Open Journal of Legal Science 法学, 2021, 9(6), 663-669
Published Online November 2021 in Hans. http://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2021.96095

Hans汉斯

“滴滴”安全审查视角下的公民数据安全保护

石飞杰

宁波大学法学院，浙江 宁波

收稿日期：2021年11月2日；录用日期：2021年11月19日；发布日期：2021年11月29日

摘　要

对于滴滴的网络安全审查，一方面折射出数据时代下的新形式的国家安全危机，另一方面也体现着国家对公民数据安全的重视程度。数据交易不可避免的与公民个人信息保护产生冲突。国家相继出台了《数据安全法》、《个人信息保护法》等法律规定，作为对这一问题的积极回应。对于个人信息权益保护与网络平台数据利用的协调发展应清晰的界定何为敏感性信息，明确非经权利人同意不得采集个人信息，并为个人信息数据提供数据权保护，从而切实保障公民个人权益，尊重人格尊严与自由。

关键词

《数据安全法》，《个人信息保护法》，网络安全审查，数据交易

Citizen Data Security Protection from the Perspective of “DiDi” Security Review

Feijie Shi

Faculty of Law, Ningbo University, Ningbo Zhejiang

Received: Nov. 2nd, 2021; accepted: Nov. 19th, 2021; published: Nov. 29th, 2021

Abstract

With regard to DiDi’s network security review, on the one hand, it reflects the new form of national security crisis in the data age, and on the other hand, it also reflects the state’s attention on citizens’ data security. Data transactions are inevitably in conflict with the protection of citizens’ personal information. The country has successively promulgated the “Data Security Law”, “Personal Information Protection Law” and other legal regulations as a positive response to this issue. For the coordinated development of the protection of personal information rights and the use of online platform data, it is necessary to clearly define what is sensitive information, make it clear that personal information cannot be collected without the consent of the right holder, and provide

文章引用: 石飞杰. “滴滴”安全审查视角下的公民数据安全保护[J]. 法学, 2021, 9(6): 663-669.
DOI: 10.12677/ojls.2021.96095

data rights protection for personal information data, so that the personal rights of citizens can be effectively protected and the dignity and freedom of the person can be respected.

Keywords

***Data Security Law*, *Personal Information Protection Law*, Cyber Security Review, Data Transaction**

1. 滴滴网络安全审查事件

1.1. 基本事实介绍

2021 年 6 月 30 日，滴滴出行在美国纽约证券交易所挂牌上市，股票代码为“DIDI”，发行定价为 14 美元，位于 13~14 美元/ADS 的发行区间上限。

7 月 2 日晚，国家互联网信息办公室下设的网络安全审查办公室发布《对“滴滴出行”启动网络安全审查的公告》：为防范国家数据安全风险，维护国家安全，保障公共利益，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对“滴滴出行”实施网络安全审查。为配合网络安全审查工作，防范风险扩大，审查期间“滴滴出行”停止新用户注册。这是国家首次对企业启动网络安全审查。

1.2. 对滴滴网络安全审查事件的评析

滴滴在国家强化网络安全管控背景下在美国纽交所低调上市，旋即触发了网信办的网络安全审查。事件不断发酵，从下架滴滴 APP 到下架滴滴旗下 25 款 APP 全家桶，一直到 7 月 16 日包括公安部、国家安全部在内的七部门进驻滴滴进行网络安全审查。这意味着滴滴公司极有可能已经涉嫌刑事犯罪，可能涉及的罪名包括境外窃取、刺探、收买、非法提供国家秘密、情报罪，侵犯公民个人信息罪等。对此本文暂不做讨论。

滴滴被执行网络安全审查程序的可能原因主要包括以下两个方向：

1、关键信息基础设施的运营者

关键信息基础设施主要指的是电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统。关键信息基础设施运营者的认定方法，即由关键信息基础设施保护工作部门认定。关键信息基础设施保护工作部门主要包括公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的主管、监管部门，具体来说包括工信部、发改委、交通运输部、水利部、中国人民银行、银保监会、证监会、国防部等。

