公司治理视域下个人信息保护的实现路径——以《公司法》第 147 条的具体化为中心

The Enforcement Approach of Personal Information Protection from the Perspective of Corporate Governance：Centered on the Concretization of Article 147 of the Company Law

张怀岭

ZHANG Huailing

【摘　要】　我国现行个人信息保护法律规范存在体系化弊端。保护路径选择上具有强烈规制法、管理法色彩，缺乏对企业内部合规机制建构的关注，导致法律实施的内生性、持续自律机制运行不畅。德国《数据保护法》、欧盟《通用数据保护条例》的立法例和司法实践表明，个人信息保护的实现有赖于与公司内部治理机制的制度对接。对接的实现路径便是法定义务的内部化，即将法定个人信息的保护义务内化为公司董事（对公司）的勤勉义务（合法义务）。内化机制构建的逻辑起点是个人信息保护义务的法理定位。而内化机制构建的重点则是个人信息保护义务作为董事勤勉义务的具体化。诉讼主体资格、举证责任风险的分配以及损害赔偿额的惩罚性则是激活内化机制司法适用性的关键。

【关键词】　个人信息保护　公司治理　勤勉义务　合法义务

【中图分类号】DF59　【文献标识码】A　【文章编号】2095－9206（2018）05－0021－13

Abstract：There are systematic defects in the current legal norms of personal information protection in China. The choice of protection approaches depends heavily on public and regulatory instruments and lacks attention to the construction of internal compliance mechanism，resulting in poor operation of the endogenous and continuous self-discipline mechanism of law enforcement. The legislation and judicial practice of the German Data Protection Law and the EU General Data Protection Regulations show that the realization of the protection of personal information depends on the internal corporate governance mechanisms. The key instrument is the internalization of the legal obligation，which internalizes the protection obligation of the statutory personal information into the diligence obligation（legal obligation）of the company director（to the company）. The logical starting point of the internalization mechanism is the legal characteristic of personal information protection obligations. The focus of the internalization mechanism is the specificity of the personal information protection obligation as directors' duty of care and diligence. The procedural qualifications，the distribution of the burden of proof and the punitive nature of the damages are crucial to activating the judicial applicability of the internalization mechanism.

Key words：Protection of personal information　Corporate governance　Duty of diligence　Duty of legality

［收稿日期］　2018－06－17

［作者简介］　张怀岭，男，1983 年 3 月生，西南财经大学法学院副教授，研究方向为民商法、比较法。

［基金项目］　西南财经大学中央高校基本科研资助项目“非上市公司治理中董事勤勉义务规则优化与实施研究”（项目编号：JBK1801074）；四川省社会科学研究“十三五规划”2017 年度课题“四川自贸区内资企业合规风险及防范机制构建研究”（项目编号：SC17FZ020）。

一、问题的提出

2016 年山东准大学生徐玉玉学费遭电信诈骗一案以极端的方式凸显了信息网络时代个人信息法律保护的必要性和迫切性。该案更深次的原因是目前猖獗的公民个人信息泄露、滥用的规制不力。[1] 而 2013 年支付宝数据泄露事件、网商京东接连大规模信息泄露事件、[2] 雅虎 30 亿用户账号信息被泄露事件、[3] 谷歌安卓系统的手机和平板收集和分析用户位置信息丑闻，[4] 以及人工智能（AI）在人脸识别领域的巨大进步等新发展显示，[5] 大数据时代互联网企业是个人信息“最贪婪”的收集者和利用者，而且其所掌握的海量个人数据信息使其成为对个人信息最严重、最广泛侵害的“潜在源头”。[6] 以数据为基础的新经济模式在巨大经济利益的驱动下，使得公民个人在现有法律框架下难以保护个人信息免于收集、传播和再利用的风险。[7]

