滴滴数据安全事件启示录

作者：杨迅 | 夏雨薇 | 胡慧雯

日前，滴滴全球股份有限公司(以下简称“**滴滴公司**”)有关网络安全审查的处罚结果尘埃落定，一时间沸沸扬扬，企业如何做好网络安全合规等议题再引热议。自国家互联网信息办公室（下称“**网信办**”）于 2021 年 7 月 2 日对滴滴公司启动网络安全审查，随后同月 4 日和 9 日连续发布两篇通报宣布滴滴系 App 存在违法违规行为并要求应用商店予以下架，再到一年后宣布对滴滴公司处以 80.26 亿的巨额罚款，滴滴公司网络安全审查充满了戏剧性。

本文将分析网络安全审查对滴滴公司的“次生”影响，进一步阐述该事件对各行业个人信息处理者的启示；并将重点介绍网络安全审查后滴滴公司可能面临的民事、公益诉讼，以及企业如何借鉴以有效进行事前预防与事后补救。

目 录

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

1. 中美法规冲突下的赴美上市

回顾事件发展: 2021 年 6 月 30 日，滴滴公司在美国纽交所挂牌。2021 年 7 月 2 日，网信办对滴滴公司启动网络安全审查。2022 年 6 月 2 日，滴滴公司申请纽交所退市; 2022 年 7 月 21 日，因违反《网络安全法》《数据安全法》《个人信息保护法》(下称"**相关法律**")的相关规定，损害社会公众利益，危害国家安全等，滴滴公司被网信办处人民币 80.26 亿元罚款，滴滴公司董事长兼 CEO 程维、总裁柳青被各处人民币 100 万元罚款(下称"**滴滴数据安全事件**")。

滴滴数据安全事件发生和发展于我国数据安全和个人信息保护领域立法迅速发展的一年。：在这一年里，数据安全与出境等领域开始构建系统性监管体系:《数据安全法》于 2020 年 7 月发布草案，于 2021 年 6 月 10 日正式发布；《个人信息保护法》于 2020 年 10 月发布草案，于 2021 年 8 月正式发布；大量配套法规同期出台。

与此同时，美国却于 2020 年 12 月 18 日颁布《外国公司问责法案》(Holding Foreign Companies Accountable Act)，要求在美上市公司使用经美国公众公司会计监督委员会("PCAOB")审查的审计机构，否则将可能强制其摘牌。而审计会涉及大量企业重要信息，内容丰富，甚至可能涉及国家安全。《外国公司问责法案》明显增加了赴美上市企业违反国内数据安全相关规定的风险。

滴滴公司因其庞大的出行业务，持有大量个人信息及涉及国家安全的信息。在这样的背景下，滴滴公司的赴美上市必然引发网信办对其数据和个人信息保护状况的担忧。，因此，在滴滴公司挂牌上市后，网信办几乎**立即**对滴滴公司启动网络安全审查，也是情理之中。

似乎是受滴滴数据安全事件的启示，同样掌握大量数据的阿里集团在 2022 年 7 月 26 日宣布于纽交所和港交所两地双重主要上市，随后阿里集团宣布其与蚂蚁集团同意终止《数据共享协议》，这可能是在上述监管大背景下的有效合规应对。

2. 巨额处罚后的"次生"影响

滴滴数据安全事件真的能以巨额罚款终结吗?至少在理论上，巨额罚款的影响不止是金钱的损失，还有可能给滴滴公司带来更深远的不利影响。

2.1 用户流失和市场份额下降

网约车市场竞争激烈。滴滴出行 App 自 2021 年 7 月至今仍处于下架状态，不但影响其获取新用户，还阻碍其巩固市场份额。经公开检索，滴滴出行 App 下架后，曹操出行、T3 出行、哈啰出行先后宣布完成了 38 亿元、77 亿元、2.8 亿美元的融资。

