论网络平台数据安全的合规治理

——以网约车平台个人信息安全为对象*

马明亮**　舒　鑫***

摘要：聚集着海量个人信息的网约车平台，在运营中存在着个人信息被泄露、滥用的风险。网约车平台个人信息安全的既有保护模式，在实践中呈现出不能有效预防安全风险、不能及时识别安全危机、不能积极应对安全事件等缺陷。为有效防范与应对数据安全事件，平衡数据的流通价值与安全价值，保障平台营利的可持续性，一种具备激励性、实时性，能够有效衔接平台内外监管功能的日常性数据安全合规治理体系呼之欲出。该体系是由制度架构与信息技术组成的闭环系统。在制度设计层面，包括数据安全风险评估制度、数据安全合规组织架构、内部数据安全管理制度、数据安全合规定期培训以及数据安全审计制度。在信息技术层面，差分隐私技术、知识图谱技术、区块链技术等新兴技术的引入发挥着预防个人信息安全风险、减轻合规治理负担、助力数据安全管理合规的功能，提升了数据安全合规治理能力。该闭环系统运行的科学性决定着合规计划的有效性，有利于逐步实现数据安全合规的自动化。

关键词：平台治理；网约车平台；个人信息安全；政府监管；数据安全合规

一、问题的提出

与之前的互联网时代相比，大数据时代是数据被广泛获取和使用的时

* 本文系中国人民公安大学课题“中国智慧出行安全治理体系研究”的阶段性成果。

** 马明亮，中国人民公安大学教授，博士生导师。

*** 舒鑫，中国人民公安大学博士研究生。

代，是凸显数据价值的时代，同时也是注重数据危机控制、保障数据安全的时代。互联网与数据采集传感器的日益普及促使数据量呈井喷式增长，云计算、人工智能、大数据等数据处理技术的革新更是进一步释放了数据的潜在价值，一场数字革命悄然兴起。数据被誉为“本世纪最珍贵的财产”“新一轮技术革命和社会变革的核心动力”，以容量大、复制成本低、传播迅速等特点，驱动着数字经济快速发展。这一新兴生产要素完成了从资源到资产再到资本的蜕变，数据资本、数据分析技术已然成为塑造网络平台“分析型市场竞争力”的战略制高点之一。相比较传统意义上的“马后炮”式商业智能模式[1]，拥有着复杂的交互依赖性的大数据技术助力“平台 3.0”[2]时代的到来，往往能够帮平台实现“未雨绸缪”的商业效果。但所谓“水能载舟，亦能覆舟”，也正如乌尔里希·贝克的《风险社会》中“自反性现代化”的理论所指，“数字社会主义”[3]在给平台企业带来利好的同时，随之而来的便是数据泄露，被滥用、误用等数据安全事件的发生。华住及万豪等酒店集团反复出现顾客信息泄露[4]、微博 5.38 亿用户数据在暗网出售[5]、大量 App 涉嫌权限越界过度收集用户信息[6]等数据安全事件的出现，表现了数据批量

[1] 商业智能指的是通过“从上至下”的组织流程管理，从资讯中得出有用信息。参见[德]罗纳德·巴赫曼等：《大数据时代下半场：数据治理、驱动与变现》，刘志则、刘源译，北京联合出版公司 2017 年版，第 67 页。

[2] “信息化 3.0”指的是“以数据的深度挖掘和融合应用为主要特征的智能化阶段”，这里的“平台 3.0”指的是在新信息技术推动下，商业智能模式向智能商业模式的转变。参见梅宏主编：《数据治理之论》，中国人民大学出版社 2020 年版，第 4 页。

[3] “数字社会主义”指的是“借助网络通信技术运行在没有边界的互联网上，催生了贯穿全球一体化经济的无形服务”，这里用来描述数据因信息技术的发展，从私人资源逐渐转变为网络共享资源的现象。参见[美]凯文·凯利：《必然》，周峰、董理、金阳译，电子工业出版社 2016 年版，第 155 页。

[4] 早在 2018 年 11 月万豪国际就宣布黑客入侵了喜达屋部门的预定数据库，造成 3.83 亿客人信息泄露；2020 年 4 月万豪国际再次发生信息泄露事件，大约 520 万客户信息被泄露。参见《万豪酒店再现信息泄漏　涉及 520 万客户》，http://xiaofei.people.com.cn/n1/2020/0402/c425315-31658267.html，最后访问日期：2021 年 12 月 20 日。

[5] 《传微博 5.38 亿用户数据在暗网出售》，https://www.sohu.com/a/381870733_120622013，最后访问日期：2021 年 12 月 20 日。

[6] 100 款 App 中，“位置信息”“通讯录信息”“身份信息”“手机号码”是用户个人信息过度收集或使用较多的内容，在受测评中分别有 59 款、28 款、23 款、22 款 App 涉嫌存在此类情况。参见《中消协发布 100 款 App 隐私政策测评》，http://finance.people.com.cn/n1/2018/1204/c1004-30442062.html，最后访问日期：2021 年 12 月 20 日。

聚集于平台的风险性。大数据技术的迅速发展与管控手段的保守滞后，会带来“技术先占”[1]等一系列数据安全隐患；网络平台私有性和公共性之间存在的张力，加剧了其在数据处理流程中失范风险的外溢可能，[2]数据安全事件呈影响逐步扩大、危害程度日益严重的态势。

我国网络安全立法在近年高歌猛进，形成了以《网络安全法》、《数据安全法》和《个人信息保护法》“三驾马车”为基础的网络空间监管法律框架，完成了从技术安全、内容安全到数据安全新维度的拓展。2022年快节奏的立法步伐仍不停息，《网络安全审查办法》等行政法规的相继出台以及《上海市数据条例》《福建省大数据发展条例》《山东省大数据发展促进条例》等地方性法规的陆续颁布，无不突出了数据安全治理的重要地位。可以预见，平台将会面临前所未有的数据安全治理和数据安全合规压力。为实现对平台更为实质性的治理型监管[3]，打破政府部门之间、政府部门与平台之间的“数据孤岛”，保证平台营利的可持续性，保障数据主体的权利不受侵害，一种具备激励性、实时性，能够有效衔接平台内外监管的数据安全合规治理体系呼之欲出。

目前学界关注于数据合规，数据安全只作为数据合规治理的组成部分被提出，单独针对数据安全的合规治理体系的研究较少。此外，学界对于数据安全的研究主要建立在数据安全与个人信息保护二分的视角，[4]以此排除了数据安全相关立法对个人信息安全的合规指引作用。而且，学界对于

[1] “技术先占”现象是指，在规范空缺的场域进行自我赋权，倒逼政府“承认”和进行制度变革，网约车的合法化就是一个典型。参见马长山：《智慧社会建设中的“众创”式制度变革》，《中国社会科学》2019年第4期。

[2] 参见陈荣昌：《网络平台数据治理的正当性、困境及路径》，《宁夏社会科学》2021年第1期。

[3] 区别于西方国家互联网企业面临的形式化监管，我国法律对互联网企业施加了更多的实质性监管，背后原因在于我国在“平台中立性”上所持态度具有特殊性，即更加重视平台的公共性功能。所以相比较西方互联网平台的“自由发展”，在我国的网络平台需受到较为严格的政府管控。参见丁晓东：《网络中立与平台中立——中立性视野下的网络架构与平台责任》，《法制与社会发展》2021年第4期。

[4] 如有学者明确指出，《数据安全法》第53条厘清了数据与个人信息的界限，将涉及个人信息的数据活动交由《民法典》、《网络安全法》和《个人信息保护法》等法律法规加以规范。参见刘新宇主编：《数据保护：合规指引与规则解析》，中国法制出版社2021年版，第97页。

网络平台合规路径的研究，多为“合规整改模式”[1]的视角，目前针对网络平台日常性合规治理的研究还不充分。事实上，首先与数据合规治理相比，数据安全合规治理至少存在由安全合规部门发起、以安全价值优先、以访问控制与数据分级分类保护为主要合规工作内容等独特之处；并逐渐从传统的从属、依附的地位中脱离出来，被赋予了在数字化社会中的重要地位。其次，个人信息与数据的界限逐渐模糊，个人信息更是作为需要“被特殊保护的数据”被提出，数据安全与个人信息竞合保护的理念在数据安全合规实践中日益普及。最后，将数据安全问题赋能于平台“日常性合规管理”体系的构建，搭建贯穿平台运营全环节的风险预防、危机识别、事故应对机制，有利于在运营合规、风险可控的前提下，实现数据价值开发的最大化。鉴于此，本文以网约车平台的个人信息安全为研究范例，通过梳理网约车平台数据处理过程中存在的个人信息安全风险点，厘清现有保护机制中存在的局限，在此基础上结合新出台的数据安全、个人信息保护相关的法律法规、行业标准，从制度框架、信息技术两方面提出对网络平台数据安全合规治理体系的具体建构建议。

二、个人信息安全的重灾区

网约车平台指的是依托北斗应用、交通信息处理等互联网信息技术，使构成预约出租车服务供需关系的双边或多边主体，在特定载体提供的规则下交互，以此营利的企业法人。用户注册、平台审核、订单匹配、行程服务、支付收款、用户评价等服务的进行，会导致用户个人信息的大量聚集与交互，网约车平台在此过程中承担个人信息安全保护的主体责任。大数据时代的到来推动了平台企业对于个人隐私保护的管理变革，即从以“个人信息控制理论”为基础的个人许可制，到以“社会控制理论”为基础，让数据使用者承担责任，[2]网约车平台须承当相应的数据使用责任。实践中，以营利性优先的网约车平台对个人信息数据的利用往往超出了其安全管控的限