基于“标本兼治”的目的，本文将从比较公司治理的角度，系统梳理我国现行个人信息保护的规范体系，并指出我国现行个人信息保护规范体系和路径选择存在的缺陷。以此为基础，将着重论证如何将（外部）法定保护个人信息的义务“内化”为公司董事、高级管理人员的勤勉义务，从而为个人信息保护构建一个内生性的、低成本的私法执行机制，摆正私权（即个人信息权）保护上民商事（董事勤勉义务）法律规范的基础性地位和市场规制性、管理性法律规范以及刑事法律规范的补充地位，搭建外在的法定个人信息保护义务规范与商事主体内在行为义务之间的联动机制。

---

〔1〕“徐玉玉被电信诈骗致死案”主犯陈文辉等庭审交代，其以非常低的成本通过网络购买学生个人信息，然后实施电信诈骗。

〔2〕2015 年京东的用户信息曾遭大规模泄露。2016 年京东再次发生大规模信息泄露事件，有 12G 数据包外泄，涵盖用户名、密码、邮箱、QQ 号、电话号码、身份证号等内容，数据多达数千万条。在最高人民检察院最近发布的六起侵犯公民个人信息犯罪典型案例中，造成损害最大的都是“内部人”的违法行为。

〔3〕See Yahoo now says all 3 billion of its accounts affected by massive hack，at http：//mashable.com/2017/10/03/yahoo-hack-bigger/#Y6kUXV1Duaq2，last visited Nov. 24，2017.

〔4〕See Google collects Android users' locations even when location services are disabled，at https：//qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/，last visited Nov. 24，2017.

〔5〕例如，中国新创公司商汤科技（Sensetime）利用人工智能和大数据已经可以实现对道路上过往行人人脸和车辆的远距离识别。

〔6〕个人信息泄露已经成为消费者投诉中极为突出的问题。2017 年 11 月 Uber 公司首次承认其 5 000 万乘客和司机信息于一年前被盗，用户个人信息范围涵盖姓名、邮件和电话信息。事件发生时，该公司既未告知受影响的用户，也未向监管部门报告，而是选择向实施盗窃数据的黑客支付 10 万美元，换取黑客销毁泄露的信息。Uber räumt Datendiebstahl ein，https：//www.tagesschau.de/ausland/uber-datenklau-101.html，letzter Abruf am 28.11.2017。

〔7〕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，第 91 页。

二、我国现行法个人信息保护的路径选择及缺陷

（一）我国现行法对个人信息的保护路径

近年来，为了应对信息网络技术的爆炸式发展对个人信息保护所带来的挑战，我国个人信息保护的法律、法规体系逐渐完善。基于笔者的考察，对于个人信息的法律保护，我国立法者主要从两个基本维度来展开：（1）如何界定个人信息的法律属性；（2）如何对侵害个人信息的不法行为予以规制。互联网时代，这是各国立法者所共同面临的重大问题。前者涉及个人信息的权利属性、权利内容。如同其他民事权利一样，个人信息的“确权”应首先是宪法性规范和民事法律规范（个人信息、数据的权利属性）的任务。[8] 而对于侵害个人信息不法行为的规制则是私法规范（民商事法律法规）、公法规范（经济法、行政法规范）以及刑法规范的共同任务。针对实践中极端猖獗的侵害公民个人信息的行为，我国新近颁布、修订了相关法律、法规。

首先是一系列法律位阶较高的基本法律得以颁布或修订。其中，最为重要的确权性法律规范当属《民法总则》。作为我国未来《民法典》提纲挈领的部分，《民法总则》第五章对“民事权利”进行了专门规定。其中，第 111 条规定：“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”《民法总则》第 111 条中并未明确采用“个人信息权”这一表述，因此，学界对于其权利属性尚有争议（宪法人权、一般人格权、新型权利、隐私权以及独立人格权等）。[9] 尤为值得注意的是，《民法总则》规定，个人信息保护的义务主体涵盖了任何组织和个人，范围非常广泛。[10]

