法学进展
2024 年 4 月第 6 卷第 2 期

数据安全保护的法律应对
——从行政处罚案件展开

罗　洁　马晓洁

上海政法学院，上海

摘　要 | 大数据安全的问题涉及个人、社会和国家安全，行政处罚作为保护数据安全的一个法律领域，与数据安全的治理目标相契合。因此，行政处罚是数据安全的保护和规制的重要领域之一。然而，由于数据的虚拟性、规模性、无限可复制性和资产性等特征，数据安全方面的行政处罚规制与传统实体场景的规制不同，导致其规制路径缺乏系统性。因此，可以适用行政法的基本原则，借鉴比较法上的经验等，构建适应数据安全保护与规制的法律体系。

关键词 | 数据安全；行政处罚；个人信息安全；数据保护

随着大数据、物联网和人工智能时代的到来，网络上产生了大量的数据。自古以来，人类就使用编绳等方式来记录数据。人类可以从数据中获得信息，从信息中获得知识，并将其应用于实践中，以促进社会进步。然而直到计算机和网络的普及，网络上才产生了大量的数据，其中包括但不限于消费数据、行

作者简介：罗洁，上海政法学院硕士研究生，研究方向：宪法学与行政法学；马晓洁，上海政法学院，硕士研究生，研究方向：宪法学与行政法学。
文章引用：罗洁，马晓洁．数据安全保护的法律应对——从行政处罚案件展开［J］．法学进展，2024，6（2）：101-112.
https://doi.org/10.35534/al.0602009

车数据、商业数据和工业数据等。这些数据规模庞大，且可以无限复制。对这些数据进行分析可以获得新的数据，从而形成了现在的大数据时代。在数据时代，大数据的重要功能是培训人工智能，同时发展数据产业可以发现新的经济增长点。此外，政务数据的开放和共享亦是值得关注的领域，有学者主张政务信息的共享和个人信息保护密切相关[①]。

在大数据时代，数据规模巨大，如在滴滴全球股份有限公司行政处罚案中，滴滴公司违法处理个人信息数量上亿条，这种海量数据是在互联网出现之前难以想象的。然而，该案件也凸显了数据安全保护的相关问题，其中包括数据泄露、侵犯隐私、非法获取信息等方面的问题。数据安全保护关系到人权的保障[②]，也关系到社会和国家安全。同时，大数据的发展需要在保护个人信息的同时，促进数据经济的发展，通过数据分析提供精准的公共治理和服务，从而提升治理效率。因此，为了促进安全与发展的协同发展，需要在兼顾数据安全的基础上，强化数据利用的保护和规范。

一、数据安全保护的相关立法

数字经济的建设与大数据密切相关。一方面，需要促进数据产业的发展；另一方面，也需要规范新出现的数据安全问题，以保障数据的安全。随着大数据浪潮的到来，数据安全问题备受关注。新出现的数据市场带来了需要治理的新问题。而行政处罚是处理数据泄露等问题的重要路径，保护和规范数据安全也成了行政处罚法现代化的一部分。

关于数据安全的分类，存在着多种不同的观点，例如将数据安全等同于个人信息安全、将数据安全等同于数据资产安全、将数据安全等同于公共安全，或者综合以上观点的多元论。本文采多元论的观点，即数据安全是个人信息安全、网络数据安全和公共数据安全等的综合。

2017 年，我国实施了《网络安全法》，该法规定了与数据安全保护相关的条款。

① 邢会强．政务数据共享与个人信息保护［J］．行政法学研究，2023（2）：68–81.

② 徐玖玖．利益均衡视角下数据产权的分类分层实现［J］．法律科学（西北政法大学学报），2023，41（2）：67–81.

例如，网络经营者应当履行数据保护的义务，防止网络数据泄露、窃取或篡改。此外，该法还对违法向境外提供网络数据的行为作出了相应的处罚规定。而《个人信息保护法》自 2021 年起正式实施，这部法律也对个人信息处理者的处理义务进行了规定，并明确了对违法处理个人信息行为的处罚。

我国于 2021 年开始实施《数据安全法》，该法将数据安全定义为“通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力”。同时，《数据安全法》中提出了保障数据的合法利用和自由流动以促进数字经济发展。这表明数据的发展需要同时注重数据的利用和安全两方面，一方面需要促进数据的利用以发展数据经济，另一方面也需要保护数据的安全以防止出现个别或甚至规模化的安全风险。该法规定了与数据安全相关的违法行为的处罚措施。