2、数据安全问题

滴滴出行因其业务需要而掌握了道路交通数据(测绘数据、车流人流数据、汽车充电网的运行数据等数据)。2021 年 5 月 12 日发布的《汽车数据安全管理若干规定(征求意见稿)》第三条对汽车行业的重要数据进行了界定。滴滴出行掌握的道路交通数据等，很可能属于该规定界定的汽车行业的重要数据。如果该等数据出现了安全问题，其可能直接影响国家安全、公共利益和社会稳定，如此便与公告所述的“防

范国家数据安全”形成对应。

对于滴滴的网络安全审查，一方面折射出数据时代下的新形式的国家安全危机，另一方面也体现着国家对公民数据安全的重视程度，随着个人数据信息采集的大面积开展，以及数据交易活动的蓬勃发展，公民的数据信息安全面临着巨大的挑战，《数据安全法》正是国家层面对于这一问题的回应。

2. 大数据时代下的公民个人信息数据安全

2.1. 对数据交易活动的界定

2015 年 4 月 15 日，全球首个大数据交易平台贵阳大数据交易所正式运营[1]。贵阳市大数据交易所官方网站显示，贵阳市大数据交易所公开进行交易的交易内容不是底层数据，而是数据清洗、建模、分析的数据结果。对原始数据进行清洗、建模、分析，挖掘出数据价值后的结果数据，是对基础数据收集、加工处理、分析得出的结论或数据产品、可视化的数据结果，是在大量原始数据的基础上，通过新的科学技术得出的二次数据，反应出事物之间新的关联性。

对于数据交易中的交易双方而言，其实现数据价值的方式的可能性是多种多样的，在现阶段，笔者认为进行数据交易的主要方式可以概括为两大类：一是两家或以上的具有商业性目的的数据持有方交换各自掌握的数据信息，进行数据整合，进而提升原有的数据价值；二是商业公司通过获取潜在客户信息或政府信息等，以达到拓展客户范围，改进客户服务质量等直接或间接地提升自身业务营收的目的。

大数据时代正在兴起，大数据流通交易才起步，源头数据、可视化数据结果等各种各样产品的具体的大数据表现形式都是数据交易中的主要交易对象。与此同时，各类数据交易产品也正处在源源不断的开发过程中。

2.2. 数据交易活动与公民个人信息权益的冲突

所谓的大数据，不可避免的与个人信息数据具有密切相关的联系。个人信息数据留存于人们日常生活中的各个领域。人们在日常的社会生活中自然而然的形成各种法律关系，同时也在产生着各类与个人相关的信息数据。个人的生活住址、出生年月、工作单位、个人健康等内容，如果这些数据可以被毫无约束地使用和交易，个人的人格权利将遭受极大的冲击，人格尊严和隐私权益将会面临极大的威胁。如果对于数据交易中的公民个体的权益保护有所松动，将会使得法律在信息社会中产生信任性危机。

数据交易合法性的质疑主要来自于对数据权利主体合法权益损害的担忧，如何解决个人权利保护和数据商业化交易之间的冲突，是解决这一问题的关键所在。信息时代数据的流通具有必然性，但一味的对个人数据进行严格限制，又可能使得数据对于人们社会生活、企业经济发展所带来的价值和利益受到减损。如何区分地涉及隐私信息的个人信息数据就成为至关重要的一个环节。

2.3. 个人隐私信息的区分标准

我国学界普遍认同以识别性标准作为区分方式，即以能否借以识别个人身份的信息数据作为个人隐私信息的区分标准。但是有关于此并未有较为系统详细的理论论证[2]。且识别性标准在司法实践中也并不常用，大多数相关的案件判决中都没有直接提及身份识别的认定问题，而是简单地给予判定的结果。检索相关的法律判决书可以发现法院并未对身份识别性给予足够的司法裁判视角的描述，多为引述关于个人信息的概念。