2.2 侵权诉讼风险

网信办对滴滴公司违反个人信息保护的行政处罚决定，可能为后续的民事诉讼大开方便之门。

根据《民法典》第一百一十一条，自然人的个人信息受法律保护。根据《个人信息保护法》第六十九条，侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。然而，如互联网企业侵犯自然人的个人信息权益，其侵权行为往往较为隐蔽，自然人难以查明，侵权损失难以确定，阻碍了自然人维护自己的合法权益。

然而，，行政处罚文书记载事项可被推定为真实，降低了侵权证据收集难度，用户可能据此起诉。《民事诉讼法解释》第一百一十四条规定，国家机关或者其他依法具有社会管理职能的组织，在其职权范围内制作的文书所记载的事项**推定为真实**，但有相反证据足以推翻的除外。必要时，人民法院可以要求制作文书的机关或者组织对文书的真实性予以说明。

本次事件中，网信办在其对滴滴公司依法作出网络安全审查相关行政处罚的决定中明确滴滴公司存在侵犯个人信息的行为，并在相关答记者问中更为细致地明确列举了滴滴公司存在的违法违规行为。相关处罚和说明将降低用户侵权证据收集难度，为其起诉提供便利。

2.3 公益诉讼风险

与普通民事诉讼类似地，有关部门也可能向滴滴公司提起公益诉讼。

《民事诉讼法》第五十八条、《消费者权益保护法》第四十七条均规定了公益诉讼，《个人信息保护法》第七十条[1]进一步明确人民检察院以及法律规定的组织可就侵害众多个人权益的个人信息处理者提起公益诉讼。此外，最高人民检察院曾于 2021 年 4 月发布《检察机关个人信息保护公益诉讼典型案例》[2]，于 2021 年 8 月下发《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》[3]，体现其规范相关公益诉讼案件办理，多维度保护自然人的合法权益的工作目标。

因此，继滴滴数据安全事件之后，相关人民检察院等有理由，也有空间进一步提起公益诉讼。

3. 滴滴数据安全事件的启示

滴滴数据安全事件体现出网信办大大增强了数据保护意识，这应当引起企业合规人员的高度重视。它也给数据安全和个人信息保护工作带来珍贵的启示。

3.1. 从滴滴数据安全事件探析个人信息保护的实践要求

《国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问》[4] (“**《网信办答记者问》**”)简要列举了八条滴滴公司违法违规收集使用

[1] 《个人信息保护法》第七十条，个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。
[2] 最高检发布检察机关个人信息保护公益诉讼典型案例_中华人民共和国最高人民检察院 (spp.gov.cn)
[3] 最高检下发通知 明确个人信息保护公益诉讼办案重点_中华人民共和国最高人民检察院 (spp.gov.cn)
[4] 国家互联网信息办公室有关负责人就对滴滴公司全球股份有限公司依法作出网络安全审查相关行政处罚的决定答

个人信息的行为，有助于广大个人信息处理者进行合规差异分析。首先，《网信办答记者问》一文中可见近年来工信部、网信办常年执法行动中的重点监管行为，如“未经用户同意收集用户的个人信息”、“向用户索取与当前业务场景无关的权限”、“未能明确说明收集使用个人信息的目的、方式和范围”、“收集个人信息的频度超出业务功能实际需要”等典型的违法违规行为。个人信息处理者需继续对这些“高危”行为进行把控，远离监管红线。

同时，《网信办答记者问》所列举的违法违规行为中也不乏有一些新鲜亮点值得企业持续关注。如滴滴公司被网信办处罚过度收集“用户剪切板信息”、“应用列表信息”以及“明文存储敏感个人信息”等行为。考虑到 App 开发者在对 App 进行设计开发时，普遍会为提高用户体验而特意设置一些快捷、跳转等功能，剪切板信息与应用列表信息(主要存在于 Android 系统)均为设备运行时较为常见的收集信息；此外，企业内部的数据安全管理、流转以及技术安全措施，也容易因其对内的性质而较容易被忽略。对于前述问题，企业需要开始重视内部的数据、个人信息管理制度和操作规程，特别是对于存储的用户个人信息应采取相应的安全措施，如加密存储、分类管理、去标识化处理等。虽目前网信办尚未公布具体的罚则依据，但是企业如已经存在相关收集行为，或内部数据安全管理体系有待完善的，也建议趁早排查整改。