其次，针对消费者这一特殊群体，根据《民法总则》（2017 年颁布）第 128 条的规定，《消费者权益保护法》（2013 年修订，以下简称《消保法》）构成特别法，具有优先适用性。以规制消费者和经营者实质不平等地位为出发点，《消保法》同时从“赋权利”和“设义务”两个角度来保障消费者的个人信息权。其一，就赋权利维度而言，第 14 条第 1 款规定：“消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。”其二，该法第 29 条第 1 款规定：“经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。”第 2 款规定：“经营者及其工

---

〔8〕 例如，《欧盟运行条约》（AEUV）第 16 条第 1 款和《欧盟基本人权宪章》（EUGCh）第 8 条赋予个人数据以基本权利和自由的地位。欧盟《数据保护基本条例》（DS-GVO）第 1 条第 2 款也明确对自然人基本权利和基本自由，尤其是对个人数据享有的基本权利予以保护。

〔9〕 多数观点认为，《民法总则》第 111 条没有采用“个人信息权”的表述，但此条款同时具有宣示性规定和确权性规定的属性。

〔10〕 其中，“任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全”这一规定是全国人大常委会法律委员会在《民法总则（草案）》提交给全国人民代表大会第五次全体会议最后审议前，在原来三审稿基础上增加的。参见陈甦主编：《民法总则评注》（下册），法律出版社 2017 年版，第 785 页。

作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生消息泄露、丢失的情况时，应当立即采取补救措施。”第 3 款规定：“经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。”

作为侵害消费者个人信息的法律后果，《消保法》第 50 条规定，经营者应当停止侵害、恢复名誉、消除影响、赔礼道歉，并赔偿损失。再者，《消保法》针对网络交易平台规定了特殊的信息义务。消费者通过网络交易平台购买商品或接受服务，其合法权益受到损害的，网络交易平台不能提供销售者或服务者真实名称、地址和有效联系方式的，应当对消费者承担赔偿责任。此外，除了承担民事责任之外，《消保法》第 56 条第 1 款第 9 项还规定了警告、没收违法所得、1～10 倍罚款、停业整顿及吊销营业执照等行政责任。

再次，针对互联网上公民个人信息的保护问题，在《全国人民代表大会常务委员会关于加强网络信息保护的决定》（2012 年）的基础上，《网络安全法》已于 2017 年 6 月 1 日生效。《网络安全法》在附则中对个人信息进行了立法定义，[11] 即是指“以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证号码、个人生物识别信息、地址、电话号码等”。对于个人信息的保护而言，《网络安全法》第 40 条规定：“网络运营者应对其收集的用户信息严格保密，并建立健全用户信息保护制度。”该法第 42 条第 1 款规定：“网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。”该条第 2 款规定：“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。”制定中的《电子商务法（草案三次审议稿）》第 23 条通过概括性的条款规定了电子商务经营者在收集、使用其用户的个人信息时，应当遵守有关法律、行政法规规定的个人信息保护规则。

最后，《刑法修正案（九）》修订和新增了涉及非法获取、出售或提供公民个人信息的刑事责任，确立了全面保护公民个人信息的精神，[12] 并对将在履行职责或者提供服务过程中获得的公民个人信息进行出售或提供给他人的予以从重处罚。两高《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“个人信息”的法律含义以及具体涉及公民个人信息的犯罪行为的认定和量刑进行了规定。

（二）现行个人信息保护法律规范的缺陷

1.“多龙治水、众法齐下”的体系化弊端

前述法律、法规着眼点不同，对个人信息提供的保护和救济手段、方式也有显著差

---

〔11〕《信息安全技术公共及商用服务信息系统个人信息保护指南》（2012 年）以及工业与信息化部发布的《电信和互联网用户个人信息保护规定》（2013）中均对“个人信息”进行了界定。

