Open Journal of Legal Science 法学, 2023, 11(3), 1445-1451
Published Online May 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.113206

Hans汉斯

大数据时代的个人信息法律保护之完善研究

刘　闯

浙江理工大学法政学院、史量才新闻与传播学院，浙江　杭州

收稿日期：2023年2月27日；录用日期：2023年3月15日；发布日期：2023年5月25日

摘　要

在网络大数据时代，各种网络工具在给人们的生活提供便利化的同时，也在其他层面暗藏着影响个人信息安全的潜在性威胁。特别是各种网络安全事件的不断发生与演变，恰恰印证了这些威胁的现实性和规制的紧迫性。大数据时代下个人信息法律保护方面存在网络后台监管不力、数据信息等级保护不够、责任主体与划分标准不明、公民个人信息安全意识不强的问题。对此可以通过细化专项监管立法、完善个人信息等级制度、明确责任主体与划分相关制度、提高全社会网络安全意识等方式加强和完善个人信息法律保护，以期尽快打造和优化符合我国网络发展特点的个人信息法律保护体系。

关键词

大数据时代，个人信息，专项立法，等级制度，提高意识

Research on the Perfection of Personal Information Legal Protection in the Age of Big Data

Chuang Liu

School of Law and Politics, Shi Liangcai School of Journalism and Communication, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: Feb. 27th, 2023; accepted: Mar. 15th, 2023; published: May 25th, 2023

Abstract

In the era of network big data, all kinds of network tools not only provide convenience for people's lives, but also hide potential threats affecting personal information security at other levels. In particular, the continuous occurrence and evolution of various network security incidents just con-

文章引用: 刘闯. 大数据时代的个人信息法律保护之完善研究[J]. 法学, 2023, 11(3): 1445-1451.
DOI: 10.12677/ojls.2023.113206

firm the reality of these threats and the urgency of regulation. In the era of big data, there are some problems in the legal protection of personal information, such as weak network background supervision, insufficient data information level protection, unclear responsibility subject and division standard, and weak awareness of citizens' personal information security. Therefore, we can strengthen and improve the legal protection of personal information by refining the special supervision legislation, perfecting the personal information hierarchy system, clarifying the responsible subjects and dividing the relevant systems, and raising the awareness of network security in the whole society, so as to build and optimize the legal protection system of personal information that conforms to the characteristics of China's network development as soon as possible.

Keywords

Era of Big Data, Personal Information, Special Legislation, Hierarchical System, Strengthen the Awareness

1. 引言

近年来，频频爆出的网络安全事件，凸显了网络大数据时代下的个人信息安全与保护问题。比如，2022 年 7 月 21 日滴滴巨额罚款事件冲上网络热点事件榜单，即滴滴平台因存在一系列危及个人信息安全的违法行为，在被有关部门进行网络安全审查时发现并依法对其作出“高额”的处罚决定；这些违法行为包括违法收集用户截图、过度收集用户应用列表信息、过度收集用户人脸识别信息、过度收集用户定位信息、收集用户出行意图等等。[1] 2019 年 11 月轰动一时的“人脸识别第一案”，起因是杭州野生动物世界人脸识别系统单方任意升级涉及其个人信息的修改，恶意增加不必要的服务等侵犯其个人信息安全，被作为消费者的浙江理工大学特聘副教授郭兵博士告上了法庭，最终法院站在了维护个人信息安全的正义一方。[2] 2019 年高校秋季开学阶段，一些高校收集和使用学生在校信息借以开展高校正常生活秩序，但在收集、使用学生相关信息时因数据信息处理后台的漏洞导致学生信息泄露，学生进出校园显示校园黑户的智慧校园管理事件[1]。