[1] “合规整改模式”指的是当企业涉嫌违规违法行为，面临行政处罚、刑事追诉或资格制裁，所作出的合规整改行为。参见陈瑞华：《有效合规管理的两种模式》，《法制与社会发展》2022年第1期。

[2] 参见高富平：《个人信息保护：从个人控制到社会控制》，《法学研究》2018年第3期。

度，导致个人信息安全风险频发，表面上来看，与制度机制、人才队伍、技术体系的滞后相关，究其根源是在于尚未形成一种科学系统的数据治理秩序，以保障数据资源有序、高效的开发利用。[1]

（一）网约车平台个人信息安全状态的规范性要求

网约车平台对个人信息安全的保护，目的在于避免收集、利用个人信息阶段，出现非法收集、滥用、泄露等安全事件。这就要求网约车平台采取必要的技术和管理措施，规范自身作为个人信息控制者的信息处理行为。为实现此目的，网约车平台需充分满足个人信息数据的有效保护、合法利用安全状态，并建立维持上述安全状态的制度。[2]

首先，应厘清个人信息安全的客体是解读网约车平台个人信息安全规范性要求。传统上，个人信息安全的客体立足于个人信息内涵界定的相关学说之上（“关联说”“隐私权说”“识别说”），依靠“同意与授权”的公式化系统，保障数据主体个人信息自决权的行使。但随着“大数据现象”深度融入人们的日常生活中，个人信息与非个人信息之间的界限逐渐模糊（在非个人信息的批量聚集下，也可达到识别个人的目的）；数据二级用途价值的凸显架空了“告知与许可”规则；[3]此外，出于个人信息安全防控的角度，安全风险出现的原因在于“如何收集、使用个人信息”而非“是否构成个人信息”，进行动态意义上的个人信息安全保护成为主流，数据使用者的主体责任地位凸显。有学者进一步提出应该淡化个人信息的静态定义，弱化个人信息与非个人信息在前端收集阶段的区分，强化对个人信息使用环节的关注，评估个人信息具体应用场景中的风险。[4] 至此个人信息安全的客体指的是个

[1] 参见梅宏主编：《数据治理之论》，中国人民大学出版社2020年版，第3页。

[2] 《信息安全技术 网络预约汽车服务数据安全指南》（征求意见稿）5.5将网约车服务数据分为四个类别，即个人信息、车辆行驶数据、统计数据和匿名化数据；《汽车数据安全管理若干规定（试行）》第3条将汽车数据分为个人信息数据与重要数据，个人信息安全是网约车数据安全的重要组成部分，也应当符合《数据安全法》第3条规定的数据安全状态标准。

[3] 因为数据的价值很大一部分体现在二级用途上，而收集数据时并未作这种考虑，所以“告知许可”就不能再起到好的作用了。参见[英]迈尔-舍恩伯格、[英]库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社2020版，第220页。

[4] 参见范为：《大数据时代个人信息保护的路径重构》，《环球法律评论》2016年第5期。

人信息数据的全生存周期。[1]

其次，个人信息安全状态中的有效保护，指的是保护已储存的、正在处理或传输的个人信息及依托该数据提供的网约车服务，不被恶意行为及非预期行为破坏，以保证网约车平台个人信息数据的完整性、可用性、机密性及非否认性，其内容具体如下：第一是个人信息数据的完整性，其要求确保用户注册账号时的基本信息、定位信息、支付信息、行程轨迹、常用地址等字段内容齐全完整，未发生遗漏或被非法修改、删除、增加。第二是个人信息数据的可用性，即个人信息数据的可访问性及依托个人信息进行的服务能够正常运行。第三是个人信息数据的机密性，要求确保一般或敏感个人信息的传输、存储或处理等不遭受未授权的浏览。第四是个人信息数据的非否认性，其所注重的是个人信息处理的痕迹管理，在过程记录下保证数据处理者不能否认其行为及处理结果，目的在于在出现个人信息安全事故时，追究数据责任人的过失责任，同时追踪进行数据恶意攻击的责任人。

再次，网约车平台应当保障对个人信息的合法利用，[2]一方面要求网约车平台依法进行个人信息的收集、存储，个人信息的展示，用户画像的使用，驾驶员信用记录的使用，紧急情况个人信息共享，平台订单数据共享，第三方地图数据共享，第三方平台数据共享，违法违规信息的公开披露，并针对行程录音录像等敏感个人信息进行重点保护；另一方面禁止违反法律法规的禁止性、义务性规范滥用、误用个人信息。

最后，安全状态的维持机制讲究通过内部流程、平台策略、安全标准以及组织建设的有效组合，实现对平台的信息建设进行全方位的监管，规范个人信息收集、存储、使用、加工、传输、提供、公开等工作；要求管理层、业务部门、技术部门的密切协作，评估个人信息安全风险等级，妥善应对个人信息安全合规风险事件，及时根据监控反馈评价进行修正，配合进行违规问题调查并及时整改。

---

[1] 根据国标《信息安全技术　个人信息安全规范》(GB/T 35273—2020)，数据全生存周期包括："收集，存储，使用以及委托处理、共享、转让、公开披露环节。"

[2] 合法利用应该满足《个人信息保护法》第5条规定的"合法、正当、必要和诚信，不得通过误导、欺诈、胁迫等方式处理个人信息"。

(二)网约车平台个人信息安全的风险

1.数据采集阶段:过度采集个人信息或索取系统权限

针对App过度采集个人信息行为[1]的专项治理已开展近三年,成效显著,以通报违规App名单、对逾期不整改的App予以下架处理、"净网行动"等方式,对未公开收集个人信息规则、强制授权、过度索权等行为进行了大范围、大力度的"清理"[2]。在网约车行业,2020年工信部通报了包括T3出行、长安出行以及蜜蜂出行在内的131家存在侵害用户权益行为App企业的名单。[3] 又如2021年滴滴出行因其App存在严重违法违规收集使用个人信息而被限制市场资格。[4] 但出于违法成本低、监管能力有限等原因,个人信息数据仍然存在被网约车平台过度采集或索取系统权限的风险,其背后是第三方共享、社交媒体、广告推广等经济价值的驱动。实践中,网约车平台包括但不限于以下过度采集个人信息数据的典型行为:第一,在提供隐私政策时设置"默认勾选"的同意选项,在未以显著方式提示用户的情况下采集通讯录、地理位置等个人信息数据,甚至是在第三方保存的信息,严重损害了用户自主选择是否授权的权利。第二,在采集个人信息时未实质履行告知义务,如以曹操出行为例,在其App中难以找到隐私政策的查阅界面。第三,网约车App在申请索取、访问收集内存、位置、相机等个人信息的权限时,并未告知用户其收集用途以及收集范围,使得用户无法根据业务需求来确定自己是否同意授权,剥夺了信息主体对于自身信息用途的预期。第四,以"捆绑授权"的方式获得用户对个人信息的概括授权,规避

[1] 依据《App违法违规收集使用个人信息行为认定方法》第3条、第4条规定,过度采集指的是"未经用户同意收集使用个人信息"和"违反必要原则,收集与其提供的服务无关的个人信息"的个人信息收集行为。

[2] 参见刘新宇主编:《数据保护:合规指引与规则解析》,中国法制出版社2021年版,第28页。

[3] 其中T3出行App因"违规收集个人信息,App强制、频繁、过度索取个人权限",被工信部两次点名要求整改。参见《T3出行悄然重新上架!因违规收集个人信息被工信部两次点名》,https://www.sohu.com/a/432712630_161795,最后访问日期:2021年12月25日。

[4] "滴滴出行"App存在严重违法违规收集使用个人信息问题。国家互联网信息办公室依据相关规定,通知应用商店下架"滴滴出行"App。参见《关于下架"滴滴出行"App的通报》,《中共中央网络安全和信息化委员会办公室官网》http://www.cac.gov.cn/2021-07/04/c_1627016782176163.htm,最后访问日期:2021年12月25日。