3.2. 明确国家维护公共利益的长期需求

与 GDPR 不同，我国的数据安全和个人信息保护更加重视国家安全和公共利益。从滴滴数据安全事件来看，政府不单关注企业发挥数据、个人信息权益的积极效益时对个人权益的平衡保护，更是前瞻性地看到了个人信息与数据的流通对国家安全，社会公共利益带来的影响。

此次滴滴数据安全事件，网信办的判罚理由不但囊括了滴滴公司对个人权益的损害，还考虑到了滴滴公司对国家安全，公共利益的严重影响，特别是对“国家关键信息基础设施安全和数据安全带来的严重安全风险隐患”。《网信办答记者问》也提到，下一步网络执法中，将“切实维护国家网络安全、数据安全和社会公共利益。”也就是说，互联网企业在处理个人信息与数据时，除进行一般对组织权益、个人权益等私人主体的权益影响评估外，也应当重点关注当前数据、个人信息的处理活动对**国家安全、公共利益**的影响程度。

3.3. 违法情节严重时或将面临顶格处罚

我国《网络安全法》《数据安全法》在对法律责任的立法中皆划定了企业罚款的具体上限，《网络安全法》的罚款上限是 100 万，《数据安全法》中的罚款上限则是 1000 万。《个人信息保护法》则采取了另一种立法模式，罚款额度最高可达“企业上一年度营业额百分之五以下罚款”，这也为监管机构根据企业违法情况的严重性与可责性决定罚款数额提供了合法基础。

记者问-中共中央网络安全和信息化委员会办公室 (cac.gov.cn)

根据笔者推测，此次判罚的主要依据可能是《个人信息保护法》第六十六条第二款[5]，即上文所述的违法企业的罚款金额最高可至五千万元或企业上一年度营业额 5%。我们根据滴滴公司发布的 2021 年财报[6]获悉，其全年营收达 1738.27 亿元，其中中国出行业务营收为 1605.2 亿元。滴滴公司的中国出行业务营收的 5%即为 80.26 亿人民币。

3.4. 执法依然看重企业主观态度

如我们的猜测属实，滴滴公司本次所适用的正好是上一年度营业额的 5%这一顶格处罚标准，也从侧面证明滴滴公司本次的违法行为情节严重，结合《网信办答记者问》中网信办强调滴滴公司拒不配合整改、阳奉阴违，恶意逃避监管，极有可能不存在行政处罚法上应当从轻或减轻行政处罚的事由。根据《行政处罚法》第三十二条的规定，应当从轻或者减轻行政处罚的事由包括:

- 主动消除或者减轻违法行为危害后果的;
- 受他人胁迫或者诱骗实施违法行为的;
- 主动供述行政机关尚未掌握的违法行为的;
- 配合行政机关查处违法行为有立功表现的;
- 法律、法规、规章规定其他应当从轻或者减轻行政处罚的。

我们建议，对企业而言，除应对违反个人信息保护法律的处罚责任后果有清晰的认识外，更需要意识到主观上配合执法，限期整改，积极应对监管的必要性。从目前网信办、工信部对侵害用户权益所采取的多批执法行动中，我们不难窥见监管机构“配合从宽”的执法作风。一般而言，针对 App 的违法违规行为，监管机构在首次发现问题后将给予企业一定的整改时间，进而对不符合整改要求的企业进行通报，通报后仍逾期不整改或不符合整改要求的 App，将面临下架或其他的处罚措施。