在司法实践中，每年也有大量因滥用个人信息侵害公民合法权益的案件。特别是在涉及公民征信信用、隐私信息等方面，不法人员借着网络信息系统存在的漏洞与间隙，通过多种手段和形式危害公民的个人信息安全[2]。比如，2022 年 7 月 23 日的一则热点新闻“咸阳一居民投诉乱倒垃圾后信息遭泄露”，该居民举报乱倒垃圾现象，在举报部门相关人员调查后却泄漏了其私密信息，反遭被举报人的事后威胁。[3] 再如 2022 年 6 月 22 日郑州通报的“储户红码事件”，部分银行储户在毫不知情的情况下，健康码一夜转红，这种对个人信息的任意滥用，严重影响到个人的正常生活。[4]

综上所述，网络安全问题在网络大数据时代需要进行重点研究，特别是在涉及到与个人切身利益紧密关联的个人信息的保护方面。如果不严以对待，个人利益受损的恶果叠加，最终也会进一步扩展到危及社会安全上至国家安全的层面[3]。

[1] 来源于人民网，2022.07.21. (http://finance.people.com.cn/n1/2022/0721/c1004-32482072.html)。
[2] 来源于光明网，2019.11.04. (https://legal.gmw.cn/2019-11/04/content_33289644.htm)。
[3] 来源于澎湃新闻网，2022.07.25. (https://www.thepaper.cn/newsDetail_forward_19161623)。
[4] 来源于搜狐网，2022.06.23. (https://www.sohu.com/a/560304430_115571)。

2. 网络大数据时代的个人信息法律保护中的问题与缺陷

2.1. 对网络后台运行漏洞的监管不力

在前文提到的滴滴巨额罚款事件中，滴滴平台因为其存在一系列危害乘客个人信息安全的违法行为事实被相关部门处罚。经仔细分析可以发现，滴滴平台的这些行为违反了《网络安全法》、《数据安全法》、《个人信息保护法》等相关法律。[5] 这些行为背后的 APP 后台未经正常程序收集用户信息、未经许可随意跟踪乘客出行轨迹等问题，所触发的都是网络运行后台管理安全的缺陷。比如，对 APP 后台软件的运行安全没有具体限制，对于运行漏洞的监测识别也没有固定标准等等。

我国当前的网络安全法律体系是建立在 2016 年通过的《中华人民共和国网络安全法》的基础上的。在此基础上，有关部门相继出台颁布了一系列配套法规、规章和规范性文件，如《数据安全法》、《网络信息内容生态治理规定》、《个人信息保护法》等。这些文件构建起涉及网络运行安全、个人信息保护和网络内容管理等三个方面的网络安全法律体系[4]。但目前的网络安全法律体系建立的框架系统并没有细化到针对网络后台漏洞监管做出详细规定。比如，《网络安全法》第二十二条、第二十五条规定在应对网络运行安全问题时采用应急预案、采取补救措施等，却并没有提供明确的方案或要求。《网络产品安全漏洞管理规定》第八条对网络运营者的义务性规定和针对其他相关主体的其他规定也只是概括性定义，没有具体细化相应的监管职责。[6]

故此次滴滴巨额罚款事件所暴露出的重要问题在于，当前网络安全法律体系对网络后台运行安全漏洞仅仅作出了相对概括的指导措施，并没有详细规定如何具体加强漏洞监管以及具体的责任承担。由于缺少强力的监管措施，滴滴旗下的各种网络平台得以借助现存网络漏洞，利用或非法收集网络用户的个人信息，对其个人信息安全产生严重威胁。同时，对网络运行安全的监管不力也会导致其他网络产品在今后的网络生活中借机作乱，衍生出侵害网络用户个人信息的新问题，危及网络用户的个人信息安全。

2.2. 数据和信息等级保护体系不完善

结合近两年发生的智慧校园事件、人脸识别案等网络安全事件，可以发现，在实际纠纷中，类似于智慧校园、人脸识别这些事件实际上是分属于不同类别的数据信息安全纠纷。比如，智慧校园网络服务产品主体针对对象是学生群体，而人脸识别大多用于商业、企业以及公司等组织性群体。实际针对对象不同，会使网络服务产品的性能以及使用也会有所差别。在发生具体实际纠纷时，对收集的信息仅按群体进行分类，缺乏对实际应用的网络产品以及支撑其运行的后台系统的分类分级和对应管理，会产生措施采取不当的问题，导致不能妥善处置相关网络安全事件带来的具体损害。这在另一方面也会实际影响到对个人信息安全的专有保护。