收集必要性原则。收集必要性原则要求网约车平台应当收集的个人数据属于能够实现其服务功能的最少数据，[1]但实践中网约车平台收集的个人信息数据远远大于上述必要数据的范围，除用户主动披露的个人信息数据、用户在使用服务过程中产生的数据之外，网约车平台收集的个人信息数据还来源于平台内的其他不相关业务。以滴滴出行为例，据其《个人信息保护及隐私政策》2.1，其核心业务不仅局限于出租车、顺风车、代驾等交通出行业务，还包括外卖、金融等非乘客运输业务，不同业务下对于个人信息收集的必要范围存在较大差异。无论业务类型区别，其所收集的个人信息均统一聚集在“滴滴基础信息服务平台”，相当于在用户授权方面，将多个平台的个人信息采集“混合打包授权”；同时平台规则方面缺乏个人信息在平台内不同业务之间流通的约束机制，极易引发对收集必要性原则的规避，用户无法得知其个人信息在何时何种范围内以何形式向哪个服务平台进行传输与分享。同样，形式化的“同意授权”规则也造成了第三方个人信息共享对收集必要性原则的规避。最后，网约车平台对个人信息数据的采集并非完全来源于手机 App 端，依托于传感技术、互联网智能信息处理技术，网约车行业正全面迈向“车联网”时代，实现车内网、车际网和车载移动互联网的“三网融合”，这意味着汽车本身就是一个大型移动传感设备，实时收集、产生着大量交通出行数据，其中涉及个人信息的数据不在少数。根据不同的采集场景，汽车数据类型可分为车外数据、座舱数据、运行数据以及位置轨迹数据，而过度收集事件的高发地在于车外数据及座舱数据的采集。在通过摄像头等车外传感器对汽车外部环境进行数据采集的同时，车外行为人的人脸、其他车辆车牌等涉及个人信息的数据被“悄然”采集，信息权利主体的知情权、信息处理权被损害。再者，车内座舱的数据采集会涉及乘客人脸、声纹、心律等生物识别信息，在《隐私政策》对乘客发挥“形式化告知”功能的现状下，乘客对座舱数据的采集用途与范围不得而知，敏感个人信息存在被侵害的风险。

2.数据存储传输阶段：未充分履行安全保护义务导致个人信息泄露

个人信息泄露指的是个人信息被非法和未经授权地获取，该事件在实

[1]《常见类型移动互联网应用程序必要个人信息范围规定》在此基础上进一步论述道：“其运营者不得因用户不同意提供非必要个人信息，而拒绝用户使用 App 基本功能服务。”此外还明确了网络约车 App 的必要个人信息数据的范围：“注册用户移动电话号码；乘车人出发地、到达地、位置信息、行踪轨迹；支付时间、支付金额、支付渠道等支付信息。”

践中发生频率低，但一旦发生，将给平台企业带来公众声望受损、经济利益受损、诉讼等法律指控风险以及内部产生不和谐因素等危害，[1]网约车平台不乏个人信息泄露事件。[2] 数据作为一种“有害材料”，在网约车平台中聚集得越多，其遭受泄露的风险就越大，影响泄露风险的因素包括保留时间、扩散、访问、流动性及价值五种。[3] 数据安全、个人信息保护相关规范的陆续公布，不断充实着网约车平台个人信息安全保障义务的内容，要求平台在数据存储和传输阶段，对数据进行分类分级保护，将用户个人身份信息与敏感个人信息存储在具备安全防护措施的终端上，达到访问权限控制的目的；在传输时采用加密、匿名化等安全措施保证特定主体不被追溯。但在实践中，拥有海量个人信息的网约车平台由于未能充分履行个人信息安全保护义务，并不能有效防范存储、传输阶段出现的外部威胁与内部威胁。外部威胁方面，首先，恶意入侵、网络攻击会直接导致个人信息的泄露，如黑客以漏洞攻击、病毒利用、“撞库”等手段进行数据的窃取，Uber就曾遭黑客攻击并导致5700万名用户个人信息泄露；其次，利用具备“自动化人工访问功能”的网络爬虫技术，违背Robot协议在未授权的情形下进行个人信息数据爬取，同样也是造成个人信息数据泄露。内部威胁方面，据相关调查显示，80%的数据泄露由企业内部人员所为，[4]平台内部人员监守自盗，内外勾结共同盗取个人信息以此牟利的事件屡见不鲜，甚至由平台管理层作出泄露个人信息数据的决策。平台在抵抗外部与内部威胁不力的原因在于未实质履行相关安全规范要求，数据安全风险防范与应对措施存在缺陷。值得注意的是，网约车平台对敏感个人信息的存储与传输并未严格贯彻数据分类分级保护原则。实际上，敏感个人信息更容易受到黑客的“眷顾”，[5]存

[1] 参见金元浦：《大数据时代个人隐私数据泄露的调研与分析报告》，《清华大学学报(哲学社会科学版)》2021年第1期。

[2] 不少用户在不知道的情况下收到滴滴打车平台注册成功的短信，网上有不少关于司机身份证号码被占用、车牌被注册的报道，在这些事件的背后是个人信息的泄露。参见王胜：《交通运输行业数据泄露现状浅析》，《中国信息安全》2018年第3期。

[3] 参见[美]雪莉·大卫杜夫：《数据大泄漏：隐私保护危机与数据安全机遇》，马多贺等译，机械工业出版社2021年版，第36页。

[4] 参见张莉主编：《数据治理与数据安全》，人民邮电出版社2021年版，第121页。

[5] 如有报告显示涉及敏感性数据泄露的事件占比较大，充分说明个人隐私数据中的核心部分在网络黑产中具有更高的可利用价值。参见金元浦：《大数据时代个人隐私数据泄露的调研与分析报告》，《清华大学学报(哲学社会科学版)》2021年第1期。

在着比一般个人信息更大的泄露风险，其危害结果也更为严重。以滴滴出行为例，尽管滴滴在进行个人信息收集时有明显提示并对敏感个人信息作出了特别标识，但未在管理过程中凸显其管控严格性，未与其他一般个人信息的处理方式予以详细的区分，行程录音录像等敏感个人信息的泄露时常发生。

3.数据共享阶段：违背同意授权规则与第三方共享个人信息数据

数据共享的概念主要在平台间使用，指的是数据控制者将自己收集的信息数据与他人分享，赋予分享者访问、操作、运算以及分析的权限，[1]具有减少数据采集成本，充分开发数据经济价值的功能。聚焦于网约车平台的数据共享实践，个人信息安全事件多发于面向私人的数据共享以及面向企业的数据共享过程中。

乘客个人信息共享的“私人”对象主要由驾驶员、紧急联系人组成。网络预约出租车业务的进行，离不开驾驶员对乘客相关个人信息的掌握。随着“私家车＋私家车主模式”与“四方协议模式”在网约车行业占比的逐步提升，平台与驾驶员开始脱离传统的雇主雇员形式，转而走向合伙制，驾驶员逐渐成为第三方的代理。平台将订单与用户个人信息分享给第三方，实际上对于乘客而言，只知道自己的信息由眼前的驾驶员所知，但对驾驶员背后主体获得自己信息的情况却不知情，违背了同意授权规则中对信息获得主体知情的要求。为乘客设置紧急联系人的业务，目的在于当乘客遇到安全事故后，一方面乘客可根据一键报警功能，通过平台向紧急联系人共享其行程信息、定位信息和报警情况，以求帮助；另一方面，当得知用户人身存在重大安全风险，紧急联系人可向平台申请查询用户行程信息和位置信息，以资帮助。对于涉及个人电话号码、精准定位等敏感信息的共享时，网约车平台应当以明显的方式告知乘客，并得到其明示的授权同意。但实践中，乘客在设置紧急联系人时，颇为随意，造成了乘客个人信息泄露的潜在危机，其背后是网约车平台未充分提示、说明紧急联系人的定位以及未向乘客明示其个人信息在紧急联系人方面的共享。

面向企业的数据共享方面，又可细分为向提供服务的第三方进行的数据共享以及为接入第三方提供服务所进行的数据共享。前者指的是，接入网约车平台为网约车服务提供服务，如接入第三方地图服务，为司乘人员提

[1] 参见王利明：《数据共享与个人信息保护》，《现代法学》2019年第1期。

供行程规划、路程导航;接入支付第三方完成车费的交纳等。后者指的是将网约车服务嵌入第三方软件中,如在高德地图中常会附带网约车平台提供的打车服务。网约车平台作为个人信息控制者,应当充分保障信息主体的权利,在将个人信息数据共享至第三方的同时,需警惕由此可能引发的个人信息安全问题。在以上对于其他平台的数据共享范围应当严格依照个人信息数据使用必要性原则,将共享的个人信息限制在约定的且业务相关的范围内,如不应共享乘客或驾驶员的手机号码及身份信息给提供地图服务的第三方。实践中,乘客以勾选"阅读并同意"的方式表达信息处置的同意授权,但前者并不是后者的充分必要条件。出于隐私条款的复杂、不易懂,对个人信息的共享规则在协议中没有以显著方式予以提及,查阅相关条款的入口不易找寻等可归责于平台的原因,乘客有意无意地忽略了自身个人信息被平台共享给第三方的实际情况,同意授权规则的运行流于形式。此外,平台通常将在个人信息收集阶段或者注册账号阶段获得的用户授权效力,延伸至数据共享阶段。实际上,乘客在收集阶段勾选"同意"的效力,不必然等同于同意授权对自身信息的共享,此"概括授权"行为对同意授权规则形成了规避,个人信息权利被侵害。

三、网约车平台个人信息安全的既有保护模式

信息技术革命对交通出行行业的"破窗效应",表现为网约车平台这种新业态对传统巡游式出租车商业模式的冲击与取缔。人们的生产生活方式在信息化、数字化的过程中被解构,使得平台原有管控或治理机制难以有效应对新的挑战,网约车平台的个人信息安全问题尤为突出。即便是在出行行业居于领先地位的滴滴出行,在拥有"五大安全科技"的同时,也频繁出现个人信息安全问题。在协同社会治理理念的推动下,网约车平台经历了由"单一主体监管"到"多主体协同治理"的理念转变。现阶段,我国网约车平台的个人信息安全保护,主要是依靠政府、行业的外部监管以及平台的内部监管。

