明示同意的话，还是需要用到默示同意的”。²⁵

（二）消减“用户同意”的强约束效力

所谓的消减“用户同意”的强约束效力，主要指通过规定更多的例外情形，让被锁死的机制能散发出一些生机出来。正如前文所述，在法律规定采集个人信息的情形下，在需要调查犯罪嫌疑人信息的情形下，在警察巡视、公安逮捕犯人等情形下，应该在这种情形下规定免除“用户同意”，也即在涉及公共利益、国家安全等情况下应该规定例外情形。

实际上，《信息安全技术 个人信息安全规范》已经对个人信息采集的“同意机制”做了例外情形的规定，例如《信息安全技术 个人信息安全规范》规定“与国家安全、国防安全直接相关的；与公共安全、公共卫生、重大公共利益直接相关的；与犯罪侦查、起诉、审判和判决执行等直接相关的”等情形无需征得用户同意。然而，《信息安全技术 个人信息安全规范》仅是推荐性国家标准，并没有法律效力，只能作为参考的依据。目前《网络》《消费者权益保护法》等法律位阶的文件均未对“用户同意”机制设置例外情形规定，笔者认为有效消减“用户同意”的强约束效力的方式在于利用实施细则或者更改法律规定的方式将“例外条款”增加进去。

（三）打破“用户同意”框架的约束

“用户同意”是《网络安全法》明文规定的内容，该规定就像紧箍咒牢牢锁住信息采集者的一举一动，使其很难有所自主举动。有学者坦言“《网络安全法》第41条第1款中写‘经被收集者同意’，这里没有给任何例外……《网络安全法》给了这样的一个框架，因此《个人信息安全规范》应当在这个框架下做进一步的细化……法律框架事先给我们就是这样的一个框架，在这个框架下，我们好比说就是带着镣铐在跳舞，我们不能说把镣铐挣脱掉在那儿跳舞，肯定是不对的”。²⁶

虽然《网络安全法》设置“用户同意”目前难以更改，然而根据“十三届全国人大常委会立法规划”规定，《个人信息保护法》归于第一类立法项目，属于“条件比较成熟、任期内拟提请审议的法律草案”。由此可以基本确定，《个人信息保护法》

²⁴ 参见《信息安全技术 个人信息安全规范》第5.3条、第5.5条的规定。

²⁵ 腾讯网：对《个人信息安全规范》五大重点关切的回应和解释。参见：<https://new.qq.com/omn/20180205/20180205B0HBL7.html>，最近一次访问：2019年7月24日。

²⁶ 腾讯网：对《个人信息安全规范》五大重点关切的回应和解释。参见：<https://new.qq.com/omn/20180205/20180205B0HBL7.html>，最近一次访问：2019年7月24日。

将在十三届全国人大常委会期间获得通过。如果在《个人信息保护法》中可以将“用户同意”的束缚打破，笔者认为将有助于个人识别机制的贯彻实施，能促进个人信息的流动和发展。

五、结 语

两岸间的个人信息识别机制在发展过程形成了各自的模式特点，大陆对于个人信息的界定范围更广，有利于拓宽实务中的个人信息监管，但是大陆对于个人信息的实质要求更加严格，可能会导致信息的流动受阻。借鉴台湾地区所采取的“多种许可渠道”方式，延伸“用户同意”的内容，消减“用户同意”的强效力约束，打破“用户同意”的框架壁垒，有助于实现个人信息的流动和发展。

