

4/25-26

XKungfoo 2018信息安全交流大会



《网络安全法》背景下的 大数据安全案例解读与风险控制


北京市京都律师事务所 翁小平



京都律师事务所
King & Capital Law Firm



目录



一

大数据管控的趋势分析

二

案例与风险研判

三

国外关于数据安全的一些立法趋势

四

大数据安全风险防控，律师能做什么？

一、大数据管控的趋势分析

在《网络安全法》颁布之后，国家对于大数据安全方面的治理政策已经十分明显。

目前是严管态势，很有可能是国家下一个严控领域。

【严管和严控的区别】

理由和依据一：

- 证券市场领域严控的数据分析（前车之鉴）

2015年之前，监管风险还只是停留在或有风险的阶段，被处罚的公司数量相对较少，金额也相对较小，受到刑事处罚的案例不多。

2016年，证监会共对183起案件作出处罚，作出行政处罚决定书218份，较2015年增长21%；罚没款共计42.83亿元，较2015年增长288%。对38人实施市场禁入，较2015年增长81%。

行政处罚决定数量、罚没款金额均创历史新高，市场禁入人数也达到历史峰值。

理由和依据一：

- 证券市场领域严控的数据分析（前车之鉴）

2017年，证券监管风暴更是狂飙突进。2017年6月，证监会已作出行政处罚决定65件，已作出的行政处罚罚没款合计超过61亿元，超过2016年全年水平。

2017年，全年被处罚金额在几千万元以上的比比皆是，超过亿元甚至十几亿元以上的也不少见。其中，徐某犯操纵证券市场罪一审被判5年6个月并处罚金110亿元。对P2P（多伦股份）实际控制人鲜某的罚没款约34.7亿元，创下当时证监会历年罚单最高纪录……

理由和依据一：

- 证券市场领域严控的数据分析（前车之鉴）

2018年3月14日，证监会组织召开稽查执法专场新闻发布会，对近期查处的三宗案件进行介绍。三宗案件中，有两宗是正在处罚程序当中的市场操纵案件。其中，“某集团涉嫌操纵市场案”因性质恶劣、涉案金额巨大，拟被开出合计约56.7亿元的史上最大罚单；“高某涉嫌操纵精华制药案”获利近9亿元，创出了操纵单只股票获利的历史之最。

理由和依据二：

- 《深化党和国家机构改革方案》：

中央全面深化改革领导小组、中央网络安全和信息化领导小组、中央财经领导小组、中央外事工作领导小组改为委员会。

优化中央网络安全和信息化委员会办公室职责。为维护国家网络空间安全和利益，将国家计算机网络与信息安全管理中心由工业和信息化部管理调整为由中央网络安全和信息化委员会办公室管理。

理由和依据三：

2016年4月19日，网络安全和信息化工作座谈会（3常委出席）

“要依法加强对大数据的管理。一些涉及国家利益、国家安全的数据，很多掌握在互联网企业手里，企业要保证这些数据安全。企业要重视数据安全。如果企业在数据保护和安全性上出了问题，对自己的信誉也会产生不利影响。”

“互联网核心技术是我们最大的‘命门’，核心技术受制于人是我们最大的隐患”

理由和依据三：

- 2018年4月20-21日，全国网络安全和信息化工作会议
(7常委全部到场)

“已形成网络强国战略思想”

“核心技术是国之重器” (核心技术包括大数据、人工智能)

“加强网络安全信息统筹机制、手段、平台建设”

理由和依据三：

2018年4月20-21日，全国网络安全和信息化工作会议

“加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然”

“要提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。”

理由和依据四：

- 美国网络安全分析机构Risk Based Security (RBS) 发布的《2017数据泄露报告》显示，2017年公开的数据泄露事件高达5207起，被泄露信息多达78.9亿条。
- 《2017数据泄露的成本》报告显示，在全球范围内，平均每条数据丢失为公司带来的损失为141美元。如果该行业运营着关键数据，损失会更高，比如教育行业数据丢失的成本高达每条246美元。

结论：

形势和趋势已经很明显了，不出意外的话，继金融和证券领域之后，互联网安全领域将会是下一个国家严厉打击和管控的领域。

所以，一定要有忧患意识！国家管控的大手早已经张开了！

二、案例与风险研判

数据安全其实就是保证用户的数据不损坏、不丢失，不会被偷走或者盗用。归纳起来就是数据获取、存储和流动的问题，也就是说数据的获取、保管和流动是不是经过授权？有没有符合要求的存储条件？所有环节是不是符合法律规定的？