3.5. 了解相关法律下的双罚制责任

本次处罚决定，不但针对滴滴公司，还对滴滴公司的董事长与总裁各处 100 万元罚款。目前，我国网络安全、数据安全、个人信息保护领域皆体现了“双罚制”的处罚模式，除一般的责任主体外，企业直接负责的主管人员和其他直接责任人员也应当就相关法律下的违法行为承担责任。在《网络安全法》下，直接负责的主管人员和其他直接责任人员的罚款范围从 5000 元 - 100 万元不等；在《数据安全法》下，直接负责的主管人员和其他直接责任人员的罚款范围从 1 万元- 100 万元不等；在《个人信息保护法》下，直接负责的主管人员和其他直接责任人员的罚款范围从 1 万元 - 100 万元不等。虽目前网信办亦没有披露具体的罚则细节，但滴滴公司的董事长与总裁所承担的个人责任，也已经属于相关法律违法行为**“情节严重”**的条件下的顶格处罚。

[5] 《个人信息保护法》第六十六条第二款 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

[6] DiDi Global - Financials - Annual Reports (第 116 页)

鉴于越来越多的企业已经开始构建企业内部的数据治理体系，不可避免需要建立(或指派)信息安全保护工作相关部门并任命相关部门负责人，对于具体负责企业网络安全、数据安全与个人信息建设工作的部门和部门负责人而言，一旦企业存在相关法律下的违法行为的，个人也难以免除并罚的责任。除考虑基于《行政处罚法》减轻或从轻处罚的情形外，负责部门与部门负责人也可以参考《网信办答记者问》给出的对"情节严重"的考虑因素，尽可能预防，或缓解违法行为可能给企业与个人带来的损失。

《网信办答记者问》中对"情节严重"的考虑因素:

1) 违法行为的性质：是否按期配合整改;
2) 违法行为的时间：是否存在长期的、持续性的违法行为;
3) 违法行为的危害：对用户隐私、个人信息权益的侵犯严重程度;
4) 违法行为的数量：违法处理的个人信息条数;
5) 违法行为的范围：违法行为所涉及的移动端应用数量。

同时，负责人也需要格外注意相关法律下的违法行为亦可能上升至违反治安管理的层面，甚至构成犯罪。目前《刑法》第二百五十三条[7]、《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》，对侵犯公民个人信息罪、以及非法获取、出售或者提供公民个人信息"情节严重"与"情节特别严重"进行了列举示例[8]，并且，侵犯公民个人信息罪也属于"双罚制"。

在网络安全，数据安全与个人信息保护的双罚制要求下，企业的决策者无法独善其身，无论从企业或是从个人可能面临的行政乃至刑事责任层面考虑，企业的首要目标都是建立并完善内部的数据治理体系，积极面对并响应监管的执法行动与整改意见，尽可能减少处理数据与个人信息对用户权益，组织权益，乃至社会公共利益与国家安全带来的负面影响。

[7] 第二百五十三条 之一【侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，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。
违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。
窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。
单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

[8] 第五条 非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的"情节严重": (一)出售或者提供行踪轨迹信息，被他人用于犯罪的; (二)知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的; (三)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; (四)非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的; (五)非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的; (六)数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的; (七)违法所得五千元以上的; (八)将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的; (九)曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的; (十)其他情节严重的情形。
实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的"情节特别严重": (一)造成被害人死亡、重伤、精神失常或者被绑架等严重后果的; (二)造成重大经济损失或者恶劣社会影响的; (三)数量或者数额达到前款第三项至第八项规定标准十倍以上的; (四)其他情节特别严重的情形。
第六条 为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的"情节严重": (一)利用非法购买、收受的公民个人信息获利五万元以上的; (二)曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的; (三)其他情节严重的情形。实施前款规定的行为，将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准适用本解释第五条的规定。

如您希望就相关问题进一步交流，请联系:

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: **master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野