参考文献：

- [1]个人信息保护课题组. 个人信息保护国际比较研究[M]. 北京：中国金融出版社，2017 年。
- [2]【德】库勒. 杨会水等译. 欧洲数据保护法：公司遵守与管制[M]. 北京：法律出版社，2008 年。
- [3]杨雪. 欧盟法中的个人数据保护问题研究——以欧盟跨境流动数据的保护为核心[D]. 北京：外交学院. 2017.
- [4]周汉华. 个人信息保护前沿问题研究[M]. 北京：法律出版社，2008 年。
- [5]腾讯网：对《个人信息安全规范》五大重点关切的回应和解释。参见：
<https://new.qq.com/omn/20180205/20180205B0HBL7.html>，最近一次访问：2019 年 7 月 24 日。
- [6]全国人民代表大会常务委员会：《网络安全法》。
- [7]全国人民代表大会常务委员会：《关于加强网络信息保护的決定》。
- [8]最高院、最高检《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》。
- [9]国家质量监督检验检疫总局和国家标准化管理委员会：《信息安全技术 个人信息安全规范》。
- [10]工信部：《规范互联网信息服务市场秩序若干规定》。
- [11]台湾地区“个人信息保护法”。
- [12]台湾地区“电脑处理个人信息保护法”。
- [13]浙江省杭州市中级人民法院(2014)浙杭民终字第 1813 号。
- [14]江苏省南京市中级人民法院(2014)宁民终字第 5028 号。
- [15]台湾地区“立法院”第 7 届第 1 会期第 2 次会议议案关系文书。

政府大数据运用中的法律合规 问题研究



蒋晓焜 律师助理

TMT 行业法律服务、私募股权与投资基金、
资本市场与金融、并购重组

摘要：为了破解政务信息化造成的“信息孤岛”，国家大力开展政务信息资源整合工作，并取得一定成效。但政务信息资源仍存在来源不明、信息整理不规范、共享界定不清、开放设计过于粗糙等问题。做好内部数据风控合规，规范外包机构的资质审批，制定政务数据的标准和政策，有助于实现政务数据整合的法律合规。

关键词：政务信息资源；政务数据整合；数据合规

随着信息时代的到来，为了对传统的政府管理和公共服务进行改革，政府在 20 世纪 90 年代启动了重大信息化应用工程，召开了全国信息化工作会议。同时，党的十六大做出了以信息化带动工业化、以工业化促进信息化、走新型工业化道路的战略部署；党的十六届五中全会进一步强调，推进国民经济和社会信息化，加快转变经济增长方式。¹

在 21 世纪初期，政府信息化发展战略取得初步成效，各大政府部门网站纷纷设立，但同时各部门间存在着“各自为政、条块分割”的问题，“信息烟囱”、“信息孤岛”林立，政务信息难以被打通，政府信息化纵深发展遭遇困境。

一、政务信息资源的整合发展

为了解决政府信息“各自为政”的问题，2015 年在党中央部署下，国务院发布了《促进大数据发展行动纲要》。该文件明确提及要促进政府数据的整合，包括数据的共享和数据的开放。政府大数据的整合工作就此开始加速开展。政府信息资源的整合主要从三方面展开，分别是：发布文件规章，力图搭建数据整合的制度体系；完善基础设施建设，支撑数据整合发展；促进政务信息资源的整合，共享开放数据资源。截至目前，政务信息资源的整合已取得一定成效。

（一）制度先行，顶层设计发挥效用

国务院在 2015 年发布《促进大数据发展行动纲要》后，随后在 2016 年 2 月 4 日批准由国家发改委、工信部等多部门牵头，共同成立了“大数据发展部际联系会议”。该“部际联系会议”作为联系各个部门的枢纽和桥梁，通过几次会议的召开，下发了诸如《政务信息资源共享管理暂行办法》、《政务信息资源目录编制指南（试行）》等文件，进一步推动了政务数据的整

¹ 参见《2006—2020 年国家信息化发展战略》的规定。

合。截至目前，通过制度巩固共识，政府部门已经摸索出一套编制政府信息资源目录的方法，并对政务数据的共享、责任划分、机构设置有了清楚认识。²

在制度建设方面，政府的做法主要是通过顶层架构的设计，利用国务院的力量，统合各部门的分散势力，并借助“大数据发展部级联系会议”的平台，将各个部委对于政务数据的不同诉求放在同一台面上进行讨论、博弈、协商。最后，将各个部门妥协的结果通过规范文件进行固定，并通过行政力量层层下发传导，最终完成数据的整合。国家利用行政的力量推动数据整合的进程图详见下图：