(一)外部监管模式

针对网约车平台的外部监管研究,自2010年5月最早的网约车公司(易到用车)出现以来就未曾断绝。网约车行业经历了从自由发展到全盘否

定，再到独立监管的阶段。出于新信息技术、新业态的冲击，政府监管部门处于一种矛盾复杂、谨慎应对、放管两难的境地，监管应对呈现反复性、多样性的特点。[1] 对网约车平台个人信息安全的外部监管而言，实践中表现为由政府部门直接监管或者由政府部门引导的行业监管两个面向。前者可以被描述为“反身式控制模式”，即在个人信息安全事件发生后，对责任主体进行行政、刑事责任的追究，以此促使平台规范个人信息处理行为。行政责任方面，处罚机构主要为公安部门及市场监督管理部门，针对网约车平台的“违法收集用户个人信息”“非法获取、出售、向他人提供个人信息”“不履行个人信息保护义务”“侵害用户依法得到保护的个人信息权利”等违法行为，要求其承担相应行政责任。[2] 刑事责任方面，网约车平台作为网络服务提供者，在明知网络产品、服务存在缺陷、漏洞的情况下，不进行补救与报告，造成个人信息数据泄露等严重后果，可能构成侵犯公民个人信息罪、泄露国家秘密罪等。政府部门引导的行业监管方面，旨在行业内部制定行业的数据管理规章、数据安全标准，为行业的个人信息安全提供示范与指引。[3] 行业自律规范作为“软法”，产生于管理检验、行业规律或既有利益诉求，虽无“硬法”的强制力作为保障，但在市场环境中依然存在着保障其实施的隐性力量，如对于网约车平台而言，个人信息安全保护机制的好坏直接与其市场信誉挂钩，是用户选择的标准，也是其从其他各类平台脱颖而出的核心竞争力。所以行业自律标准依然具有划定新业态市场尺度的规范功能。值得注意的是，行业标准一般由政府部门牵头，吸收行业代表、学界权威等进行协商起草，其形成是多种利益追求和价值取向之间的博弈与妥协，该种以协商方式建立起的“准公共秩序”更易于行业主体的遵守。

（二）内部监管模式

外部监管在面对新科技带来的个人信息安全风险问题时，是保守与滞

[1] 参见马长山：《智慧社会建设中的“众创”式制度变革——基于“网约车”合法化进程的法理学分析》，《中国社会科学》2019 年第 4 期。

[2] 依据《网络安全法》《数据安全法》《个人信息保护法》进行责令改正、警告、没收违法所得、罚款、责令暂停相关义务、责令停业整顿、责令关闭网站、吊销相关业务许可证、吊销营业执照等行政处罚。

[3] 如 GB/T 35273—2020《信息安全技术　个人信息安全规范》、《信息安全技术　网络预约汽车服务数据安全指南》（征求意见稿）、《汽车采集数据处理指南》等。

后的，给平台自治留下了更多的发挥空间；在深度落实“三个清单”制度的背景下，市场的自由度被大大提高，给平台自治带来了生存土壤。[1] 为弥补数字经济时代政府规制能力缺陷的需要，平台“私权力”[2]兴起。为维护“私人秩序”，平台须行使其“私权力”，对虚拟空间内发生的对个人信息安全造成威胁的隐患进行监管。网约车平台对个人信息安全进行内部监管的目的，在于为平台共享开放个人信息，盘活数据价值的进程中设定一个安全底线，对超越红线损害用户权益的个人信息处理行为进行及时的识别与整改。为实现此目标，平台不仅需要在规范层面限制双方的数据交易行为，还需在平台内部建立一套科学的个人信息数据管理机制。区别于传统的实体店经营者，平台依托互联网技术搭建虚拟空间聚集供需多方，实际上成为交易活动的管控者、协调者。此场景下，平台行使内部监管的职能表现为平台规则的制定，即为保障平台的营利性不被外部行为所影响，保护信息主体的权利不被侵害，平台需搭建规则框架，确保参与平台的人们和商家都“有规可依”。[3] 除对交易者行为的监管之外，对个人信息安全的内部监管更多指的是“自我规制”[4]，即平台内部的个人信息数据管理机制[5]。根据某网约车平台内部的安全处置手册来看，个人信息安全问题主要由安全处置部[6]负责。平台从安全事件所造成的损失程度、紧急程度、有责范围、敏感因素等方面，将应急事件分为普通级、较大级、重大级、特大级四个等级，且

[1] 参见马长山：《迈向数字社会的法律》，法律出版社2021年版，第215页。

[2] 平台的“私权力”现象指的是，独特的市场地位使得平台集制定规则、解释规则、解决纠纷等多项“权力”于一身，承担着规制网络市场、维护网络市场秩序的公共职能。参见刘权：《网络平台的公共性及其实现——以电商平台的法律规制为视角》，《法学研究》2020年第2期。

[3] 参见金善明：《电商平台自治规制体系的反思与重构——基于〈电子商务法〉第35条规定的分析》，《法商研究》2021年第3期。

[4] 学界中的自我规制一直具有多义性，有时指向心理学意义上的自律行为；有时指向集体组织对成员的约束和规范。本文的自我监管强调的是集体性，其本质是一种集体治理过程。参见李洪雷：《论互联网的规制体制——在政府规制与自我规制之间》，《网络信息法学研究》2017年第1期。

[5] 一般而言，平台通过建立具有针对性的数据资产管理体系，以管理组织架构、管理流程、管理机制和考核评估办法，通过管理手段明确“责权利”保障数据资产管理工作的有序开展。参见梅宏主编：《数据治理之论》，中国人民大学出版社2020年版，第151页。

[6] 该部具体设置总监、指挥、指挥值班、区域管理以及城市安全五大履行安全处置职责的岗位，负责安全事故的应对。

根据不同级别的事件设置不同的响应部门与应对手段。泄露个人私密信息、信息泄露等个人信息安全事件散见在突发事件与涉案事件中，并未单独作为一类事件列出。

（三）面向个人信息安全风险的局限

在云计算、物联网、大数据等新兴技术对网约车平台进行“创造性破坏”的背景下，网约车个人信息安全风险呈不断升级、影响逐步扩大、危害程度更加严重的态势。与此同时，个人信息安全相关法律法规、国家标准陆续出台，合规性审查被逐渐提上重点监管日程。[1] 网约车平台亟待加大个人信息安全保护力度，以达到防范风险、符合规范性要求的目的。但网约车平台现有的个人信息安全保护模式没有形成合力，并不能很好地实现上述目的，在实践中存在不能有效预防个人信息安全风险、不能及时识别个人信息安全危机、不能积极应对个人信息安全事件三大局限。

1.不能有效预防个人信息安全风险

个人信息安全事件的风险预防讲究针对个人信息数据危机产生的原因和因素，采取有效措施予以消除，并对可能造成事故出现的人员进行早期防御与矫治，从根源上杜绝个人信息泄露、滥用行为的出现。多数安全事件的发生源自企业员工个人信息安全意识的欠缺，诸如内部人员窃取个人信息数据非法牟利、研发人员向业务系统中放置后门、驾驶员泄露乘客信息数据等造成个人信息泄露的事件屡屡发生。个人信息安全风险预防的关键之一就在于提高平台内部人员的个人信息安全保护意识，但无论是外部规制模式还是内部规制模式都在人员安全意识提升实践中呈现出“乏力”的效果。无论是外部规制模式中的政府部门监管还是行业监管，在作为唯一治理手段时都无法有效地促使个人遵守相关规范。其原因在于单单依靠外部规制的威慑机制，难以“倒逼”当事人遵守相关法律法规，相反实践中当事人往往

[1] 针对网约车行业的合规性审查已初见苗头，如2021年9月1日上午，交通运输部会同中央网信办、工业和信息化部等，对T3出行、美团出行、曹操出行等11家网约车平台公司进行联合约谈。在保障用户信息和数据安全方面，要求各平台公司在用户数据收集、传输、存储、处理等环节，要依法建立相关数据安全管理制度，采取必要的安全技术和管理措施。参见“五部门联合约谈11家网约车平台公司：保障司乘人员合法权益”，《人民网》http://finance.people.com.cn/n1/2021/0902/c1004-32215608.html，最后访问日期：2021年12月26日。

不惧“威胁”,并抱有侥幸心理实施违规行为。一方面,行业标准在缺乏“强制力”约束的同时,并未在行业之中产生让人发自内心的敬重与服从,造成对相关人员的“放纵”。再者,数据安全正处于快节奏“立法”阶段,对于众多法律法规、行业标准的解读都要通过实践运用来加以明确,这就导致被规制的主体并不能及时、准确地把握数据安全相关规范中规定的数据权利义务关系,导致规范性要求落空,法律法规的“野蛮生长”甚至影响立法的权威性与公信力。另一方面,个人信息安全意识的提高在内部规制模式中不具有重要地位,专门针对个人信息安全问题的覆盖企业上下层的数据安全培训更是少数,甚至在内部人员违规的情况下予以包庇。在大多数企业内,数据安全问题都尚未得到高级管理层的充分重视,而是交由信息或网络安全技术部门负责,由于缺乏高管的有效参与以及协调,数据安全治理机制在推进过程中困难重重。数据安全制度的建立、方案的实施与执行都受上述影响流于形式,不能对数据安全进行有效的保护。