国外有做出对敏感信息的范围进行列举式规定的立法尝试，但列举式的立法选择的明显缺点就在于其覆盖范围的不周延。对此的通常解决办法是为此增加兜底性条款。而选择兜底规定作为补充，就又会造成认定标准范围的模糊，数据交易方在获取法律明确列举为敏感数据以外的其他数据时，仍然需要对

其是否属于敏感数据进行个别判断，从而增加了数据的收集成本和合规风险。这样的区分方式对于司法实践的帮助并无较大意义。

我们认为，对于数据的区分，不应当是非此即彼的机械性判断，而应当区分不同的规制需要，考察各类数据要素，进而做出合法合理的分类。具体的评价判断体系的构建还需要包括立法部门、学界、商业公司、数据交易所等在内的各方主体共同努力。

为解决这一问题，《数据安全法》明确定义了数据、数据活动、数据安全等相关名词的概念。通过数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放等核心内容的规定，确立了国家坚持维护数据安全和促进数据开发利用并重的原则，凸显出数据安全制度建设的重要性，并确定了在开展数据活动中不同主体的数据安全保护义务。同时也体现出国家对政务数据安全与开放的重视程度。

构建数据安全保护体系的重要意义不言自明。如前所述，建设数据安全保护体系，首先需要明确数据的业务范畴，建立数据分类分级制度。同时也应当建立起与之配套的数据安全监管与风险预警体系，全方位的保障大数据时代各类具有法律权益的数据安全。随着《数据安全法》《个人信息保护法》的正式发布实施，将与《网络安全法》形成从数据、网络数据、个人信息三个维度构建数据安全保护体系，也必将对各个依托于数据交易运营的行业提出更高的数据监管与合规要求，进而实现数据产业发展与数据安全法律体系相互协调发展的数据时代新格局。

3. 互联网时代下的公民个人信息数据保护

3.1. 我国数据安全保护体系的建设

1、人脸识别国家标准征求意见稿

人脸识别国家标准征求意见稿要求，收集人脸识别数据时应征得数据主体明示同意，不得利用人脸识别数据评估或预测数据主体的工作表现、经济状况、健康状况、偏好、兴趣等情况。数据主体授权人脸识别后仍可在明示停止使用功能、服务，或撤回授权等情况下，要求数据控制者删除人脸识别数据或进行匿名化处理。人脸识别数据原则上不应共享、转让，若因业务确需如此，则应按照相关规定开展安全评估，并单独告知数据主体共享或转让的目的、接收方身份、接收方数据安全能力、数据类别、可能产生的影响等相关信息，征得数据主体的书面授权。对于人脸图像，开发商应在完成验证或辨识后立即删除，如果希望存储，需要经过数据主体单独书面授权同意。在公共场合收集人脸识别数据时，应设置数据主体主动配合(指要求数据主体直视收集设备并做出特定姿势、表情，或者通过标注“人脸识别”的专用收集通道等)的人脸识别机制，以防范人脸数据在不知情的时候被收集，保障数据主体的知情同意权。

人脸识别国家标准征求意见稿要求，应提供除人脸识别外的其他身份识别方式供用户选择，不应因用户不同意收集人脸识别数据而拒绝数据主体使用基本业务功能等。同时还对进行人脸识别的开发商提出了技术资质门槛，要求其具备相应的数据安全防护和个人信息保护能力，数据控制者应具备相应的数据安全防护和个人信息保护能力，能够防护呈现干扰攻击。呈现干扰攻击主要包括使用人脸照片、纸质面具、人脸视频、人脸合成动画、仿真人脸三维面具等攻击和干扰人脸识别，借此防范此前媒体多次报道的利用“活照片”破解刷脸技术的漏洞。

此外，人脸识别国家标准征求意见稿还特别提到了“原则上不应使用人脸识别方式对不满十四周岁的未成年人进行身份识别”。

2、《数据安全法》

2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议表决通过《中华人民共和国数据安全法》。

《数据安全法》明确定义了数据、数据活动、数据安全等相关名词的概念。通过数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放等核心内容的规定，确立了国家坚持维护数据