二、数据安全相关的行政处罚案件

随着大数据技术的发展，数据侵权案件越来越频繁。这些案件可以分为两类：一类是涉及违法获取或利用个人信息的行为，另一类是涉及数据安全的违法行为。

（一）侵犯个人信息安全的案件

1. 滴滴案件

滴滴公司因为违法收集信息、过度收集信息、索取无关信息、未说明信息处理目的等行为，同时存在严重影响国家安全的数据处理活动。该公司的行为违反了《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等多部法律，因此被处以八十多亿元的罚款。此案例是一个从严从重处罚的典型案例。

2. 平安保险六盘水中心支公司泄露个人信息案件 [①]

本案的当事人“案防管理不到位，原职工利用职务便利泄露在业务活动中

① 参见中国银行保险监督管理委员会六盘水监管分局行政处罚决定书：六银保监罚决字〔2022〕9、10、11、12、13号。

https://doi.org/10.35534/al.0602009

知悉的投保人、被保险人的个人信息”，依据《保险法》第一百六十一条，被处以罚款十万元。同时，该案实行双罚，直接责任人员被处以禁止进入保险业三年等处罚。

3. 房地产公司违法采集个人信息案件

第一，扬州某房地产公司违法采集个人信息案件[①]。当事人扬州某房地产开发有限公司在其项目售楼处安装了智能人像抓拍机，用于识别来访客户的人脸信息，主要目的是确认客人的身份。然而，该售楼处未向被推荐的客人或进入售楼处的自然访客告知其有人脸识别机器。行政机关依据《消费者权益保护法》第 29 条的规定，对当事人处以罚款，理由是其未经消费者同意采集消费者个人信息。

第二，嘉兴某房地产公司违法收集个人信息案[②]。本案当事人在事先未向消费者明示并经同意的情况下，通过“人脸识别”技术收集消费者信息，且没有明示收集、使用该信息的目的、方式和范围。根据《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题（法释〔2021〕15 号）》第四条、《消费者权益保护法》第二十九条第一款、《侵害消费者权益行为处罚办法》第十一条第一款第（一）项等，当事人应被依法处以罚款。

（二）数据泄露方面

依据《数据安全法》的规定，当事人如未履行数据安全保护义务，将会受到相应的处罚；而若造成了大量数据泄露等严重后果，则不仅要接受行政处罚，还可能构成犯罪并被追究刑事责任。因此，数据泄露案件可以分为存在泄露风险的案件和已经造成数据泄露的案件。

1. 存在数据泄露风险的案件

第一，上海首例根据《数据安全法》罚款的数据安全案件，因为有数据泄露的风险，并没有实质性的泄露，被处罚款并给予警告。

第二，山东数据安全处罚首例案件。山东某一家公司因在对个人信息相关

① 参见扬州市邗江区市场监督管理局行政处罚决定书：扬邗市监处罚〔2021〕182号。

② 参见桐乡市市场监督管理局行政处罚决定书：桐市监处罚〔2022〕749 号。

的数据的存储中，没有采取安全的防护措施，违反了《数据安全法》第二十七条的规定，即这一个企业应当建立健全数据安全的管理制度并且采取相应的措施保护数据安全。被行政机关给予了警告的处罚并责令改正。这也是山东省首例依据《数据安全法》进行行政处罚的案件。

第三，郴州的数据泄露案件[①]。当事人未制定相应方案，未制定保障数据安全制度，未分级分类，未开展年度常态化技术检测，未履行数据安全保护义务。该案中的当事人未履行数据安全保护的义务。数据处理者应当采取技术措施和其他必要措施保障数据安全，防止数据泄露、毁损、丢失等情况发生。因此，当事人未履行数据安全保护的义务，需要承担相应的法律责任。

第四，盘锦银行股份有限公司数据泄露风险案[②]。当事人因敏感数据信息存在泄露风险等行为，根据《银行业监督管理法》第四十六条，被处以罚款。

2. 数据已经泄露的案件

第一，上海警方侦破一起侵犯大型游戏著作权案。2022 年 7 月，上海警方宣布侦破一起侵犯大型游戏著作权案，该案的犯罪嫌疑人在未取得权利方授权的情况下，利用从报案公司挖来的员工非法窃取的游戏代码架设网游推广牟利，侵犯了他人的著作权。该案中的代码属于数据，犯罪嫌疑人窃取数据的行为已经触犯了刑法。