2.不能及时识别个人信息安全危机

及时识别个人信息安全危机,有利于控制危害范围的继续扩大,及时发现个人信息安全问题的产生原因。目前我国对网约车平台的数据监管,在外部规制中由于行业组织的缺位,主要由政府部门负责,在内部规制方面由平台进行自我监管。[1] 但政府对于行业存在的“专业壁垒”,在缺乏足够的信息与专业知识下,不能准确把握行业的未来发展趋势,在面对新领域的监管过程中,由于信息不对称等原因,具有滞后性的缺陷,不能有效地防止风险的产生与扩大;而且,政府内部决策流程往往不能适应经济社会发展对规制灵活性、动态性的要求,在实现对个人信息安全的实时、全覆盖监管方面难度加大;此外,网络技术日新月异,网络侵权具有隐蔽性强、涉及面广、调查取证困难等特点使得政府监管职责难以落实。[2] 内部规范模式下,由于个人信息安全问题并未上升至公司战略高度,为控制成本收益,平台具有简化个人信息安全保护措施的动机,难以投资革新现有技术。传统的被动式个人信息安全防护技术不足以面对数据大量聚集、信息技术驱动带来的新

[1] 根据《网络预约出租汽车监管信息交互平台运行管理办法》规定,“交通运输主管部门负责网约车监管信息交互平台使用、运行和维护管理工作,各网约车平台公司负责规范本企业网约车平台的运行管理和数据传输工作”。

[2] 参见肖成俊、许玉镇:《大数据时代个人信息泄露及其多中心治理》,《内蒙古社会科学》(汉文版)2017年第2期。

挑战，不能满足对数据流通安全性能的实时检测要求，不能及时识别新型网络攻击手段及预测其所造成的危害后果。个人信息安全技术的不成熟是导致个人信息泄露的重要原因，如2019年Grab个人信息泄露事件[1]。这就要求技术需跟随数据安全的相关政策、法律法规、监管要求和标准规范的颁布和更新进行持续性的优化。

3.不能积极应对个人信息安全事件

外部规制模式不能促进平台合法、正当应对个人信息安全事件的原因在于激励性的缺失。平台经济的基础是盈利的可持续性，这使得平台具有扩大数据收益，减少数据成本的倾向。数据收益方面，网约车平台依托于北斗应用与交通信息技术，对司乘数据进行精准匹配，司乘双方因此向平台支付匹配服务的使用费用。除此之外，还存在与第三方基于数据共享的收益，如商业广告、社交媒体等数据交易。数据收益一般与数据的流通性成正比，平台存在促进数据流通的趋势。数据成本方面，数据匹配的前提是对非结构性数据的收集与整合，该行为会导致个人信息数据批量集结，平台的数据资产更容易成为被破坏的目标。为保障数据安全，平台对数据安全内部管理体系、数据安全保障技术、数据安全应急措施、专业技术人员的招聘等方面的投入，构成主要的数据成本。外部规制主体通过提高个人信息数据安全保护标准以此防范风险，导致网约车平台的数据成本提升，数据流动性减弱，数据收益减少，以惩罚为核心的外部规制理念与平台经济发展的理念背道而驰，是导致网约车平台“形式守法”发生的主要原因。另外，内部规制模式在应对个人信息安全风险上具有先天的缺陷，即“规制者被待规制利益所俘获的风险”，在独立监督机构缺失的情形下，容易引发“自我放纵”的危机。实践中，网约车平台在遭受漏洞攻击、病毒利用、“撞库”等外部的恶意入侵事件，导致大范围的个人信息泄露后，出于平台声誉、受司法追究等不利后果的考虑，并没有积极实施紧急预案或事后处置措施，甚至有些平台企业试图隐瞒安全事件的发生，如2017年Uber数据大泄露事件中平台的消极应

[1] 2019年8月30号新加坡网约车Grab公司，由于应用更新后缓存机制的不兼容，导致众多司乘个人信息泄露。参见《国内机构重大数据泄漏案例》，https://zhuanlan.zhihu.com/p/113257010，最后访问日期：2021年12月26日。

对态度。[1] 平台之所以选择以违规的方式应对个人信息安全事件，原因是合规激励性机制的缺位。

四、网络平台的数据安全合规体系：制度架构与信息技术

网约车平台个人信息安全的既有保护模式并不能很好地实现数据安全保护功能。内部监管模式主要依靠对企业文化的认同、个人道德的培养来促使员工遵守规范，但由于个人信息安全问题未提升至公司战略意义，在实践中存在执行力不足的问题，自发的监督还存在着“自己如何监督自己”的悖论，监督功能被架空。主要依靠“威慑”促进规范落实的外部监管模式也会导致规范被规避的异化现象，在禁止性规范、义务性规范存在“高质量执法能力缺失”“规范与实践的脱节”等弊端下，激励性监管的作用被凸显出来。[2] 当下，作为通过政治组织社会进行社会控制的法律，存在着“必须求助于个人”的限制，即“依靠个人主动精神来保障法律救济和实施法律规则”。[3] 普通法中依靠个人检举揭发来促使守法的极端个人主义已趋于消灭，兴起的是个人与公权力以“合作”方式去实现法律规范的落实，而数据安全合规体系的建设，在一定程度上符合了该“社会控制”的发展趋势。数据安全合规并不局限于对规范的遵守，而是在立法引导与安全审查的推动下，平台自主建立的以数据安全风险防控为直接目的的规范落实机制，讲究在注重平台内部的数据管理与安全治理的同时，关注数据治理如何与相关法律法规、政策及行业标准保持步调的一致。其核心在于以行政责任的减免、刑事实体与程序上的“出罪”[4]、资格制裁的撤销等激励为导向，通过衔接内外监管，以公私合作的方式促进规范的落实，获得平台营利与权益保障的“共赢”。“自创生”系统论视角下，信息技术与制度架构构成数据安全合规

[1] 彭博社爆出Uber在得知数据被窃取后并没有第一时间向相关监管机构、用户履行报告及通知义务，而是向黑客支付了10万美元，试图销毁被盗数据以隐瞒泄露事件。参见《5700万用户数据被盗，黑客勒索赎金，优步的做法让人大跌眼镜！》，http://www.nbd.com.cn/articles/2017-11-22/1163917.html，最后访问日期：2021年12月26日。

[2] 参见周汉华：《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》，《法学研究》2018年第2期。

[3] 参见[美]罗斯科·庞德：《通过法律的社会控制》，沈宗灵译，商务印书馆2010年版，第36页。

[4] 参见李玉华：《我国企业合规的刑事诉讼激励》，《比较法研究》2020年第1期。

治理生态的子系统。子系统之间若存在沟通障碍，难以形成功能系统间的良性共振环境，系统间的不兼容极易诱发风险。[1] 这就要求制度架构与信息技术能够形成相互预期的闭环系统，即信息技术的引进将助力制度架构的有效实施，制度架构落实的反馈机制又将促进信息技术的革新，两者共同作用于数据安全合规治理体系的完善。“制度＋技术”闭环系统运行的科学性决定着合规计划的有效性，有利于逐步实现数据安全合规的自动化，达到对数据应用场景的全流程实时控制，减少了“人为因素”干预的不确定性。

（一）数据安全合规体系的制度架构

1.建立数据安全风险评估制度

预防数据安全风险的最佳措施是设立数据安全风险评估制度。该制度作为数据安全防控的第一线，不能局限于平台数据安全自查的初期，还要贯穿于平台数据安全合规制度的始终。这一阶段平台的风险评估应当立足于对自身业务领域的模块化梳理，将法律法规、行业标准要求的与数据安全相关的基本原则、数据主体权利及数据处理者的义务作为评估依据，目的在于评估出数据全生命周期中的风险，给平台的数据处理活动以指引。

第一，对数据的收集与使用进行评估。对数据收集与使用的评估重点在于如何防范个人信息数据滥用与误用的风险。无论是平台直接收集的个人信息数据，还是间接收集的个人信息数据，都应当评估平台有无遵守、是否严格遵守《数据安全法》第32条、《网络安全法》41条规定的“合法、正当、必要原则”。首先，明确平台收集、使用的个人信息范围。平台应在内部章程文件中梳理并明确平台的业务，并根据其业务范围严格限定平台所需收集、使用的数据范围。其次，区分一般个人信息与敏感个人信息。立足于“敏感”的法律规制的高反应速度、权益侵害风险性两个法律基准，[2]平台需对敏感个人信息进行更高质量的安全保护。再次，收集、使用个人信息应向用户明示且经用户同意授权。平台在收集个人信息数据时，需在程序上符合“告知—同意”规则，实体上受到正当目的原则、必要性原则的限制，实

[1] 参见陆宇峰：《“自创生”系统论法学：一种理解现代法律的新思路》，《政法论坛》2014年第4期。

[2] 参见宁园：《敏感个人信息的法律基准与范畴界定——以《个人信息保护法》第28条第1款为中心》，《比较法研究》2021年第5期。

体原则作为基本原则指导程序的具体运行。[1] 这就要求平台的《隐私政策》或者《用户协议》中的隐私条款应当按照《个人信息安全规范》中的《隐私政策模版》,明确收集、使用的范围。对于上述隐私条款中的关键条款,应通过"增强式告知""主动触发"等对用户进行显著的告知。[2] 再者,当产品服务在升级或者增设功能后,需要扩大对于个人数据的收集范围时,需依据同样的"明示授权"标准。最后,平台收集的数据不完全是涉及个人信息的数据,对于非个人信息数据也需要进行风险评估,其目的在于防止非个人信息的聚集导致的个人信息重新识别,在非个人信息批量聚集具备"识别性"时,也需经过信息权利主体的同意与授权。