对于数据和信息等级保护制度，我国《网络安全法》第二十一条对网络安全等级保护制度作了简要概括性规定，并在第三十一条中明确对公共通信、信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域的数据信息实行重点保护。《数据安全法》第二十七条也规定在进行或者开展数据处理活动时应当按照法律规定的流程和安排有条不紊地实施，以确保数据信息的安全性等等。[7] 通过这些法律条文可以看出，现有立法关于网络安全下的数据和信息等级保护的规定，主要是对数据信息等级保护制度作出法律定义以及指导性规制。

[5] 来源于人民网，2022.07.21. (http://finance.people.com.cn/n1/2022/0721/c1004-32482072.html)。

[6] 《网络产品安全漏洞管理规定》第八条规定，网络运营者发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证并完成修补。

[7] 《中华人民共和国数据安全法》第二十七条规定，开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

而前面对智慧校园案件、人脸识别案件的分析，结合我国目前的相关立法实践，凸显出目前关于数据信息等级保护存在的问题，即虽然我国立法涉及数据信息等级保护，但在如何对数据信息系统进行分层管理以及采取何种措施实施等级保护方面却缺乏应有的细节性规定。这就导致了不同数据信息的混乱管理，从而引发个人信息安全事件的发生。

2.3. 责任主体和责任划分的标准不明

据不完全统计，2021 年，全国公安机关共侦办侵犯公民个人信息、黑客攻击破坏等案件共 6.2 万余起，同比增长 10.7%，抓获犯罪嫌疑人 10.3 万余名，同比增长 28.7%。[8] 由此可见，个人信息滥用案件每年层出不穷。前文提及的举报乱倒垃圾事件、储户被赋红码事件，也正是个人信息被滥用的代表性案件。这些个人信息安全事件的发生，很大一部分是源于掌握公民个人信息的相关个人信息收集者、处理者利用法律规制的漏洞来借机侵害他人的个人信息安全。对责任主体以及责任划分的规定不明确，导致责任承担的主体最后可能并没有落在违法者个人身上，是助长这些实际责任主体不法心态的症结所在。

我国现有相关立法对网络安全事件的责任主体和责任承担方面仅仅做出了概括性的规定，缺乏确定责任主体以及相应的责任划分的具体适用依据。《网络安全法》第六章、《数据安全法》第六章、《个人信息保护法》第七章对法律责任作出了相关规定，涉及网络运营者、网络产品或服务的提供者或者国家机关以及其他个人以及组织在侵害他人个人信息安全的情况下的责任承担。比如，《数据安全法》第四十九条规定了对国家机关主管人员相关违法行为进行处分的情形；《个人信息保护法》第六十九条明确了个人信息处理者危害个人信息安全时遵循过错推定的侵权法律责任，等等。[9] 然而，这些规定较为宏观，具有一定的指导性，但缺乏细致具体的适用条件和主体确定等内容。

如果不能做到精确打击违法行为者、让他们切实承担应有的法律责任，就无法进一步遏制和消除他们的违法而不自知的放纵心态，形成对个人信息持续性滥用的社会态势。这将严重损害和危及公民个人信息的安全与保护。

2.4. 公民个人信息安全法律意识淡薄

就国家层面而言，相关部门一直在努力为完善个人信息保护实施诸如立法等活动，借以实际行为强化对个人信息安全的保护。如前文提及的针对网络后台的监管、数据等级保护制度、责任主体承担职责等方面，目前立法实践都有涉及[5]。但是，仅仅依靠国家社会层面的努力是远远不够的。如果忽视对利益群体自身的安全意识教育，不能从根本上改变公民个人网络安全法律意识淡薄的症结，那么将不能从根本上消除祸患之源。就如滴滴巨额罚款事件中，个人信息未经用户授权被任意收集等凸显出公民个人信息安全意识匮乏，因此危及到个人信息的安全与保护。