〔12〕参见赵秉志：“公民个人信息刑法保护问题研究”，《华东政法大学学报》2014 年第 1 期，第 117～127 页。

异。这种“多龙治水”的局面，一方面是由于法律规范的位阶不同以及一般法与特别法有机结合、体系化的要求，另一方面也是源于个人信息保护所涉及法律领域的复杂性。然而，“多龙治水”的最佳效果发挥依赖于法律规范以及实施机制之间的协调、统一。由于前述各种法律规范分属不同的法律部门，在不同的时间由立法、司法（两高）或者行政主管部门颁布，在体系化上存在不协调，甚至冲突之处。例如，个人信息的“权利”为何，其与隐私权和名誉权等人格权的关系问题，[13] 并未因《民法总则》的颁布和生效而最终得以解决。[14]《网络安全法》、《信息安全技术公共及商用服务信息系统个人信息保护指南》以及《电信和互联网用户个人信息保护规定》等不同法律规范关于个人信息法律内涵的界定及其外延也不统一。相比之下，已经于2018年5月25日生效的欧盟《通用数据保护条例》（General Data Protection Regulation）第4条第1项将“信息与特定或可特定的人相关联”作为该条例适用（个人数据）的前提。[15] 不同于原欧盟《数据保护指令》的法律效力，[16] 欧盟法中的条例不需要成员国进行“转化”，而是在其全部范围内对于所有成员国具有直接的拘束力（《欧盟运行条约》第288条第2款）。[17] 因此，欧盟成员国在个人数据的范围上采用上述同一标准。而且，欧盟《通用数据保护条例》的适用地域范围不限于欧盟内部，而是采取所谓“市场地原则”，即对于欧盟外向欧盟境内以有偿或无偿方式提供商品或服务的企业也具有拘束力（《通用数据保护条例》第3条第2款第a项）。这一立法变化使得该条例具有域外适用效力，从而具备成为国际标准的潜力。[18]

2. 现行法对侵害个人信息的行为规制“公法”色彩浓厚，民商事法律规范尚未发挥应有的基础性保障功能

尽管我国学界对于个人信息的具体权利属性存在争议，但其民事权利的属性为我国学界主流观点和立法（《民法总则》第111条）所认可。现代法治社会，民事权益即私权实现的核心在于私力救济。民事法律在实现确权的同时，也为权利主体提供了权益受到侵害时的司法救济途径。德国法学家耶林在《为权利而斗争》的演讲中主张，“为权利而斗争是权利人对自己的义务……抵抗不法是权利人对集体的义务”，“只要制定法不是无用的游戏和空洞的废话，制定法就必须被维护，与受害人的权利一同陨落的是制定法本身”。[19]

然而，我国现行法律规范对于侵害个人信息不法行为的规制具有强烈的公法色彩。

---

〔13〕 参见王利明：“论个人信息权的法律保护——以个人信息权与隐私权的界分为中心”，《现代法学》2013年第4期，第62～72页。

〔14〕 参见前注〔10〕，陈甦书，第781～801页。

〔15〕 See REGULATION (EU) 2016/679, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, last visited Aug. 4, 2018.

〔16〕 Datenschutz-Richtlinie 95/46/EG (DSRL).

〔17〕 Niedobitek M (Hrsg.), Europarecht-Grundlagen der Union, De Gruyter, 2014, § 7 Rn. 16.

〔18〕 Schanz, Die Datenschutz-Grundverordnung-Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW, 2016, 1841.

〔19〕〔德〕鲁道夫·冯·耶林：《为权利而斗争》，郑永流译，法律出版社2012年版，第12～30页。

无论是体系上作为市场规制法的《消保法》，还是行政管理法色彩的《网络安全法》以及《刑法》，其中公民个人信息保护的规范都体现了国家公权力强势介入相关领域的特征。显而易见，这些具有公法色彩的法律规范被立法者作为首要的规制工具来对待。公法规范与私法规范相比，在设定权利和义务上以不对等、向信息收集主体单方面施加法律义务为主要特征。尽管这在个人信息侵犯极为普遍的情况下，具有一定合理性和必要性，但是，内在的私法保障机制相较于外在的公法保障机制更具有持续性和全面覆盖的优势。因此，笔者认为，对于私权的维护应当内化外部法定义务，发挥私法实施机制的基础性作用。