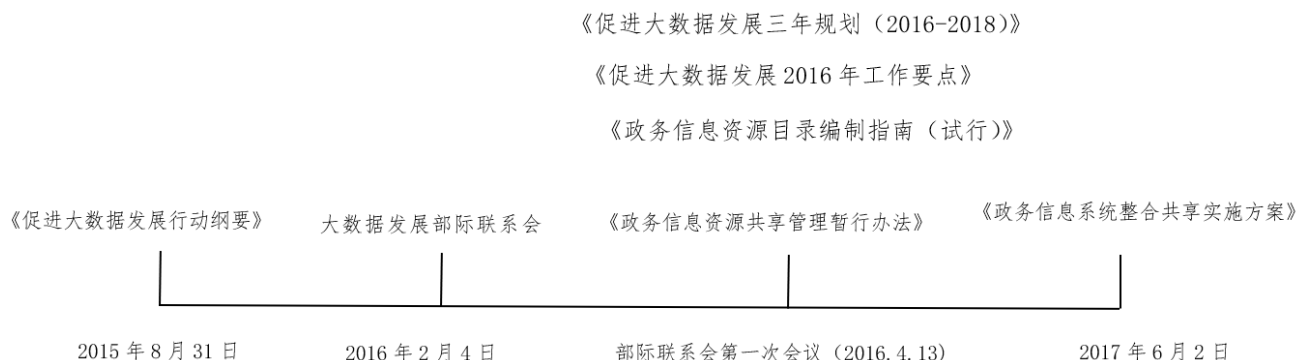


图 1：数据整合的进程图

（二）技术支持，基础设施初具规模

除了制度先行外，政府在基础硬件设施上也投入了大量人力、物力进行建设。《“十三五”国家政务信息化工程建设规划》明确提出，要按照“数、云、网、端”融合创新趋势及电子政务集约化建设需求，建设综合性公共基础设施平台；同时要建成统一的国家数据共享交换枢纽，全面贯通省级数据共享交换枢纽节点。³截至目前，政府已经搭建了国家电子政务内网和外网，并实现中央、省、市、县各级政府部门的多级覆盖。⁴

在技术支持方面，政府的做法主要是依照政务数据共享和开放的思路进行基础硬件设施的搭建。通过构建一体化政务数据平台，建设政务外网和内网，并通过内网和外网多环节、多节点的打通互联以实现数据无阻碍、多级流通、各点共享和有序开放。

（三）数据整合，政务平台共享开放

政府的制度推行和基础设施建设，归根到底是为了实现数据的整合。在数据的整合上，政府利用政务云搭建全国统一国家政务数据中心，通过元数据的抽取、编制，政府信息资源目录的采集、归类，将编排合理的数据归类为人口基础信息库、法人单位基础信息库、自然资源和地理空间基础信息库等，存储入国家政务数据中心。截至目前，国家政务数据中心初具规模，中央、省、市、县四级的数据开始逐步汇入数据中心。⁵

在数据整合方面，政府的做法主要是通过政务数据的有序编制、汇总，形成政务数据库，在各级政府部门有需要时，通过申请，直接在数据库中共享相关数据；在政府开放网站有需要时，直接提出不涉密信息，对外进行开放。最终，使整个政务数据体系高效、有序运行。