第二,对数据的存储进行评估。此阶段的重点在于数据分级分类保护制度。《数据安全法》第21条要求建立数据分级分类保护制度,目的在于合理配置数据保护资源,将一旦安全事件发生,容易造成权益严重损害的数据类型进行重点保护,但法律并未进一步明细数据的具体分类分级方式、保护措施。出于行业、领域的巨大差异性,需要作为数据控制者的平台企业根据法律法规、行业标准予以明确。[3] 具体而言,平台应基于对数据资产的梳理,在不违反合法合规原则、分类多维原则、分级明确原则、从高就严原则以及动态调整原则的前提下,对数据先分类再定级,设置不同标识进行管理,对不同类型不同级别的数据设立梯度式的保护措施。在数据的分类层面,平台需首先按照法律法规或监管部门对数据的专门管理要求,对特殊数据进行区分识别,其次按照行业共识、平台内部数据管理需求对数据进一步分类。在数据定级层面,首先参考核心数据目录、重要数据目录,将该种数据与一般数据分开,[4]若平台存储的数据不属于目录所列,则参照数据的重

[1] 参见张新宝:《个人信息收集:告知同意原则适用的限制》,《比较法研究》2019年第6期。

[2] 告知的内容应包括:"收集、使用个人信息的目的;个人信息的收集方式和手段、收集的具体内容和留存时限;个人信息的使用范围,包括披露或向其他组织和机构提供其个人信息的范围;个人信息的保护措施;个人信息管理者的名称、地址、联系方式等相关信息。"参见于莽主编:《规·据:大数据合规运用之道》,知识产权出版社2020版,第189页。

[3] 如法律法规层面的《网络安全法》《数据安全法》《个人信息保护法》等;行业标准层面的《信息安全技术 网络安全等级保护定级指南》(GB/T22240-2020)、《网络安全标准实践指南——网络数据分类分级指引》等。

[4] 如至少应区分涉及国家秘密的数据、个人信息数据、重要敏感信息数据、关键数据。参见于莽主编:《规·据:大数据合规运用之道》,知识产权出版社2020版,第75页。

要程度，即数据安全问题发生时对权益造成的影响大小，来类推数据级别的适用；在符合行业标准的前提下，平台可以依内部管理的特殊需要，将数据进行进一步划分，如将敏感个人信息进一步划分为一般敏感与重要敏感。数据存储期限层面，数据的存储需要较高的成本，实践中平台会对不被业务需要的数据进行删除，对具有经济价值的数据进行长期限的保留，而法律法规会对某些数据的存储期限予以限定。对平台在存储期限上的要求，是《网络安全法》第41条规定的收集、使用必要性原则理念在存储阶段的自然延伸，将数据的存储期限，限定在实现业务功能所必需的最短时间内，对于超出必要期限的数据，应当要求平台予以删除。数据存储地点层面，一般将采集的数据以及数据分析结果进行本地化存储或者借助第三方存储，出于对实时数据的需求与对存储成本的控制，只有部分数据需要长时间地保留，进入数据生命周期的其他阶段。涉及国家安全、社会公共利益、重要个人权益的敏感个人信息、关键信息数据、重要数据等应存储在中国境内；不同类别的数据应当分开存储，并采取物理或逻辑隔离机制。最后，平台应对已存储的数据履行安全保护义务。《网络安全法》第22条、第41条要求作为数据控制者的平台企业，为防止数据的泄露、毁损、丢失等数据安全事件的发生，应当对存储的数据采取必要的技术措施予以持续性保护。

第三，对数据的传输进行评估。数据的传输指的是平台将收集存储的数据、处理分析过的数据，以线上或者线下的方式，在平台内各部门之间流转或者向平台外的合作伙伴进行传递。法律法规要求平台在进行数据传输时，概括承担包括传输事后的数据责任，严格限制跨境数据传输的数据内容，规范审查备案程序。数据的境内传输层面，平台内部各部门之间的传输，依据内部规定进行，法律法规更多关注的是平台之间的数据传输活动，又被称为数据共享活动。首先，平台企业不因完成数据传输活动，就免除其个人信息保护义务与数据安全保护责任，而将其责任延伸至数据及其副本的完全销毁阶段，[1]所以平台的评估范围应当包含对自身与接受方/提供方数据传输安全保护能力的评估，评估内容包括数据的敏感性、脱敏措施的有效性等。其次，平台不得传输《保守国家秘密法》等法律法规要求的禁止

[1] 在数据共享和流通环节不能只关注自身范围内的数据安全保障制度，还应该将接收方的数据安全保护能力考虑在内。参见周瑞珏：《数据治理语境下公司社会责任的基本内涵和制度构建》，《政法学刊》2019年第4期。

传输的数据，若发现该违规行为，则应依据《网络安全法》第50条的可审计原则，对相关数据操作记录进行保存，保证涉密、违法数据的可追溯性，以配合相关部门调查。再次，平台在为第三方划定访问控制权限时，应当在合作协议中明确与合作第三方的数据安全保护权利义务边界，以及违反上述条款时，双方应承担的责任范围。数据的境外传输层面，关于数据跨境传输安全评估制度的立法指引仍然比较宏观，缺乏统一的部署，[1]但企业还是应该建立跨境数据传输相关的基本保护制度。针对数据跨境传输的审核应当着重对数据信息内容的审核，在可能涉及国家安全、社会公共利益、重大个人权益的信息时，若未经相应主管部门批准，不得通过线上或线下方式进行传输。

第四，对数据的删除进行评估。数据删除不仅包括删除平台存储的静态数据及其副本，还包括断开实时数据流的链接通道。法律法规要求平台对其不当收集、正当收集但已超存储必要期限、正当收集存储但数据转变为不与业务相关的数据进行主动删除；此外，平台也应当遵从信息权利主体对于个人信息数据的删除要求。

2.建立数据安全合规组织架构

“合规”不局限于“守法”，更加强调规范在组织的有效执行，其关键在于建立科学的合规组织架构，以此保障合规工作的有效开展。依据有效的合规计划标准，合规组织的构成应当包括合规委员会、首席合规官、合规部门以及合规人员，[2]即合规组织的建构应当贯穿于平台企业的决策层、管理层、技术部门、业务部门及审计部门。数据安全合规属于网络平台专项合规的一类，在上述各层级的合规组织中应当分别、单独设立专门的数据安全合规组织。首先，在企业核心高级管理人员当中，设立专职或兼职的数据安全合规管理人员，是数据安全合规工作能够顺利、有效进行的前提，发挥着统筹规划、宏观指导、资源调配、部门联动等作用。其次，需依据法律法规、行业标准等规范，对平台运营在数据全生存周期方面的规范性要求，明确数据安全合规各级部门的职责范围与工作重点。再次，平台还需结合具体的业

[1] 比如安全评估的标准不够明确具体；哪些数据传输出境情形属于达到了难以有效保障个人信息安全的程度，没有给出统一的评估标准；如何对境外接收者的网络安全能力进行评估也没有具体规定。参见翁国民、宋丽：《数据跨境传输的法律规制》，《浙江大学学报(人文社会科学版)》2020年第2期。

[2] 参见陈瑞华：《企业合规的基本问题》，《中国法律评论》2020年第1期。

务，制定数据安全合规的追责制度，签订安全责任协议和保密协议，划定数据安全责任人员被追责的情形，对数据安全岗位人员的履职情况制定绩效考核方法并与工资待遇、惩戒措施挂钩。最后，平台企业在条件允许的情形下，可以设立与数据处理人员分离的数据安全监督员，对数据主体进行实时性和系统性的监控，并赋予其发现数据安全问题直接向管理层汇报的特权。

3.建立内部数据安全管理体系

解决数据安全问题的关键在于根据平台现实需求，建立一个较为完备的数据安全管理体系。首先，做好身份信息认证。数据安全的主要威胁来自未授权的非法访问，身份认证的目的在于赋予特殊身份主体的特定访问权限，以此禁止未认证或者未授权的访问申请。基于智能卡、生物特征、动态口令、Usbkey等技术措施的验证身份功能，[1]平台可以通过证书管理，编入加密算法，实现对访问身份的合规性识别与确认。其次，做到数据访问权限管控。权限管控在于为数据处理主体划定业务必要的权限范围，是精细化、系统化管理的题中之意，有利于系统资源的合理配置，也是防止数据处理主体滥用数据权限的必要措施。数据访问权限管控的本质在于为权限的使用设置实体访问控制、数据访问控制，[2]确保员工权限都是其业务所必需的最小权限。在涉及敏感个人信息数据的访问、修改等处理时，设置更加严格的审批流程。值得注意的是在人员转岗或离职时，平台系统应当及时修改其对数据的处理权限范围。再次，对数据资产进行加密存储与脱敏传输。进行数据资产管理的前提在于对平台自身数据资产的梳理与识别，即要求对平台内部的现有各种结构化或非结构化数据以及历史存留的数据表进行分级分类，确定对各数据项的具体访问权限，在此基础上利用分布式数据库存储等加密技术进行分级保密处理。将涉及敏感个人信息的数据进行静态或动态脱敏，达到无法识别到特定个人且不能复原，彻底消除身份指向性的目的。[3] 最后，设立数据安全事件的处理措施。相关法律法规要求