第二，滨海县双盛燃气有限公司案[③]。该当事人篡改隐瞒直接关系生产安全的相关数据信息的违规行为。违反了《安全生产法》第三十六条第三款，被处以罚款。

三、数据安全法律保护的困境

从上述数据安全类行政处罚的案件来看，从《数据安全法》实施以来，和数据安全相关行政处罚的案件数量还不多，但在处罚上呈现以罚款为中心。从这些案件之中看出，数据安全的法律保护主要存在以下几个方面的问题。

① 参见郴州市公安局白露分局：白公（白）决字〔2023〕第0019号。
② 参见辽宁银保监局：辽银保监罚决〔2022〕89号。
③ 参见苏盐滨住建罚决〔2023〕8号。

https://doi.org/10.35534/al.0602009

第一，当前行政处罚的处理重心在于保护前端的数据，包括数据违规收集、数据侵权和数据泄露等方面。然而，对于数据后续的流动安全方面的保护较为缺乏，例如对数据的违规交易的处罚等。而数据产生的经济效益主要取决于后续的数据流通，但目前尚未有完善的关于数据后续流通的保护措施。此外，数据具有无限复制性，加上数据使用之后会产生新的数据，对后续产生的这部分新数据仍然需要法律来进行保护和规制。

第二，在处罚种类中，虽然也存在适用警告、竞业禁止等处罚方式的情况，但更多的数据安全处罚案例仅适用罚款这一种处罚的方式。然而，仅靠罚款是否能够达到警示的作用是存在疑问的。如果数据违法所获得的利益大于罚款的数额，那么从成本的角度来看，很难完全遏制信息泄露的问题。

第三，处理自然人相关的数据要先确认数据的所有权，而在海量的大数据面前，这一确认工作变得十分困难。因此，目前收集或处理自然人信息相关数据时，需要事先获得知情同意。然而，在自然人授权知情同意的过程中，当事人通常只是简单地点击了同意按钮，而并未充分注意到已经授权同意。此外，自然人授权了信息之后，如果后续信息处理者使用该信息进行分析得出新的数据，进而带来商业利润，那么提供原始信息的自然人是否可以获取部分收益，这是值得研究的。

第四，不同行业的数据内容不同，但现在缺乏不同种类的数据保护标准。数据分级分类管理是确保数据安全的重要一环，有学者主张将数据分级分类作为数据安全保护的基本法律原则[①]，为数据安全的法律保障提供指引。例如，能源数据和企业的经营数据就存在区别，能源数据涉及国家的能源安全和发展，其涉及较多的重要敏感数据，应适用不同于一般数据的安全保护法律规范。

第五，企业数据合规的不充分性。首先，部分企业还没有建立起完整的数据合规体系，对企业运营中收集到的数据及处理的数据，没有进行定期的审查。其次，关于企业数据合规的法律规范较为分散，这增加了企业关于数据合规内

① 刘冰．我国能源数据安全法律规制研究［J］．政法论坛，2023，41（2）：48–59.

容的不确定性。[①] 此外，在司法的适用上，认定存在数据安全违法行为时，因为网络数据的虚拟性，如何识别存在数据泄露的风险，以及在数据已经泄露了之后如何认定损失的大小，这都是需要研究的问题。

第六，数据资产化保护相关的法律供给不足。数据资产化即数据成为可以带来收益的资产。数据资产化的前提是数据确权的明晰化，即数据的所有权或使用权要明晰。例如，个人信息授权信息处理者使用之后，要明晰个人信息的所有权的归属问题。明晰的产权可以促进数据的流通以及可以带来新的经济增长点。但现行的法律对于数据资产的隐私保护和安全保护还未完善。数据确权的相关规则存在争议，未形成一致的观点[②]。

四、域外经验借鉴

（一）美国

1. 立法

在美国联邦方面的法律，尽管《美国数据和隐私保护法》草案已于 2022 年提出，但该法案受到了一定的阻碍。而在美国州层面，以《加州消费者隐私法》（CCPA）为典型的法律主要保护个人数据，赋予消费者知情权。该法案规定了企业必须明示收集的数据类型和使用目的，消费者有权了解其数据的收集情况和去向，并有权拒绝企业出售其数据。消费者可以要求企业披露并删除自己的数据，企业不能因消费者不同意数据处理而拒绝提供服务。消费者可以选择退出其个人信息的销售，企业必须提供相应选项。此外，未成年人的信息必须获得明确的授权才能销售。在数据侵权发生时，消费者只有在某些情况下才能起诉企业并要求罚款，例如仅适用于可以识别个人身份的信息泄露情况。对于大多数数据泄露情况，只有总检察长才能提起诉讼。

① 胡玲，马忠法．论我国企业数据合规体系的构建及其法律障碍［J］．科技与法律（中英文），2023（2）：42–51.