² 参见《政务信息资源目录编制指南（试行）》。

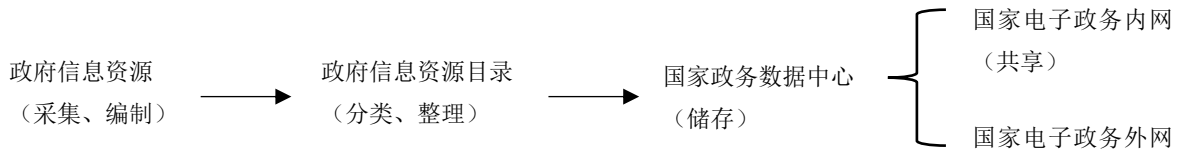
³ 参见《“十三五”国家政务信息化工程建设规划》第三章“主要任务”。

⁴ 参见景亚萍：《贵州省政务数据治理探索与实践》，载《软件与集成电路》，2019，（8）：72-73；应验：《政府数据开放共享与共享社会建设：海南的举措和探索》，载《电子政务》，2019，（198）：82-90；周亚，李东，王翠：《对北京市政务大数据建设与发展的建议》，载《中国工程咨询》，2019，（8）：65-68；

⁵ 铁金，刘光昊，刘苑，冯鑫：《国内政务大数据研究热点分享》，载《中国管理信息化》，2019，（22）：116-117。

二、政务信息资源整合发展中的法律问题

政务信息资源的整合截至目前具有一定的成效，它通过硬件设施的建设、制度的推行，按照一套规范流程进行数据的整合。具体的流程为：首先，各级政府部门进行政务信息资源的采集，在采集的政务信息资源中抽取出元数据，将其数据化。⁶其次，将数据化的信息放入各类政府信息资源目录，例如“姓名”以编号 01 的方式放入人口基础信息库，“长江”以编号 02 的方式放入地理空间基础信息库。⁷然后，再将政府信息资源目录统一存储在国家政务数据中心。最后，各级部门机构如有需要，可申请共享政务数据，公民如果有需要查询，政务数据中心可开放非涉密信息以供查询。⁸整体流程详见下图：



然而，经过研究分析，笔者发现政府数据的整合在数据的来源、整理、共享和开放等多个环节都存在着法律问题。

（一）数据来源不合法，数据毒果暗自潜藏

在数据的来源上，《政务信息资源共享管理暂行办法》规定政务数据可通过政府部门直接采集或者第三方依法采集。⁹实际上，政府直接采集的数据因为有公权力的背书，因此本身具有一定的合理性。但是，通过第三方采集的数据，如何确保数据来源的清洁度，如何评估数据来源的合法性？

须知，政务数据的整合，从 2015 年国务院发布《促进大数据发展行动纲要》至今，才发展短短数载，制度推行上更关注的是如何协调各部门的利益冲突，以落实政务数据的整合。而对于如何通过第三方合法采集数据，并未出台专门的规范性文件。换言之，在政府数据的第三方采集上法律上并未做出专门规定。而在政府未经监管的地带，灰色空间便会滋生，或慑于政府公权力或贪于数据的财产价值，第三方在采集数据时未免不会发生违法收集数据的问题。由于上述观点未有真实数据加以支撑，论证难免显得单薄，笔者在下文将以征信机构为例，¹⁰反面论证上述观点。

众所周知，征信机构的职责在于采集用户的征信数据，个人征信机构的设立须经中国人民银行批准，并应具备相应的资质条件，同时征信机构的相关信息也须进行公开披露。¹¹按理说，由于征信机构的运作较为规范，政府采集该类机构的数据理应较为合规。然而实践中仍存在征信机构非法收集用户数据的问题，最典型例子是 2017 年“支付宝账单案”。2017 年支付宝在《芝麻服务协议》里规定芝麻信用可以直接向第三方提供用户的相关信息，而无须再经过用户的明示同意。该协议的规定被用户视为霸王条款，引发社会的广泛争议，最终以芝麻信用道歉并取消该协议而告终。

可以看出，即使在有政府监管的地带，第三方采集用户数据尚且存在违法行为，遑论未经监管的地带呢？一旦第三方收集信息数据存在清洁度不够，违法收集信息，此类数据将可能成为数据毒果，对后期数据的使用、共享和开放都产生难以想象的危害。

（二）数据整理不规范，数据泄露存在风险

在数据的整理上，《政务信息资源共享管理暂行办法》规定各政务部门应按要求编制、维护、更新部门政务信息资源目录。

⁶ 参见《政务信息资源目录编制指南（试行）》的做法。具体做法为将政务信息资源数据化，例如身份证上 18 位数字代表个人信息一样，政务信息资源的多位数字，代表某一种政务信息。

⁷ 此处编号 01、02 只是为了方便展示，并非实务操作中的正式编号模式。

⁸ 彭 景, 郑玉波, 李思思. 构建政务数据开放共享体系[J]. 电信技术. 2019, (7): 85-88.