[1] 参见周丽娅：《身份认证技术在网络安全中的应用》，《信息与电脑（理论版）》2021年第16期。

[2] 参见张锐卿、汤泰鼎、万可：《大数据环境下细粒度的访问控制与审计管理》，《信息安全研究》2017年第6期。

[3] 参见包英明：《大数据平台数据安全防护技术》，《信息安全研究》2019年第3期。

网络平台针对数据安全事件建立相应的处置措施，[1]但未对具体处置措施予以明细。鉴于此，为防止危害的继续扩大、避免相关安全事件的再次发生，网络平台需明确以下几项措施：其一，在数据安全事件爆发后，建立专项应对小组对事件性质进行判断，以此协调人员的具体分工与操作流程；其二，及时上报主管部门，报告的内容应当包括相关数据的数量、类型、信息内容等基本属性，可能造成的影响，已采取的处置措施以及相关专员的联系方式；其三，履行安全事件的告知义务，将数据安全事件发生的原因、平台已采取的补救措施、可能产生的损害结果，以合理、有效的方式告知权利主体，并在此基础上提供自主防范风险的可行建议以及数据安全负责人的联系方式；其四，对数据安全事件的全流程进行记录，以备监管部门调查以及平台内部的经验教训总结。[2]

4.定期进行数据安全合规培训

数据安全合规培训应当定期对董事、高管、雇员和第三方进行，且根据培训对象职能、层次的不同，建立更有针对性的培训内容。管理层方面的数据安全培训的关键在于打通管理层与技术部门的“业务壁垒”，强化管理层对数据安全合规的重视程度。为此应定期让管理层参与到涉及数据安全的重要会议中，同时对管理层定期开展对国内外数据安全典型案例的研读活动，并对数据安全事件发生的原因、平台的先进应对经验以及风险预防措施进行探讨与学习。业务部门层面的数据安全培训的症结在于对数据安全相关规范的理解、最新进展以及相关司法案例不熟悉。所以须定期对内部工作人员进行数据安全保护相关知识培训，并对培训结果进行评价、记录，确保员工能够熟悉掌握个人信息保护、数据安全国家相关法律法规及平台内部规定。此外平台还要重视对合作第三方的培训，与合作第三方的数据安全合规培训重在合规信息的互通。第三方个人数据安全合规意识的强弱以及应对合规风险的能力大小，会对平台自身产生重要影响。因此平台要主动重视与第三方的沟通，协调双方关系，定期开展个人数据安全合规业务交流和培训，提高第三方合规风险意识与抵御能力。

---

[1] 依据《数据安全法》第29条“发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。”

[2] 参见刘新宇主编：《数据保护：合规指引与规则解析》，中国法制出版社2021年版，第309～312页。

5.建立数据安全审计制度

建立数据安全审计制度是保证数据非否认性的重要途径，有利于有效防范内部滥用数据的行为，也是对业已建立的数据安全合规制度的检验与考察，其本质在于跟踪数据处理主体对数据操作的每个步骤，使得用户在使用数据资源访问权限时留下包含操作人、内容、时间等信息的记录。[1] 在人工智能自动化技术措施下，平台可自动形成操作监控的审计报告，以备管理层、数据安全合规负责人等相关数据安全人员查询、审计、评估，在发现数据安全合规制度隐患时迅速处理，并及时对相应制度进行优化、整改。对数据安全进行审计的必要性还在于与监管部门的衔接。[2] 当监管机构展开对平台的数据安全合规调查时，平台应设立安全专员与监管机构进行对接，将具备自查功能的审计报告交由相关机构调查。对监管机构经过合法调查发现的合规问题，平台须按照监管机构的要求及时整改。

（二）助力数据安全合规治理的信息技术

数据安全监管的日益严格、数据安全风险的不断升级，对网络平台提出了更高的数据安全治理要求，“制度＋技术”治理模式是平台作出的回应，目的在于平衡商业发展与合规工作。事实上，数据的全生命周期无不依赖信息技术及其基础设施，采取技术措施本就是平台数据安全合规治理的一部分，[3]创新“合规科技”[4]更是衡量数据安全合规治理能力的重要因素，发挥着预防数据安全风险、减轻合规治理负担、有效衔接内外监管的重要作用。当然，在“制度＋技术”闭环系统中，技术的功能在于助力合规制度的高效运行，而非重复甚至替代合规制度的运行，这也意味着信息技术的引入需

[1] 参见于莽主编：《规·据：大数据合规运用之道》，知识产权出版社2020版，第218页。

[2] 《网络安全法》第28条规定“提供技术支持和协助”、《数据安全法》第35条规定需配合有关机关维护国家安全或者侦查犯罪进行调取数据。

[3] 《数据安全法》第四章明细了数据处理者的数据安全保护义务，其中的第27条要求平台“采取相应的技术措施和其他必要措施”。

[4] “监管科技”最早出现在2015年英国政府科学办公室对金融科技优势的研究报告中，后成为全球监管讨论中的通用词语，狭义上仅指金融机构内部的合规程序通过使用科技的辅助手段变得更加有效和高效。广义上还包括为与金融行业的数字化发展同步，监管机构对技术创新加以利用。国内多数学者将狭义上的“监管科技”称为“合规科技”，这里的“合规科技”不单局限于金融领域，而在整个被监管主体意义下使用，指的是平台企业为实现合规而进行的技术创新。

受到制度架构的限制，否则将陷入“法律代码化”的极端之中。目前，全球正兴起着合规信息技术的研究，甚至出现以行业标准等规范形式予以合规技术指引的现象，技术逐渐成为合规治理体系中不可或缺的一部分。本文选取业界较为前沿的三种信息技术，并结合其技术原理，分析其在数据安全合规方面的应用价值，为网络平台的数据安全合规治理带来新的方案。

1.助力个人信息安全保护：差分隐私技术

网络平台建立数据安全合规体系的初衷在于预防数据安全违规风险，以运营的合规化对数据安全事件防患于未然。信息技术在带来风险的同时，也为数据安全治理能力的提升提供了机遇。恶意攻击技术的升级，为网络平台的数据安全合规治理带来了新挑战，驱动着合规信息技术革新。个人信息泄漏作为数据安全防范的重点，具有危害影响深远、造成损失严重、预防困难的特点，多因外部恶意攻击、内部人员滥用发生。为避免个人信息泄漏事件的发生，相关法律法规、行业标准通常要求网络平台对个人信息进行匿名化处理。实践中平台通过 k-Anonymity 等技术为非权限访问者增加访问难度，以此保护个人信息的机密性。随着攻击手段的升级，传统信息技术不足以支撑数据安全维护，平台违规风险剧增。为将平台拉回合规的“正轨”，信息匿名化技术亟待进一步革新，差分隐私技术应运而生。

差分隐私技术最初应用于数据库之间的交互式查询，将其应用于数据安全合规治理中的价值，在于以更高级的匿名化方式，确保个人信息处于“不能复原”的安全状态，有效防范数据处理过程中恶意主体对特定个人的“重新识别”，避免个人信息泄漏。差分机制能够隐藏特定数据主体的具体信息，原理是在将终端采集的数据上传至服务器前，为数据随机编入噪声算法，依据数据被记录时的敏感度设定相应的查询数值；要达到“返回查询答案”的目的，对于敏感度为均值的来说，轻微的噪声就足够了；而对于涉及敏感度较高的数据（如特定身份信息）则需要非常大的噪声，[1]以此增加访问难度。添加噪声的数据无法被用于追溯到特定主体，但匿名化技术的核心并非“不可还原信息”[2]，即商家依然可以通过整合分析碎片信息，用于群

[1] Domingo-Ferrer J, Sánchez D, Blanco-Justicia A. The limits of differential privacy (and its misuse in data release and machine learning), *Communications of the ACM*, 2021, Vol.64, No.7, pp.33-35.

[2] Aricle 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques.