② 刘冰．论数据资产化的法律障碍及破解路径［J］．中国法律评论，2023（2）：51–63.

https://doi.org/10.35534/al.0602009

2. 数据泄露的诉讼

目前国内许多学者认为，要保护和治理数据安全，主要需要依靠行政监管。而在美国这个民商法诉讼非常发达的国家，民商法诉讼已经成为保护个人信息的主要途径，包括个人起诉企业索赔和集团诉讼两种方式。

美国数据泄露案件涉及的处罚和和解金额比较大。2019 年 9 月，美国联邦贸易委员会（FTC）宣布，谷歌及 YouTube 违反儿童隐私法，谷歌将支付一亿多美元罚款。2019 年 2 月，Tiktok 因收集儿童个人信息受罚五百多万美元。2021 年 2 月，TikTok 与美国用户就数据隐私问题达成和解，同意支付九千多万美元的集体诉讼和解金。

（二）欧洲

1. 立法

《一般数据保护条例》（GDPR）是欧盟于 2018 年制定的条例，其中对数据违法行为进行了严格的处罚。

2. 数据泄露的处罚案例

2020 年 10 月，英国航空公司因泄露客户数据，被英国数据安全监管部门罚款两千万英镑。

2020 年 10 月，HM 公司因收集和使用员工的信息超出了最小化原则，被德国汉堡的数据保护机构“数据保护及信息自由委员会”处以三千多万欧元的罚款。

2022 年 11 月，由于泄露用户的数据，爱尔兰数据保护委员会对脸书（Facebook）处以上亿欧元罚款。

在《一般数据保护条例》的适用下，欧盟对数据泄露事件的处罚金额相对较高。同时，《一般数据保护条例》的实施使得欧盟对于数据保护问题的监管更加严格，企业也提高了对数据保护的重视程度。

五、数据安全的法律应对模式

（一）行政法原则的适用

尽管《行政处罚法》的法律条款中尚未明确对于数据安全违法行为的处罚，

该类案件主要适用《数据安全法》等法律来规制。但数据违法案件涉及领域广泛且科技发展较快，即便在《行政处罚法》中增设一类规范，可能仍无法涵盖所有数据安全的违法行为。在这种情况下，可以适用行政法的原则来指导案件的解决。比如行政法治原则、依法行政原则、法律保留原则和比例原则等。

（二）多种处罚方式并行

现行关于数据安全的行政处罚主要适用罚款这一种类。而处罚过重可能不利于行业的发展，能承受额度较高罚款的企业往往是大企业，这容易导致垄断的形成[①]。因此，在适用罚款的行政处罚之外，可以适用警告、降低资质等级等其他的行政处罚种类。根据不同的数据违法行为，适用不同的处罚方式，更好地做到数据保护和处置违法的平衡。

（三）部门法之间协同发展

对于数据安全违法行为，如果仅适用行政处罚来应对，那反映出缺乏其他法律例如民商法的协同适用。而且，法律存在着滞后性的特征，一旦制定出来就可能落后于社会生活的发展。在大数据时代，大数据增长非常迅速，导致数据安全案件的数量和种类也在不断增加，某些案件往往无法仅仅用单一的一部法律去规范。因此，应协同发展不同的部门法来应对数据安全的事件。

涉及数据安全的案件还有民事侵权案件、行政处罚案件和刑事犯罪案件。民事案件有知识产权侵权、对个人信息泄露的侵权等。民事侵权中，构成对他人人身、财产权益的侵害，数据处理者需要承担侵权赔偿责任[②]。行政处罚案件中，处罚的主要方式是罚款。而刑法上关于数据违法犯罪的罪名包括非法获取计算机信息系统数据罪等。

（四）数据跨境流动的监管

数据的跨境包括数据出境和数据入境两个方面的数据流动，涉及国内法和

① 王玎．论数据处理者的数据安全保护义务［J］．当代法学，2023，37（2）：40–49.