⁹ 《政务信息资源共享管理暂行办法》第 2 条规定：“本办法所称政务信息资源，是指政务部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等。”

¹⁰ 征信机构采集的用户数据，可供政府部门做决策参考。国家对于征信机构有出台一系列的文件进行规范。例如《征信业条例》、《征信机构管理办法》、《征信机构监管指引》等。但由于监管文件只局限在规范征信领域，不属于专门规范第三方采集用户数据的文件。因此，笔者认为截至目前，我国尚未出台专门的规范性文件，以规范第三方合法采集用户数据。

¹¹ 参见《征信机构管理办法》的规定。

¹²经悉，政务信息资源目录分类包括资源属性分类、涉密属性分类、共享属性分类和层级属性分类，各个分类还需进行对应的小项分类。¹³同时，根据《网络安全法》的规定，网络运营者应当按照网络安全等级保护制度的要求，制定网络安全管理制度和操作规程，进行数据分类、重要数据备份和加密等。¹⁴同时，政务信息资源目录等数据整理好后，还需要上传至政务云平台。

15

从上文可以看出，政务信息资源目录的编制耗时长、工程量较大，需要的人手较多。行政资源有限的政府部门常将数据外包给外面的第三方机构处理，¹⁶同时由于政务云的搭建专业技术壁垒较高，很多政府部门无法独立完成，也常外包给第三方技术机构进行处理。¹⁷其中，数据的外包，特别是承载数据的基础设施的整体外包，存在极大的数据泄露风险。

而在政务信息资源的维护、更新上，笔者经检索，发现很多事业单位尚未意识到数据的重要性，并未贯彻落实网络安全等级保护制度的要求，未做数据备案，未设置数据安全负责人，在数据安全保护上存在诸多缺失，极易导致数据的泄露。¹⁸数据规范不到位的案例详见下表：

表 1：数据安全违规违法案例表

处罚对象	执法机关	检查/违规行为	处罚措施
某社区服务中心工作人员	旺苍县公安局网警大队	利用服务部门内网，非法获取个人信息	移送法办
某省直事业单位	某市、县两级公安机关网警	未按照网络安全法规定，采取内部安全管理制度和操作规程等措施	警告并责令改正
淮南职业技术学院	淮南市公安局网警支队	未落实网络安全管理制度，未建立网络安全防护措施，网络日记留存少于 6 个月	警告并责令改正
某事业单位	某公安机关网警	未落实网络安全管理制度，未建立网络安全防护措施，网络日记留存少于 6 个月	罚款
.....			

可以看出，政务部门在政务信息资源的编制、维护和更新上，由于数据保护的意识不强，存在着数据保护力度不足，数据泄露问题等突出问题。

（三）数据共享不明确，数据孤岛难以破除

政务信息资源按共享类型分为无条件共享、有条件共享和不予共享等三种类型。¹⁹其中，无条件共享的信息资源，使用部门可以直接获取；有条件共享的信息资源，使用部门须提出申请；不予共享的信息资源，提供部门须说明说明。²⁰

政务信息资源的共享类型看似分类清晰，然而仔细推敲会发现，该划分并未能起到实际作用。由于三种类型的概念界定都属于不确定性法律概念，究竟哪些信息资源可以无条件共享，哪些可以有条件共享，哪些是不予共享的，法律并没有给予清晰的界定。进一步分析，在不予共享的类型上，《政务信息资源共享管理暂行办法》规定只要提供部门提供理由，可以不予共享。实务操作中常有行政部门不愿共享、不敢共享的情形，在这种情形下，如果把信息资源不予共享的主动权给予提供部门，信息资源的整合便会存在阻碍，“信息孤岛”问题照旧无法彻底解决。²¹