安全和促进数据开发利用并重的原则，凸显出数据安全制度建设的重要性，并确定了在开展数据活动中不同主体的数据安全保护义务。同时也体现出国家对政务数据安全与开放的重视程度。

构建数据安全保护体系的重要意义不言自明。如前所述，建设数据安全保护体系，首先需要明确数据的业务范畴，建立数据分类分级制度。同时也应当建立起与之配套的数据安全监管与风险预警体系，全方位的保障大数据时代各类具有法律权益的数据安全。随着《数据安全法》《个人信息保护法》的正式发布实施，将与《网络安全法》形成从数据、网络数据、个人信息三个维度构建数据安全保护体系，也必将对各个依托于数据交易运营的行业提出更高的数据监管与合规要求，进而实现数据产业发展与数据安全法律体系相互协调发展的数据时代新格局。

3、《个人信息保护法》

2021 年 11 月 1 日，《中华人民共和国个人信息保护法》正式施行。《个人信息保护法》的正式发布和施行，强化了对公民个人信息的系统保护，从法律层面对各类侵权行为加以禁止，同时进一步完善了个人信息保护投诉及相关举报工作机制，为破解个人信息保护工作中的难点提供了强有力的法律支撑。

《个人信息保护法》要求处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式；在公共场所安装图像采集、个人身份识别设备，应设置显著的提示标识；所收集的个人图像、身份识别信息只能用于维护公共安全的目的；个人信息处理者在利用个人信息进行自动化决策过程中，不得对个人在交易价格等交易条件上实行不合理的差别待遇等。

作为具有较强针对性的法律规定，对于个人信息处理的一般规则做出了较为具体和全面的规定。《个人信息保护法》较为系统和具体的对个人信息权益的范围、行使及保护措施进行了规定，随着其正式施行，可以与《民法典》中人格权内容相互呼应，更加全面有效的对个人信息权益进行保护。

3.2. 互联网时代下个人信息权益保护与网络平台数据利用的协调发展

互联网时代，不仅在大数据时代背景下，网络用户的个人信息极易被侵害，这已成为现实生活中不可回避的问题。互联网的普及和应用，一方面给人们的日常工作生活带来了极大的便利，即使足不出户，依旧能够通过互联网满足自己大部分的日常工作生活需求；但另一方面也给我们的社会带来了许多新的问题与挑战，网络社会中的公民隐私问题尤为明显。

以人脸识别为例，其在金融、交通、人社、医疗等等行业均得到广泛地落地应用，创造了巨大的社会以及经济价值。但同时，人脸识别信息不易改变，一旦丢失可能永远失去，是个人敏感信息的一种。人脸识别数据滥采、存储、使用方面没有明确的安全要求，安全防护措施薄弱，未经用户明确授权或超范围使用人脸信息的情况普遍存在。

本文认为，对于个人信息权益保护与网络平台数据利用的协调发展应从以下几个方面入手：

1、敏感性信息的明确界定

解决个人信息权益保护与网络平台数据利用之间的冲突，首先应该解决的问题就在于如何区分地涉及隐私信息的个人信息数据。我国学界普遍认同以识别性标准作为区分方式，即以能否借以识别个人身份的信息数据作为个人隐私信息的区分标准。但是有关于此并未有较为系统详细的理论论证。且识别性标准在司法实践中也并不常用，大多数相关的案件判决中都没有直接提及身份识别的认定问题，而是简单地给予判定的结果。检索相关的法律判决书可以发现法院并未对身份识别性给予足够的司法裁判视角的描述，多为引述关于个人信息的概念。

国外有做出对敏感信息的范围进行列举式规定的立法尝试，但列举式的立法选择的明显缺点就在于其覆盖范围的不周延。对此的通常解决办法是为此增加兜底性条款。而选择兜底规定作为补充，就又会造成认定标准范围的模糊，数据交易方在获取法律明确列举为敏感数据以外的其他数据时，仍然需要对