3. 缺乏对企业内部合规机制建构的关注，导致保护个人信息规范实施的内生性自律机制运行不畅

如前所述，在大数据、人工智能时代，相较于个体甚至公权力机关，对公民个人信息的收集、处理、传播能力最强的是互联网信息科技企业。[20] 实践中频繁出现的大规模、恶性个人信息侵害事件的发生，多数与互联网科技企业有关，抑或企业自身故意为之（例如，谷歌安卓系统收集和利用用户位置信息、人工智能监控软件对个人生物特征的收集），抑或企业未能采取足够的安全措施（例如，雅虎公司的用户数据泄露），抑或是企业内部人员所为（例如，京东用户数据泄露事件）。针对当前对个人信息侵害肆意泛滥的现象，我国立法者和监管者的规制路径和工具具有强烈的公法色彩，具有一定的合理性。尽管我国学者已经意识到将个人信息权界定为民事权利的重要性，倡导建立以私法保护为中心的个人信息保护体系，[21] 并且也有学者基于比较法的考察主张针对网络安全保护引入“以管理为基础的规制”，[22] 但这均未能从公司治理的角度提出可行性法律对策。

不容忽视的是，缺乏从公司治理角度将外部的以公司为义务主体的法律义务内化为公司董事、高级管理人员对公司承担的勤勉义务（和忠实义务），导致企业自身自律、合规缺乏主动性。相较于由公权力机关实施的外部监管（考虑到对利用大数据和人工智能的经营活动进行监管的难度和法律实施成本问题），企业公司治理中的内部监督、自律机制（即内部利益主体之间的监督机制）则能够以较低的成本，[23] 实现更加持续性的规制效果，也有利于鼓励权利主体积极行使自己的权利。[24]

就此而言，欧盟以及德国的立法经验和实践具有启示意义。德国《联邦数据保护法》（BDSG）于第一章“一般条款与共同条款”中规定了个人数据收集、处理和利用主体的一般行为义务和组织义务。其中，第 4f 条规定了“数据保护监察专员”（Beauftragter für den

---

〔20〕 新创公司商汤科技（sensetime）的人脸识别技术和物体识别技术便是典型代表。尽管这一人工技术可以发挥帮助抓捕逃犯等功能，但不容忽视的是其强大的个人生物信息的收集和利用能力。

〔21〕 参见前注〔13〕，王利明文，第 62～72 页。

〔22〕 参见洪延青：“以管理为基础的规制——对网络运营者安全保护义务的重构”，《环球法律评论》2016 年第 4 期，第 20 页。

〔23〕 参见徐丽枝：“个人信息处理中同意原则适用的困境与破解思路”，《图书情报知识》2017 年第 1 期，第 106 页。

〔24〕 参见前注〔13〕，王利明文，第 62～72 页。

Datenschutz）制度，即“自动化处理个人数据的公共主体以及非公主体应当以书面形式任命数据保护检查专员”。于 2016 年 4 月 27 日颁布、2018 年 5 月 25 日生效的欧盟《通用数据保护条例》除了对责任主体的采取技术措施的一般义务和组织义务进行了规定之外，还首次在欧盟层面以法定义务的形式引入了“数据保护监察专员”（Data Protection Officer）制度。[25] 另外，欧盟《通用数据保护条例》也首次为建立自律机制（行为规范）和认证机制设立了法律框架。[26] 前者类似于《公司治理准则》，属于软法机制的范畴，后者类似于“数据保护审计”，由独立第三方进行。[27]

概言之，个人信息内化机制的建立和完善不仅具有改善我国公司治理总体水平的一般意义，而且能够对个人信息保护的私法保障机制的建立发挥核心功能。以下将从公司治理的角度，对个人信息保护内化为董事勤勉义务的逻辑起点、内化机制构建的重点和关键制度进行详细论述。

三、个人信息保护义务的法理定位是内化机制构建的起点

公司治理的语境下，个人信息保护内化机制的构建必须首先厘清的问题是：（1）前述不同法律规范所设定的个人信息保护义务是否以及如何内化为公司[28]（经营者、网络服务提供者等等）内部特定主体的法律义务？以及（2）可以内化、转换为何种法律义务？