¹² 参见《政务信息资源共享管理暂行办法》第 8 条规定。

¹³ 参见《政务信息资源目录编制指南（试行）》。

¹⁴ 参见《网络安全法》第 21 条规定。

¹⁵ 参见“十三五”国家政务信息化工程建设规划。

¹⁶ 例如广州 12345 政府服务热线数据就外包给第三次数据机构处理，参见：中国政府采购网：

http://www.ccgp.gov.cn/cggg/dfgg/gkzb/201905/t20190515_12079830.htm。最后一次访问：2019 年 10 月 28 日。

¹⁷ 例如关于金华市电子政务中心金华市政务云资源大数据服务外包项目的单一来源采购公示，参见：中国政府采购网：

http://www.ccgp.gov.cn/cggg/dfgg/dylygg/201512/t20151217_6353663.htm。最后一次访问：2019 年 10 月 28 日；内蒙古自治区经济信息化委员会本级内蒙古自治区电子政务外网云中心外包服务项目中标（成交）公告，参见：中国政府采购网：http://www.ccgp.gov.cn/cggg/dfgg/zbzg/201710/t20171023_9030164.htm。最后一次访问：2019 年 10 月 28 日。

¹⁸ 周汉华. 个人信息保护前沿问题研究[M]. 北京：法律出版社，2008 年，57-79.

¹⁹ 参见《政务信息资源共享管理暂行办法》第 9 条规定。

²⁰ 参见《政务信息资源共享管理暂行办法》第 12 条规定。

²¹ 徐冠军. 试论政务大数据——政府回应改造现实性路径[J]. 北方经贸. 2019, (8)：3-6.

为了验证笔者的观点，笔者研究对比了“国家政务服务平台”APP、福建省“闽政通”APP和厦门市“i 厦门”APP存在数据开放不充分的问题。²²经对比，笔者发现福建省“闽政通”上的政务数据并未完全开放至“国家政务服务平台”，²³“i 厦门”上的政务数据也未全部开放给福建省“民政通”，²⁴也即中央、省和地市的政务数据并未全部互通开放。

笔者认为上述政务信息资源的开放共享目前存在最大问题的因素在于，立法机构尚未厘清哪些政务数据可以开放共享，哪些政务数据不能开放共享。而最本质的原因在于提供部门本身出于部门利益及害怕担责，不敢分享、不愿共享数据。

（四）数据开放不谨慎，数据爬取问题突出

2019年4月国务院发布《政府信息公开条例》，该行政法规正式确立了行政机关公开政府信息，应坚持“以公开为常态，不公开为例外”的原则，²⁵同时修改了旧条例对于公民、法人或其他组织因“自身生产、生活、科研等特殊需要”才能申请信息公开的规定，规定公民、法人或者其他组织可以直接申请信息公开。²⁶可见，新《政府信息公开条例》扩大了政府信息公开的深度和广度，有利于政府信息的透明和公正。

但同时，笔者也对政府信息的扩大开放深感忧虑。众所周知，在旧《政府信息公开条例》期间，政府信息公开网就经常出现公民信息遭受泄露的情况，如今新《政府信息公开条例》的发布，进一步扩大了政府信息公开的幅度，但同时也提高了个人信息泄露的风险。如何有效平衡政府信息公开与个人隐私之间的冲突值得引起深思。下表为政府信息泄露的案例情况检索：