其是否属于敏感数据进行个别判断，从而增加了数据的收集成本和合规风险。这样的区分方式对于司法实践的帮助并无较大意义。

本文认为，对于数据的区分，不应当是非此即彼的机械性判断，而应当区分不同的规制需要，考察各类数据要素，进而做出合法合理的分类。具体的评价判断体系的构建还需要包括立法部门、学界、商业公司、数据交易所等在内的各方主体共同努力。

2、非经权利人同意不得采集个人信息

如人脸识别国家标准征求意见稿中的规定一般，应对互联网平台、互联网经营者等进行明确，必须经过自然人同意方可采集信息。而同意条款不得违反格式条款的法律规定，应该以醒目的字眼、用突出的或不同的字体尽说明解释义务，让自然人知道自己的信息正在被采集，并引起足够的重视。同时需要加强个人信息数据问题的宣传教育，提高个人信息权保护的意识。

有学者认为，《民法典》第 111 条规定了一项以保护“控制个人信息传播”为目的的个人信息权。控制个人信息传播的意义在于塑造“他人眼中的自己”，是个体自由发展人格的组成部分，该利益因此不同于其他利益，具有独立性和内在重要性。由“控制个人信息传播”的性质所决定，在信息主体“知情同意”的前提下，他人的个人信息处理行为具有合法性。个人信息权有其内在限度，《民法典》第 111 条对控制个人信息传播利益的保护并非绝对。在未经信息主体许可的条件下，如果处理他人信息的行为的理由在分量上超过信息主体控制个人信息利益，同样具有合法性。

3、个人信息数据的数据权保护

随着现代信息技术的快速普及应用，大数据时代已经到来。大数据技术深刻地改变了人们的生活，同时也给公民个人隐私权保护带来了巨大的冲击和影响，隐私侵权隐患无处不在。如何规范各种应用场景下的人脸识别，还有很长的路要走。现实生活中，还会存在“数字弱势群体”，其权利以“权利束”形式呈现，主要包括隐私权、知情权、个人信息权和数据权以及其他社会发展权利，需诉诸规范立法完善保障体系[3]。

信息时代背景下的一个突出特点就是信息数据的作用和价值愈发突出，个人信息可能伴随着数据价值，且我国《民法典》也已经将数据列为财产。此时，个人信息权保护便过渡到了数据权保护。随着科技的飞速发展，信息网络触及到人们生活的方方面面，政府、企业甚至于公民个人都可能会在网络工作生活环境中涉及到他人隐私。加强对公民个人信息权利的保护，并不意味着对与公民个人信息相关的行为完全禁止，否则将给社会的发展与进步带来极大程度的阻碍。“大数据隐私权规范内容的高度不确定性，不仅导致其无力直接规范大数据处理活动中的隐私风险，更引发了立法、司法和执法领域的一系列问题。大数据隐私权不确定性的形成既有规范的表层原因，也有模式方面的深层原因。只要大数据基本模式不变，大数据隐私权的不确定性就无法完全消除”[4]。

4. 小结

保护个人信息的本质意义在于对公民个人权益的保障，对人的尊严和自由的尊重。如何对公民个人信息与个人隐私进行合理区分，建立与之配套的数据安全监管与风险预警体系，进而对与公民个人信息的相关行为进行合理限制，解决大数据时代背景下隐私保护与互联网经济发展之间的矛盾，正是时代发展中面临的巨大现实挑战。

参考文献

[1] 刘霖霖. 关于人工智能时代个人信息保护研究[J]. 社会科学论坛, 2020(4): 172-178.

[2] 程啸. 论我国民法典中个人信息权益的性质[J]. 政治与法律, 2020(8): 2-14.

[3] 于柏华. 处理个人信息行为的合法性判准——从《民法典》第111条的规范目的出发[J]. 华东政法大学学报, 2020, 23(3): 81-93.

[4] 刘泽刚. 大数据隐私权的不确定性及其应对机制[J]. 浙江学刊, 2020(6): 48-58.