（一）公司董事、高级管理人员应当是内化后的义务主体

现代公司治理模式以所有权与控制权的分离为基本特征，公司治理中奉行“董事会中心主义”。[29] 股东在履行完出资义务之后，作为公司财产（即清理完债务后的剩余财产）抽象意义上的所有者原则上并不直接参与公司经营和管理。[30] 公司作为法人，[31] 其法定义务的履行需要经过其组织机构，即董事会、监事会和经理层来实现。鉴于我国公司治理模式中，监事会抑或上市公司的独立董事的核心功能在于监督（其他组织机构）职责的履行，因此，个人信息保护履行和实现的义务主体应是负责公司经营的董事和高级管理人员。

（二）勤勉义务应为个人信息保护义务内化的董事义务类型

比较公司法学者从功能主义的角度将企业法的功能总结为两个方面：其一，制度供给，即为企业家、创业者提供具备特定组织结构的法律形式；其二，控制和减少公司不

---

〔25〕《通用数据保护条例》第 37—39 条。

〔26〕《通用数据保护条例》第 40—43 条。

〔27〕参见前注〔18〕，Schanz 文，第 1842 页。

〔28〕不同法律规范所采用的术语也不尽相同，例如：《消保法》采用“经营者、网络交易平台”，《民法总则》采用“任何组织和个人”，《网络安全法》采用“网络运营者”，而《刑法》则完全以“行为标准”来判断。

〔29〕参见张维迎：《理解公司：产权、激励与治理》，上海人民出版社 2014 年版，第 184 页。

〔30〕Kraakman R. etc，The Anatomy of Corporate Law-A Comparative and Functional Approach，Oxford University Press，2009，p. 28.

〔31〕即便是非法人组织形式的合伙企业也大体相同。

同利益群体之间的利益冲突，即代理问题。[32] 其中，第二个方面的问题是公司治理的核心任务。而规制股东与公司管理层之间、股东与股东之间以及公司与第三人（诸如，债权人、雇员等）之间利益冲突的核心法律工具是董事、高管的信义义务（fiduciary duties）。无论是在大陆法系国家还是普通法系国家，这一义务又可以被划分为：注意义务（duty of care）和忠实义务（duty of loyalty）。忠实义务以董事高管与公司争利的行为，诸如自我交易（self-dealing）、篡夺公司机会、竞业竞争为规制对象。相比之下，注意义务（我国《公司法》采用的是“勤勉义务”的表述[33]）强调的则是董事、高管应当尽职尽责，努力实现公司利益的最大化。[34] 遗憾的是，我国《公司法》[35] 不仅没有给“勤勉义务”提供清晰的界定标准，而且也没有以列举的方式规定违反勤勉义务的典型行为类型。我国的司法实践[36]则呈现出较为明显的借鉴美国 1984 年版《标准上市公司法》（MBCA）第 8.30（a）（2）条规定的倾向。[37] 就履行个人信息保护法定义务而言，在学理上属于公司董事、高管应当履行的勤勉义务，即公司管理者应当保障公司能够切实履行法律规定的保护个人信息的义务，从而维护公司的利益，避免公司因义务不履行而遭受不利的法律后果，诸如，损害赔偿、行政处罚，甚至刑事处罚。

四、勤勉义务具体化是个人信息保护义务内化机制构建的重点

（一）董事勤勉义务具体化的比较法经验

1.“一般条款＋具体行为规范”的规制模式

基于对两大法系代表性国家制定法和判例规则的考察，[38] 笔者发现勤勉义务在大陆法系的规定采用了“一般条款＋具体行为规则”的规制模式。这一模式在 2005 年英国《公司法案》的修订中也得到了典型体现。其中，一般条款中最为核心的是勤勉义务的判断标准规则。诸如，《德国股份法》（AktG）第 93 条第 1 款、《德国有限责任公司法》（GmbHG）第 43 条第 1 款规定了公司董事在履行职责时应当尽到“谨慎、有序业务领导人的注意义务”（Sorgfaltsmaßstab eines ordentlichen und gewissenhaften Geschäftsleiters）。除此