个人信息安全与保护的问题在网络大数据时代一直是社会关注的焦点问题。我国近年来已连续出台一系列法律法规以期不断加强和着力于对个人信息的保护，也构建起了一套不断加以完善的网络安全法律体系。但更值得注意的是，个人信息安全与公民个人切身利益息息相关，如果作为利益所有者的公民个人缺少自保的武器，就好比釜底抽薪，失其根本，再多的外力也不能解决根症所在[6]。

3. 加强和完善个人信息法律保护的对策与建议

在目前我国大数据时代的网络环境下，如何解决网络安全事件中所涉及的个人信息安全与保护方面及其存在的一些问题，是影响公民个人正常网络信息生活、确保个人信息安全的关键。现结合国外相关

[8] 来源于人民政协网，2022 年 01 月 14 日(http://www.rmzxb.com.cn/c/2022-01-14/3028017.shtml)。

[9] 《中华人民共和国数据安全法》第四十九条规定，国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。《个人信息保护法》第六十九条规定，处理个人信息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。

的立法实践与经验，提出如下建议与对策。

3.1. 细化专向监管立法，弥补网络后台漏洞监管不力的缺陷

网络后台漏洞问题涉及的是网络运行安全方面，但影响的却是我们个人信息的安全与保护，必须给予应有的重视。当前我国逐步构建起了涉及网络运行安全、个人信息保护和网络内容管理等三个方面的网络安全法律体系。在这个法律体系的大框架中，作为漏洞监管方的网络运营者和其他相关主体，现有立法对其监管义务仅只是做了指导概括性的规定，对于具体如何实施监管以及怎样落实监管的措施却规制的不够明确和完整。滴滴巨额罚款事件也正是折射这个问题的代表事件之一。

对于此，作为信息化强国的美国采取了不同的做法。2021 年 11 月，美国的国土安全部网络安全与基础设施安全局发布了《网络安全事件与漏洞响应指南》。漏洞响应指南的发布意味着美国在今后应对网络安全事件和漏洞时能有一套标准程序手册作为依据，从而能够有效开展对网络安全事件及漏洞的监测、识别、处理以及上报等活动。这也说明美国作为当今世界的大国强国之一，在信息化时代，网络和信息安全俨然已成为其国家安全的重要组成部分。漏洞响应指南在安全事件等级划分、响应程序、监测识别、漏洞修补、事后记录等方面也做出了详细规定，形成了一个系统完整化的针对网络安全事件中涉及网络漏洞方面的应对战略体系[7]。

故针对网络漏洞监管，可以借鉴美国的有利经验，对于后台漏洞的监管进行专向细化性立法，采取具体可行的措施对网络后台漏洞进行监管，比如纳入分布式监测管理的具体措施、充分利用分布式监测管理技术等。通过这些技术和措施能让网络安全人员及时发现各种网络后台安全漏洞的问题，当漏洞被检测出来时，服务器系统会自动生成事先利用算法技术构建的防御体系，保护网络后台服务器，避免个人信息被盗取，确保个人信息的安全性等[8]。这样在完善对后台漏洞。

3.2. 强化数据信息分层级管理，完善个人信息等级制度

数据信息的等级保护亦需强化与重视。通过对当前一些热点网络安全事件的分析发现，在数据信息等级保护相关制度体系方面，我国目前的相关法律并没有作出详细的分等级监管的规定，因此影响到个人信息的安全与保护。2013 年 7 月 10 日，国家档案局发布的《档案信息系统安全等级保护定级工作指南》，对我国档案管理相关部门有效地开展非涉密信息系统安全等级保护定级工作，并对工作原则、内容等方面的释明，提供了相应的制度依据[9]。