体用户画像的建立，实现对用户行为趋势的预测，使得平台在挖掘个人信息商业价值的同时，始终保持在合规的界限内。此外，差分隐私技术还具有抵抗恶意攻击的功能。该技术能保证任何对于个人隐私的推断都是相同的，[1]即使在数据库中删除或增加一个记录也不影响数据分析结果，攻击者获得除了一个特定的目标信息之外的所有内容也不能锁定和判断出这个记录内容。[2] 合规信息技术的革新能够有效防范数据安全风险，从源头上避免了平台因发生数据安全事故而引发的违规风险。

2.助力数据安全合规效益提升：知识图谱技术

合规效益由收益与效率组成，前者指的是除去合规成本之后的合规利润；后者指的是单位资源投入下合规收入的比例。作为影响合规体系制度架构是否被有效执行的关键，合规效益越低，制度架构在实践中落实的阻力就越高；合规效益越高，则执行制度架构的激励性越高，合规制度架构被执行的程度就愈深。将知识图谱技术引入合规治理体系的优势，在于通过其智能技术与结构化的表达方式，减少人工成本、提高沟通效率，从而提升数据安全合规效益，促进数据安全治理制度的落实。

知识图谱的正式概念由 Google 在 2012 年提出，指的是由代表不同实体的节点、揭示实体间关联性的边组成的语义网络，出于其将知识进行“结构化表达”的优势，常应用于搜索引擎、社交网络、辅助决策等领域。知识图谱的体系建构基础在于知识抽取、知识融合与知识推理三大要素。知识抽取目的在于获取并识别源数据，并在其基础上挖掘数据之间的关系，在深度学习方法的驱动下，实现“去人工化”；知识融合阶段目的在于通过本体的、数据的融合做到实体对齐，实现非机构数据之间的深入关联；知识推理部分的重点在于通过逻辑规则、分布式特征、深度学习进行信息的整合，形成知识。[3] 知识图谱技术主要以 RDF、图数据库的方式表达知识，该种方式便于对复杂关联信息的查询与表示。

以数据安全风险评估制度为例，平台建立的风险评估制度讲究以法律法规、行业标准等规范为参考，对数据处理全流程的风险进行持续性的自

[1] 参见魏国富、石英村：《人工智能数据安全治理与技术发展概述》，《信息安全研究》2021 年第 2 期。

[2] 参见谷镇：《大数据环境下个人信息安全问题研究》，《情报科学》2021 年第 12 期。

[3] 参见张吉祥、张祥森、武长旭等：《知识图谱构建技术综述》，《计算机工程》2021 年 10 月 15 日网络首发。

查，这就要求相关标准的变动能及时传达并转化为内部约束。在知识图谱技术中机器学习技术的支撑下，规范的更新动态能够被实时抽取与融合，再通过其中的自然语言处理技术转换为平台内部规则，帮助平台在监管规范更新后及时响应合规要求；当然，该技术还拓展了合规的视野，如可对国内外相关规范进行知识抽取，以便数据安全经验的吸收与跨境业务的进行。又如在平台的内外监管衔接方面，相关规范要求平台形成数据处理流程报告并及时传输至监管机构，以满足监管机构把控平台数据安全风险态势的要求，确保网络平台运营的实时合规。知识图谱技术有助于智能化报告的生成，其结构化表达方式将数据处理流程可视化，便于监督主体进行直观的审核，在出现数据安全事件时，也能很好地呈现事件与处理流程的关联性分析，减轻了数据安全审计的人力投入，优化了数据安全合规信息的沟通程序。

3.助力数据安全管理合规：区块链技术

平台管理正处于一场颠覆性的变革之中，具有典型科层制的商业智能模式出于滞后性、资源消耗大、容错率高等缺陷，逐渐被具备扁平化结构的智能商业模式所取代，一种“众创”式数据安全管理模式逐渐成形。为满足数据安全相关规范规定的持续性合规要求，平台须严格对数据全生存周期的管理，实时把控数据访问权限，对数据业务进行动态监管，在提升数据安全防护能力的同时，建立数据安全事件应对预案，依据反馈机制进行合规维护。平台管理理念的转变、数据安全合规要求的提高推动着数据安全管理模式升级，区块链技术的引入在加快这一进程的同时，实现了数据安全的分布式管理，为动态管理提供了支撑技术，避免了由“管理不当”引发的平台违规风险。

自2008年“中本聪”提出比特币概念，其经历了让大众怀疑到成为主流流通货币的巨大转变，以太币、瑞波币等加密数字货币的陆续出现预示着“货币4.0时代”的到来。区块链技术作为数字加密货币的核心技术，突破了传统上以个人、制度等第三方为核心的信任建立模式，通过分布式数据库、共识机制、智能合约和密码等技术提供完全技术化的、去中心化的信任机制。区块链技术的本质是一种不依赖第三方、通过自身分布式节点进行网络数据的存储、验证、传递和交流的一种新型技术模式，[1]其可追溯、不

[1] 参见王兆君、王钺、曹朝辉编著：《主数据驱动的数据治理：原理、技术与实践》，清华大学出版社2021年版，第351页。

可篡改、去中心化的信任建立、多方共同维护等特性，[1]对促进数据安全管理合规具有重大意义。

第一，区块链用于数据安全存储。首先，区块链技术通过共识机制拓展了数据共享的主体范围，在一定程度上减少了平台对重要数据和敏感数据收集的必要性，从根源上避免了存储上述数据时的安全风险。其次，区块链利用链式结构来存储及验证所有采集到的数据信息，其分布式存储方式使得数据均匀分布在各个节点上，对数据的控制、维护都在各节点上进行，提升了系统的容错率，有效避免了以往集中存储方式中的数据安全风险。最后，区块链技术使得底层数据处于封闭状态，即对时间、处理、更新等数据信息进行密码学方式的保障，以此避免权限外的违规访问。在涉及数据各方之间采用非对称加密技术，可以更好地划分角色，更加精细化划分数据的操作权限，保障数据隐私安全。[2]

第二，区块链促进数据流通共享。一方面，区块链内的数据流通方式可被概括为“点对点的无中介传输”，其背后是共识机制在发挥作用，即节点之间的交换需遵循固定的、公开的、默认的、有效的算法，将数据流通的信任功能交由区块链技术的程序规则发挥，实现信任最小化，完成数据传输的双方甚至不用公开其身份，降低了“人为因素”在建立相互信任上的作用，也避免了造假、欺骗、出尔反尔等行为对数据安全造成的威胁。另一方面，区块链上的智能合约技术为数据的传输、共享提供了安全保障。数据共享的安全风险重灾区在于权限之外的非法访问，而智能合约技术通过编码以数字形式呈现出协议双方的权利义务，并由计算机系统自动执行，在实际操作过程中部署了访问控制策略，实现数据共享的自动化。

第三，区块链助力数据安全审计。正如制度架构部分所述，数据安全审计的关键在于记录完整的数据操作流程，包括操作主体、内容、时间等信息，以便监督主体进行核查。区块链技术的数据可溯源性表现在为每一类数据建链的同时，数据的来源、权属、数据的操作者、对数据的操作内容（更新、访问下载等）、当前时间戳等都会形成一个区块接入链式结构。区块在共识机

[1] 参见陈性元、高元照、唐慧林等：《大数据安全技术研究进展》，《中国科学：信息科学》2020年第1期。

[2] 参见范灵俊、洪学海：《政府大数据治理与区块链技术应用探析》，《中国信息安全》2017年第12期。

制下生成，数据处理记录是所有参与者认可的、透明的、可追溯的，对数据的全生命周期都“有迹可循”。区块链中的数字时间戳技术讲究将接收到的数据信息与接受的时间信息加密到该文件中去，以此形成数据签名，发挥了实时记录时间的功能；另外由独立于数据处理双方的认证单位DTS负责时间戳的添加，保证了时间记录的准确性、可信性。[1]

结　语

云计算、物联网、大数据等信息技术的兴起对网络平台的运营进行着“创造性破坏”，在促进数据流通，盘活数据价值的同时，使得数据安全风险不断升级、影响逐步扩大、危害程度更加严重。作为典型网络平台的网约车平台，常发个人信息被滥用、泄漏等数据安全问题，其根源在于既有保护机制存在不能有效预防风险、不能及时识别危机、不能积极应对安全事件的局限。数据安全相关法律法规、国家标准陆续出台，合规性审查逐渐被提上重点监管日程，敦促着平台积极治理数据安全问题，保障数据主体权利。建设日常性数据安全合规治理体系将有利于上述局限的修复，是实现网络平台数据安全治理的重要途径。制度架构与信息技术是构成该闭环体系的两大组成部分，呈现出“技术驱动制度，制度回馈技术”的智能商业态势，有利于实现数据安全的自动化合规。如何科学地建立制度架构，处理科技与制度架构的关系，将成为未来网络平台数据安全合规治理的重要议题。

Compliance Governance of Network Platform Data Security

—Take the Personal Information Security of the Car-hailing Platform as the Object

Ma Mingliang　Shu Xin

Abstract: There is a risk that personal information will be leaked or abused in the operation of the online car-hailing platform with a large

[1] 每个数据块都携带着可信时间戳，这个好处应用到数据管理当中可以帮助准确记录数据的产生、交换、转移、更新、开发利用整个过程。参见周晓垣：《区块链时代：数字货币意味着什么》，天津人民出版社2018年版，第96页。

amount of personal information. The existing protection mode of personal information security of online car-hailing platform shows some defects in practice, such as unable to effectively prevent security risks, unable to identify security crises in time, unable to actively respond to security incidents and so on. In order to effectively prevent and respond to data security incidents, balance the circulation value and security value of data, and ensure the sustainability of the platform's profit, a daily data security compliance governance system with incentive, real-time performance and effective connection between the internal and external supervision functions of the platform is ready to emerge. The system is a closed-loop system composed of institutional framework and information technology. At the system design level, it includes data security risk assessment system, data security compliance organizational structure, internal data security management system, regular data security compliance training and data security audit system. At the level of information technology, the introduction of emerging technologies such as differential privacy technology, knowledge map technology and blockchain technology plays a role in preventing personal information security risks, reducing the burden of compliance governance, helping data security management compliance, and improving data security compliance governance capability. The scientific operation of the closed-loop system determines the effectiveness of the compliance plan, which is conducive to gradually realizing the automation of data security compliance.

Key words: platform governance; car-hailing platform; personal information security; government supervision; data security compliance