---

〔32〕 参见前注〔30〕，Kraakman R. etc 书，第 28 页。

〔33〕《公司法》并未对勤勉义务进行立法定义，学界和司法实践主流观点认为，勤勉义务与传统民法上的“注意义务”含义一致。

〔34〕 公司利益并不等同于（大）股东利益。股东的利益可能与公司长期、稳健的经营利益相冲突。

〔35〕 我国《公司法》第 147 条第 1 款规定：“董事、监事、高级管理人员应当遵守法律、行政法规和公司章程，对公司负有忠实义务和勤勉义务。”

〔36〕 例如，北京妙鼎矿泉水有限公司诉王东春损害公司利益赔偿纠纷案，《北京市门头沟区人民法院民事判决书》，（2009）门民字第 4 号；上海川流机电专用设备有限公司诉李鑫华案，《上海市闵行区人民法院民事判决书》，（2009）闵民二（商）初字第 1724 号。

〔37〕 由于我国民法法系的传统，如何协调英美法信义义务基于信托法的特征与我国民法以委托代理理论来解释董事与公司法律关系的问题还亟待解决。

〔38〕 本文大陆法系考察限于潘德克吞法系的德国以及罗马法系的法国以及欧盟层面的制定法，包括《欧洲股份公司条例》（SE-VO）和《欧洲私公司条例（草案）》（SPE-VO）；英美法系的考察范围则限于英国法和美国的《标准商事公司法》。

之外，法律还规定了董事的一系列具体勤勉义务。诸如，申请进行商事登记的义务、[39]遵守法律关于资本履行和资本维持的义务、[40]对股东的信息义务、及时召集股东会议的义务以及公司危机情况下的特殊义务（尤其是，及时申请破产义务）。勤勉义务最核心的要求为，公司管理者在法律、章程和股东决议的框架内并在妥当考虑公共利益的基础上，追求和实现公司的利益，避免公司利益遭受损失。[41]

2．两大法系的规制模式和规则内容上的相互靠近

一个非常值得关注的现象是，两大法系董事勤勉义务（和忠实义务）规则和规制模式（制定法抑或判例规则）上从不同的出发点相互靠近。例如，在英国《公司法案》（Companies Act）修订过程中，曾对是否以及在多大的范围内将关于董事信义义务的判例规则成文法化进行讨论。最终的结果是，判例法中大量能够相对确定表述的董事信息义务规则被纳入到英国现行《公司法案》（CA 2006）中。[42]除此之外，尚有一些董事信义义务，诸如，董事对债权人的义务、法律义务以及商业判断规则。即便在这些判例规则实现成文化之后，对于相关法律条款的解释，依然应当参照相应的判例规则。[43]而作为典型大陆法系国家的德国则在制定法之外，借由法官法（Richterecht）[44]来对法典中董事义务的一般条款予以具体化。这一过程通常通过法律解释，甚至法律的续造（Rechtsfortbildung）来完成。[45]例如，源自美国公司法的商业判断规则，[46]最初通过德国的判例被司法实践所继受。此后又在逐渐成熟的基础上，最终被法典化到《德国股份法》第 93 条中。当然，这一制度对于其他法律形式，尤其是有限责任公司的可适用性依然是通过法律解释来完成的。[47]可见，无论是大陆法系国家（如德国）还是英美法系国家（如英国），判例规则对于董事勤勉义务的发展都具有核心意义。

3．勤勉义务具体化的比较法经验

比较法的公司理论上，董事勤勉义务又被划分为（1）合法义务和（2）狭义的勤勉义务。[48]合法义务是指遵守所有外部行为约束规范，来保障管理行为的合法性。这些约束性的规范不仅包括法律规定，还包括公司章程和股东决议等规范。而且，这些规范既可以公司本身作为义务主体（诸如，网络运营者的个人信息保护义务），也可以直接以公司董事、高管为义务主体。合法义务不仅要求公司高管在经营管理中考虑到企业经

---

〔39〕 参见《德国有限责任公司法》第 7 条第 1 款。

〔40〕 参见《德国有限责任公司法》第 9a、19、30、31、33、43a、57iv 条。

〔41〕 OLG Zweibrücken NZG 1999，506，507.