表 2：政府信息公开泄露案例表

政府	公开行为
铜陵市政府信息公开网	《阳光社区 2017 孕优生健康检查人员名单》（索引号 080313743/201708-00058）公布了 40 对夫妻的姓名及检查日期，其中 77 人的身份证号码完整呈现，名单仅对现居住地地址做了模糊处理。
合肥市政府信息公开网	《庐阳区杏林街道城市医疗救助对象花名册（1-10 月）》（索引号：77499343X/201710-00017），公开了居民住址、联系电话等个人信息。此外，这些人的病情也可以被查看，包括尿毒症、肺癌、慢性肾衰竭等。
景德镇市政府信息公开网	《第二批大学生一次性创业补贴公示》（信息索取号：H00140-0403-2017-0077）公布了学生姓名、完整身份证号以及联系电话等。
宜春市政府信息公开网	《关于公布 2017 年会计专业技术初级资格无纸化考试宜春考区合格人员名单的通知》（信息索取号：C00120-0403-2017-0005）中，包括了泄露详细个人身份证号码的人员名单。
.....	

实际上，实务中常出现大数据公司利用爬虫技术爬取政府公开的相关信息，再利用爬取的数据进行二次利用。大数据公司爬取数据的行为本身问题不大，但问题在于有些大数据公司并未做好风控合规，对爬取的数据未清洗、未去标识化，而是利用数据的财产属性，直接将数据转卖给需求方，对数据主体造成了很大的伤害。前段时间杭州大数据公司高管纷纷被逮捕，最初的起源便是来自于催收公司购买大数据公司所爬取的个人信息，再利用拿到的贷款人的定位信息找到被害人，最后将被害人逼到跳楼自杀。²⁷

²² 由于政务信息资源共享须有限进入行政机构内部调研，受制于现实因素，政务信息资源的共享无法调研。但由于政务信息资源在开放和共享上具有共同性，笔者尝试通过政务信息资源在开放上的对比研究，验证政务信息资源在共享开放上并不透明，导致“信息孤岛”问题难以被打破。

²³ 具体而言，“国家政务服务平台”上关于福建省的政务数据只有“医疗卫生”和“其他”两类；但“民政通”服务平台上，福建省的政务数据有“台风路径”“公积金查询”“ETC 预约办理”“医保二维码购药”“社保查询”等多种分类。

²⁴ 具体而言，福建省“民政通”服务平台中关于“纳税缴费”栏目只有“财政票据真伪查验”一栏；而厦门市“i 厦门”服务平台上关于“税务服务”栏目有“厦门税务”“办税等候情况”“办税预约”“非税票据验证”等多种分类。

²⁵ 参见《政府信息公开条例》第 5 条的规定。

²⁶ 参见《政府信息公开条例》第 27 条的规定。

²⁷ 参见中国新闻周刊：整肃爬虫公司，网址：<http://www.inewsweek.cn/survey/2019-10-21/7327.shtml>，最后一次访问：2019 年 10 月 28 日。

三、政务信息资源整合发展中的法律合规路径

根据上文可以看出，政务信息资源仍存在来源不明，信息整理不规范、共享界定不清、开放设计过于粗糙等问题。笔者认为做好内部数据风控合规，规范外包机构的资质审批，制定政务数据的标准和政策，有助于实现政务数据整合的法律合规。

（一）搭建内部数据风控体系，保证数据合规

对于政务数据整合，笔者认为外部的监管有助于控制数据泄露的风险，但是最根本的控制方法在于相关机构要做好内部的风险控制。例如，政务部门应当建立健全内部控制制度，对于易发生政务数据泄露的环节进行充分排查，强化网络数据安全全流程管理，及时整改消除重大数据泄露、滥用等安全隐患，明确规定部门岗位和人员的管理责任，加强政务数据管理的权限设置，形成相互监督、相互制约的管理机制。²⁸

同时，政务部门还应该完善政务数据安全管理制度设计，加快建立政务数据分类分级保护、政务数据安全风险评估、政务数据安全事件通报处置、政务数据对外提供使用报告等制度，完善信息安全技术防范措施，确保政务数据在采集、编制、储存、使用、共享、开放等环节不被泄露。

（二）规范外包机构的资质审批，避免数据泄露

根据上文可以看出，政府的数据经常委托第三方机构进行处理，甚至是承载数据的基础设施，例如政务云等都委托给外面的第三方进行处理，这其中数据泄露的风险不言而喻。因此，规范外包机构的资质审批就显得格外重要。