但该指南主要针对的对象是非涉密的档案信息，而对于在具体实际中涉及到多方利益群体不同的私密信息方面，我国目前的相关立法并没有建立起相对较完整的法律应对体系。指南提供的针对数据信息等级保护方面的指导意义就在于，在今后的立法层面，应持续加强和增加对数据信息实行等级分层化管理方面的规定，对不同利益群体以及不同网络信息系统进行层级细化。与此同时，对不同层级的数据信息持续开展网络安全等级保护测评，使企业、高校学生群体抑或是个人，都能有相对应的具体的数据信息等级保护措施。通过这些实际措施保证信息系统安全稳定运行、数据合法合规获取和利用[10]，这也将有利于增强对我们公民个人信息安全的专有化保护。

3.3. 细化相关部门的具体职责，明确责任主体与责任划分的相关制度

对于相关部门负责的问题，从前文叙述中可知我国《网络安全法》、《数据安全法》、《个人信息保护法》等仅做了概括性规定，而对于相关部门具体的负责范围以及各部门如何配合缺乏明确具体的针对性内容[11]。

前文提到，目前我国网络安全法律体系所涉及的几个不同板块，主要包括网络安全运行、个人信息

保护和网络内容管理等。可以看出，不同的板块所涉及的利益相关体亦有所不同，且针对不同的部分更是需要不同的部门履行各自相关的职责，落实相关责任。网络安全事件中具体责任主体的确定与相关责任划分缺乏具体依据的问题，得以让不法者借助法律的漏洞结合网络系统的漏洞对个人信息进行不断的侵害。

与之不同的是，在英国的相关立法实践中，英国将有关网络安全的相关部门进行了细化，构建了多层次、多方位的部门分管与合作体系，对网络安全政策体系的规制也更全面细致[10]。此外，美国在网络安全治理方面，例如前文所提及的《网络安全事件与漏洞相应指南》中，也强调国家有关部门与企业、事业单位以及其他组织的通力合作，多方位共同合作，以应对和解决网络安全事件[11]。

因此，对责任主体与责任划分方面存在的不足之处，可以借鉴英美等国家的有益经验，进行专项对应布防。比如，通过细分不同的职能部门进行专事专办，对于国家省市等不同地域级别划分出相应的不同的专职部门。下一级职能部门具体负责细化相关网络安全的标准，同时对于上级网络安全职能部门的指令加以贯彻执行，落实网络安全战略的宏观目标，惩治违反网络安全的具体行为等等。以此来确保个人信息安全与保护能确切落到实处[12]。

3.4. 聚集各方面力量，共同提高全社会网络安全意识

网络安全事件下的各种网络安全危险和挑战，从表层看涉及的是对多种网络安全问题的防御和应对以及解决，但其深层次的影响是关乎公民个人利益的保护。公民作为个人利益所有者，更要明白打铁还需自身硬的道理，若自身没有自卫的能力，即使赋予再多的外部盔甲，也终将被击溃。

网络安全意识的培育即是目前急需发力的要点之一。在这个方面，英国的做法值得借鉴。英国在 2021 年 12 月和 2022 年 1 月接连发布的《2022 年国家网络战略》和《2022~2030 年国家网络安全战略》等文件中，全面分析了英国当前所面临的一系列网络安全风险环境，并通过分析提出构建网络生态应对持续变化的一系列举措，将网络安全意识提高到文化的高度[12]。此外，英国另一方面还制定了完善的网络安全人才培养机制，先后出台了《网络安全知识体指南》、《信息安全保障专业人员认证框架》、《连接世界的教育框架》、《未成年人网络安全计划》等一系列针对网络安全专业人才培养方面的文件，以期借助于高端人才培养优势来助力与对网络安全事件的应对与处理[13]。