② 程啸．论数据安全保护义务［J］．比较法研究，2023（2）：60–73.

https://doi.org/10.35534/al.0602009

国际法两个方面的法律。有学者指出，应当“尽快厘清重要数据的范围和出台重要数据出境安全评估制度，以明确我国数据出境的‘负面清单’”[①]。本文作者认为，应当加强国际合作，构建全球数据安全的监管模式。在存在数据争议时，积极寻求司法途径解决。在数据出境方面，企业要积极进行数据合规和报备，在合法合规的范围内促进数字经济的发展。在现行我国区分重要数据和个人信息跨境流动的模式下，跨境数据监管方面凸显出事前监管和备案的重要性。

（五）企业数据合规的完善

企业生产经营所涉及的数据包括企业收集到消费者信息、员工信息，以及企业生产经营所产生的数据，比如便利店每个时间段客流量的数据、游戏公司开发游戏的代码数据等。这些数据中的一部分涉及知识产权，适用知识产权法律来保护。但更多的数据安全都可以适用《数据安全法》来保护。同时，企业在进行数据分析时，要注重保护个人的隐私数据。在数据合规中重视个人信息保护、数据安全和商业效益之间的动态平衡。[②] 此外，企业应当建立数据分级管理制度，履行法律要求的义务以防止数据泄露。

（六）数据安全保护的其他应对方式

第一，根据不同的应用场景，细化数据安全保护措施。第二，建立数据安全的问责制度。第三，建立数据安全的公益诉讼制度。第四，发展数据流通、利用的保护与规制。数据经济离不开数据流通、利用和分析。经济发展、科技发展与数据保护的平衡发展。第五，重视敏感数据和重要数据的认定和保护。

六、结语

数据是商业上的资产，企业应加强内部数据安全设置，全周期全链条地建

① 刘金瑞．迈向数据跨境流动的全球规制：基本关切与中国方案［J］．行政法学研究，2022（4）：73–88.

② 胡玲，马忠法．论我国企业数据合规体系的构建及其法律障碍［J］．科技与法律（中英文），2023（2）：42–51.

设数据安全，而非仅在事后进行补救。同时，企业应站在更高的角度看待数据的社会和国家安全价值。而在数字社会中，我们仍应当反思其中隐藏的数据安全风险，若仅仅追求数据的运行效率，可能会发生个体无法预料和抵御的风险。[①] 此外，数据的安全涉及个人的数据和信息权益，应当保障个人的救济权，允许相关的个人对信息授权进行撤回和更新等，建立健全个人信息侵权的救济机制。

目前已经有许多省份颁布了关于数据安全方面的法律规范性文件，这表明了全国数据市场发展的迫切性。从另一个方面来看，数据地方立法的差异化，不一定有助于构建全国统一的数据大市场，因此这需要加快全国性的数据法律制度供给。[②]

而行政处罚作为数据安全保护领域的重要法律，在数据泄露等案件中发挥了重要的作用。数据安全保护涉及的领域较广，数据需要实行分类分级保护，这需要多领域法律相结合进行治理。在数据安全治理方面，公法和私法应当加强协调合作，以保障数据安全保护和数字经济发展两方面取得新进展。

① 郑晓军．反思公共数据归集［J］．华东政法大学学报，2023，26（2）：53–67.

② 时建中．数据概念的解构与数据法律制度的构建 兼论数据法学的学科内涵与体系［J］．中外法学，2023，35（1）：23–45.

https://doi.org/10.35534/al.0602009

The Legal Response of Data Security Protection
—From the Administrative Penalty Cases

Luo Jie Ma Xiaojie

Shanghai University of Political Science and Law, Shanghai

Abstract: The problem of big data security involves personal, social and national security. As a legal field to protect data security, administrative punishment is in line with the governance goal of data security. Therefore, administrative punishment is one of the important areas of the protection and regulation of data security. However, due to the characteristics of data as virtual, scale, unlimited replicability and assets, the regulation of administrative punishment in data security is different from that of traditional entity scenarios, resulting in the lack of systematic regulation path. Therefore, the basic principles of administrative law can be applied, and the experience of comparative law can be used to build a legal system adapted to data security protection and regulation.

Key words: Data security; Administrative penalty; Security of personal information; Data protection