案例一 “中国用户愿意用隐私换效率”

- 2012年全国人大常委会专门颁布的一个决定——《关于加强网络信息保护的決定》
- 《网络安全法》总共79个法条，去掉开头的总则和最后的附则，有实际意义的法条是61个，其中有多少处提到了公民个人信息？——共20处，涉及9个法条！

案例一 “中国用户愿意用隐私换效率”

- 这些已经充分说明了数据隐私问题的重要性，这也是我们技术和法律人员不得不面对的一个深层次问题，在大数据时代，技术的发展和隐私保护之间是一对很深的矛盾体。而且，随着法治意识的发展、权利意识的觉醒，个人隐私的问题只会越来越受到国家和社会的重视。
- 我们在处理数据相关技术的过程中，要控制法律上的风险，首先就是要有这个意识，要高度重视，对用户的个人隐私问题要做好保护。

案例二 某数据公司涉嫌侵犯公民个人信息案

- 《网络安全法》第七十六条：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。
- 《刑法》第二百五十三条之一：“违反国家有关规定，向他人出售或提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”
- 对关键隐私信息要进行必要的处理，数据可以加工，但应让别人“读不懂”。

案例二 某数据公司涉嫌侵犯公民个人信息案

- 《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》

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253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。

案例三 某公司流量变现涉嫌破坏计算机网络信息系统案

该案涉及两个关键问题：

- 一是安装插件用户是否知情：关乎是否具有用户授权。该案用户在主动安装关联软件时，会有选项提示“是否允许修改某浏览器的设置”等字样，系强制勾选（即选项框为灰色，不得拒绝）。
- 二是劫持，无法修改：就是做免杀。那么，就涉及免杀技术到底违不违法？

案例四 Facebook第三方App数据泄露事件（数据流转）

在美国选举门事件之前，脸书就已经因使用个人敏感信息推送广告在西班牙遭致行政处罚。2017年9月11日，西班牙数据保护监管部门AEPD宣布，脸书因收集西班牙用户的个人信息并将之用于发放广告被罚款120万欧元。AEPD认为脸书的隐私政策存在“一般性且不清晰的描述”，从而导致了三项具体违规：

- 首先，脸书收集了个人信息主体的政治观点和倾向、宗教信仰、性取向、个人兴趣等，但并未告知用户会将上述信息用于何种用途；
- 其次，脸书在收集、使用上述信息前，并未获得用户的知情同意；
- 再次，脸书在使用上述信息后，并没有及时删除上述信息。

案例四 Facebook第三方App数据泄露事件（数据流转）

该案也涉及两个关键问题：

- ◆ 一是用户同意的范围（数据获取和知情权）
- ◆ 二是对第三方的管理（也就是对数据流转的管理）

我国的《网络安全法》第四十条确立了数据流转“谁收集，谁管理”的原则。但是，现有的法律框架体系对于数据流转所涉及到的同意的明晰与必要、责任分配、利益保护等一系列问题基本无解，不是技术和流程层面无法实现，就是合规执行成本太高，只能关注于两头即事前的权利和隐私申明以及事后的审计调查追责，对中间数据流动缺乏实质有效的控制和监管手段。这需要理论与立法上都要重新认识数据属性和定义权利。

案例四 Facebook第三方App数据泄露事件（数据流转）

教训：

◆ 一是收集数据时应以必要为原则

数据收集的必要以及最少原则

◆ 二是使用信息之前需要获得用户同意

什么叫知情同意？明式同意还是暗式同意？同意到什么程度？

◆ 三是使用用户信息之后应及时删除

欧盟的相关条例里已有很多非常完善的规定，规定企业在使用用户的数据信息后有及时删除用户信息的义务。而脸书正是因为没有做到及时删除相关数据信息而遭到了行政处罚。

三、国外关于数据安全的一些立法趋势

1. 2018年2月6日，美国共和党和民主党两党议员联合在参议院和众议院提出《澄清域外合法使用数据法案》

核心问题：对数据的管辖是应采取“数据存储地原则”还是“数据控制者原则”。

《澄清域外合法使用数据法案》

- 对于危害美国国家安全的犯罪、严重的刑事犯罪等重大案件，可以根据该法案调取相关证据。通常而言，危害美国国家安全的犯罪、严重的刑事犯罪通常包括：恐怖主义犯罪、重大暴力犯罪、剥削儿童的犯罪、跨国组织犯罪以及金融欺诈犯罪。
- CLOUD 法案规定，无论服务提供者的通信、记录或其他信息是否存储在美国境内，只要相关通信内容、记录或其他信息为该服务提供者拥有、控制或者监管，均应当按照法令要求，保存、备份、披露。