笔者认为规范外包机构的资质审批，首先应先界定外包机构参与招投标的门槛条件，即外包机构应进行许可进场，例如在名称上、营业场所、注册资本、业务范围和信用信息系统安全登记等诸多方面应满足一定条件，同时报送所在地的省级发改委审批；其次，应将外包机构的数据采集、使用等情况进行备案说明，发生数据的重大变化时还需做备案更新，要制作外包机构备案管理规则，规定备案主体等，以贯彻落实数据的保护。最后，要落实数据泄露第一责任人倒查制度，明确数据泄露时追究直接相关人责任，并应制定追究细则，提高处罚力度，以震慑分子的投机行为。

（三）制定政务数据的标准和政策，加强数据监管

如同上文所述，政务信息资源的共享存在不确定性法律概念，数据的第三方来源也没有专门的规范性文件，诸多情况导致政务数据的整合存在诸多模糊地带。通过立法模式消弭不确定性法律概念是解决问题的重要方式，然而如果各个问题都采用人大、人大常委会立法模式进行监督规范，将消耗巨大的司法成本。同时，立法耗时长，效率低，也难以及时处理实务中层出不穷的新问题。

因此，笔者建议，对于政务数据共享中的不确定性法律概念以及数据的第三方来源规范文件等，可以采用制定政务数据共享等领域的标准和政策的方式解决该问题。具体来说，由发改委、工信部和中央网信办等部门牵头，联合其他部门，共同研究、制订政务数据的标准和政策，也可以委托下属的事业单位或者相对应的技术部门研究制订。实际上，在政务数据整合的标准制定上，政府也意识到政务数据整合标准制定的重要性，要求“国家标准委会同共享平台管理单位，在已有政务信息资源相关标准基础上，建立完善政务信息资源的目录分类、采集、共享交换、平台对接、网络安全保障等方面的标准，形成完善的政务信息资源共享标准体系。”²⁹因此，对于政务数据整合，制定政务数据的标准和政策，加强数据监管不失为有效之举。

四、结 语

政务数据的整合涉及国家机密、个人信息等敏感信息，庞大的政务数据一旦出问题，对国家经济安全、社会公共利益均会产生极大的冲击和影响。因此，对于政务数据进行合规研究是必要之举。经过研究发现，政务信息资源目前存在来源不明，信息整理不规范、共享界定不清、开放设计过于粗糙等问题。解决政务数据整合问题的方法在于做好内部数据风控合规，规

²⁸ 参鉴《电信和互联网行业提升网络数据安全保护能力专项行动方案》等文件。

²⁹ 参见《政务信息资源共享管理暂行办法》第19条。

范外包机构的资质审批，制定政务数据的标准和政策。然而由于政务数据整合问题纷繁复杂，本文权属抛砖引玉，希望后期有更多实务界和理论界的专家学者能做更深入的研究。

参考文献:

- [1] 应验. 政府数据开放共享与共享社会建设：海南的举措和探索[J]. 电子政务, 2019, (198): 82-90.
- [2] 徐冠军. 试论政务大数据——政府回应改造现实性路径[J]. 北方经贸. 2019, (8): 3-6.
- [3] 铁金, 刘光昊, 刘苑, 冯鑫. 国内政务大数据研究热点分享[J]. 中国管理信息化. 2019, (22): 116-117.
- [4] 景亚萍. 贵州省政务数据治理探索与实践[J]. 软件与集成电路, 2019, (8): 72-73.
- [5] 彭 景, 郑玉波, 李思思. 构建政务数据开放共享体系[J]. 电信技术. 2019, (7): 85-88.
- [6] 周汉华. 个人信息保护前沿问题研究[M]. 北京：法律出版社，2008 年。
- [7] 周亚, 李东, 王翠. 对北京市政务大数据建设与发展的建议[J]. 中国工程咨询. 2019, (8): 65-68.