而反观我国有关方面的立法实践，对于网络安全意识的培育以及对网络安全专业化人才的培养方面的规定还略显匮乏。为此，应学习借鉴国外的有利经验，采用深层次、多方位、高效能的方针政策。比如发挥政府部门在网络安全意识培养方面的主导作用；持续加强对网络安全专业人才培养机制的构建；把提升网络安全意识作为国家网络安全战略部署实施等。同时应加强对国民的网络安全意识和防范水平教育，大力开展网络安全知识的相关普法宣传工作，使社会公众对网络安全引起必要的重视，将以往的被动性预防转化为主动性预防。借助汇聚社会各方面力量的优势，全方位加强提升公众的网络安全意识，从而真正提高公民个人对抗网络风险的能力。

4. 结语

身处瞬息万变的网络大数据时代，到处都交织遍布着多种多样的网络安全威胁，各式各样的网络安全事件也在层出不穷的上演。一系列的网络安全事件也时刻警示着，个人信息安全在如此错综复杂的环境下，随时可能遭受不期而来的危害。

本文通过介绍一些时下热点，包括滴滴违法收集用户个人信息被罚款、动物园任意升级信息系统侵害个人信息安全的“人脸识别第一案”以及高校学生信息被滥用等网络安全事件，分析探究出我国目前应对网络安全事件特别是当下个人信息安全与保护事件的法律体系所存在的诸如网络后台漏洞监管不力、

数据信息等级保护不完善、责任主体以及责任划分规制不明和公民自身网络安全意识不强等问题与不足之处。在立足于当前我国制定的应对网络安全事件的法律框架之下，并在参照英美等国外的相关立法实践与经验的基础上，研究得出如下建议与对策：一是细化专向监管立法，弥补网络后台漏洞的监管不力；二是强化数据信息分层级管理，完善个人信息等级制度；三是细化相关部门的具体职责，明确责任主体与责任划分的相关制度；四是聚集各方面力量，共同提高全社会网络安全意识。希望本研究能在为更好地维护我国网络安全大环境下落实对个人信息安全与保护方面发挥一点建言献策的功效，以期进一步构建完善我国网络安全应对防范机制，切实维护好个人信息安全。

参考文献

[1] 杨峰, 郭巍, 孙海亮, 关兴卓. 智慧校园背景下高校网络信息安全管理与服务研究[J]. 网络安全技术与应用, 2021(12): 81-82.

[2] 杨立新. 侵害公民个人电子信息的侵权行为及其责任[J]. 法律科学(西北政法大学学报), 2013, 31(3): 147-152.

[3] 周加海, 邹涛, 喻海松. 《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》的理解与适用[J]. 人民司法, 2017(16): 35-40.

[4] 方禹. 2021 年国内网络安全相关立法回顾及思考[J]. 中国信息安全, 2021(12): 48-52.

[5] 王利明. 数据共享与个人信息保护[J]. 现代法学, 2019, 41(1): 45-57.

[6] 东力力. 我国法律对个人信息安全保护的现状与完善[J]. 法治与社会, 2020(24): 7-8.

[7] 李艳霄. 美国《网络安全事件与漏洞响应指南》解读[J]. 信息安全与通信保密, 2022(1): 45-50.

[8] 姜可. 我国网络安全运维存在的隐患及改善策略[J]. 无线互联科技, 2022, 19(3): 19-20.

[9] 刘珂. 《档案信息系统安全等级保护定级工作指南》的主要内容及思考[J]. 北京档案, 2022(3): 21-25.

[10] 史宝虹. 高校网络安全等级保护的研究[J]. 信息与电脑(理论版), 2018(10): 182-184+187.

[11] 侯东德, 姚万勤. 美国网络安全战略及其对我国的启示——兼论我国《网络安全法》的规定及未来的完善[J]. 人工智能法学研究, 2019(1): 77-89.

[12] 王磊, 杨锐, 刘金琳. 英国网络安全治理体系研究[J]. 网络安全技术与应用, 2022(4): 38-41.

[13] 陈伟. 英国网络安全意识教育主要做法及启示[J]. 中国信息安全, 2022(1): 131-132.