我国的现状与应对

我国目前对于数据出境管控与跨境数据协助的已经生效的法律法规只有《网络安全法》（关键数据不准出境）、《征信业管理条例》、《人口健康信息管理办法（试行）》、《网络出版服务管理规定》、《网络预约出租汽车经营服务管理暂行办法》、《地图管理条例》等有限几部。对于境外政府、组织调取我国境内存储数据的规则短缺，境内组织、个人在面临境外调取数据资料的指令时，缺少法律法规的明确保护。

我国的现状与应对

- 比如苹果，根据我国现行政策法规的规定，“云上贵州”是icloud数据的实际存储方，但由于苹果公司是数据的收集方与实际管理人，苹果公司也被视为数据的共同控制者。即：即使“云上贵州”不受Cloud法案的管辖，但苹果公司仍不可避免地受到该法案的制约。

欧盟对Cloud法案的回应

- 4月17日，欧盟宣布将会出台一个对该美国法案的立法，提出了一些要求：

首先，如果面向欧盟提供服务，服务提供者应当在欧盟境内设立法定代表，以接收调取证据的法令。但欧盟强调，这个要求并不会强制要求服务提供者对数据存储地的选择。

其次，如果证据调查令指向的是存储在欧盟境外的数据，则在满足两个条件的情况下，服务提供者应当向发出命令的欧盟成员国提供：1) 发出调取证据命令的司法机关对刑事侦查具有管辖权限；2) 服务提供者确实向欧盟居民提供服务（无论是否在欧盟境内设立了分支机构）。

如果导致了法律冲突怎么办？例如我国的网安法不允许服务提供者对外提供某些数据？欧盟指出，在立法中会考虑这样的情况，但最终决定是否应该提供证据的还应该是欧盟成员国的法院。

2. 欧盟《一般数据保护条例》的希腊草案

- 关于数据保护官（DPO）的规定：

除了《一般数据保护条例》第37条第1款中规定的几种必须选任数据保护官员的情形外，当控制者和处理者基于希腊数据保护机构的指示开展活动需进行系统的大规模数据主体监控时也应当选任数据保护官。数据保护官的选任、地位和义务均以书面形式明文规定。数据保护官受法律中保密义务的约束，不得向任何第三方透露其履行职能的内容。

2. 欧盟《一般数据保护条例》的希腊草案

- 关于数据主体“知情同意”的规定：

根据数据主体的同意进行的处理应当基于明确的法律规定，并且控制者应当能够证明数据主体做出的处理同意或者要求。在做出同意表示之前，数据主体应当被告知数据处理的目的；被处理数据的类型，尤其是所涉及的特殊类别的个人数据；控制者；处理的时间期限；接收者；是否同意的法律后果以及数据主体的撤回权等等。数据主体必须以书面形式作出同意表示，且所做的同意表示必须清晰、明确。数据主体有权随时撤回其同意，同意的撤回不影响在撤回之前基于同意作出的合法的数据处理。当数据主体以书面形式作出的同意声明涉及其他事项时，那么所做的同意表示应当以能与其他事项显著区别的方式作出。当涉及特殊类别的个人数据处理，同意表示中应当明确提及。



四、风险防控，律师能做什么？

我们踩在一个周期更替的节点上，踩在重大变化的关键点上，看清方向、把控风险比什么都重要，它关系着是上天堂还是下地狱。

律师在信息安全合规、风险控制方面的作用一

- 告诉你方向在哪里！
- 风险在哪里！
- 法律的边界在哪里！

律师在信息安全合规、风险控制方面的作用二

- 告诉你什么是违法，什么是犯罪！
- 提醒你哪些雷不能踩！
- 哪些路可以走！



京都律师事务所
King & Capital Law Firm



Thank You!