〔42〕 参见英国《公司法案》（CA 2006）第 173 条及以下诸条。

〔43〕 See Davies P，Worthington S，Principles of Modern Company Law，Sweet & Maxwell，2012，p. 503.

〔44〕 这是德国法对于基于判例所形成的不成文判例规则的专门称谓，并非组织法意义上的法官法。

〔45〕 参见〔德〕卡尔·拉伦次：《法学方法论》，陈爱娥译，商务印书馆 2004 年版，第 249 页。

〔46〕 参见〔美〕弗兰克·伊斯特布鲁克：《公司法的经济结构》（第 2 版），罗培新、张建伟译，北京大学出版社 2014 年版，第 93 页。

〔47〕 Zhang H，Die Rechtspflichten der Leitungsorgane der geschlossenen Kapitalgesellschaften，Dr. Kovac Verlag，2017，60.

〔48〕 同上，第 71～72 页。

营活动应当遵循的法律、法规，而且还必须采取必要、妥当的措施以保障企业的行为符合法律的要求并及时识别和防范经营过程中可能存在的法律风险。其中尤其包括相应的组织措施（如设立合规部门、配备相应人员和资源）。

下面以在德国法上有重大影响的“西门子股份公司诉纳伯格案”作为剖析样本，具体地说明合法义务的适用逻辑。[49] 该案以西门子公司长时间、大规模向海外政府官员以及个人行贿丑闻的爆发为背景。除了刑事处罚和德国、美国证券交易监管机构的处罚外，西门子公司还聘请了一家美国律师事务所来调查本公司内部的行贿“黑金系统”，并为此支付了约 1 300 万欧元律师费用。在西门子公司行贿丑闻发生后，西门子公司监事会以违反勤勉义务为由要求所有前任董事会成员向公司承担损害赔偿责任，并对唯一一个拒绝承认自己存在违反董事义务行为的董事纳伯格（负责财务管理、报告和法务部门的董事）提起 1 500 万欧元的损害赔偿诉讼。西门子公司的诉讼请求获得法院的全额支持。本案法院的司法适用逻辑在于，西门子公司的跨国商业贿赂行为不仅违反了商业道德，而且也违反了《国际商务交易活动反对行贿外国公职人员公约》在缔约国（德国）国内法上的规定，从而构成违法行为。合法义务不仅要求董事不得从事违法行为，而且还要求董事负有对董事会其他成员和员工行为进行监督的义务。这种监督义务被《德国股份法》具体化为一种组织义务，即董事会必须采取合适的措施，尤其是通过建立监督体系来及时发现威胁企业存续的状况。[50] 因此，董事只有在企业内部设立了相应的预防损害和控制风险的“合规机构”的情况下，才符合组织义务（合法义务）的要求。

（二）个人信息保护内化为董事合法义务的制度基础

我国《公司法》第 147 条规定，董事、监事、高级管理人员应当遵守法律、行政法规和公司章程，对公司负有忠实义务和勤勉义务。尽管学界对于“遵守法律、行政法规和公司章程”与“勤勉义务”的关系有争议，[51] 但依据前述比较法的主流理论，遵守法律、法规和公司章程属于“合法义务”范畴；而合法义务又属于“勤勉义务”（注意义务）的一种具体类型。合法义务要求董事、高管必须采取妥当措施保障公司遵守法律的行为约束，避免因违法而使公司遭受损失。就个人信息保护而言，上述德国法中关于董事合法义务的司法适用逻辑不仅在法理上值得我国立法和司法实践所借鉴，而且，随着《民法总则》、《消保法》以及《网络安全法》等法律的颁布或修订，我国现行法已经具备了相应的制度基础。

1. 企业作为信息收集者，其法定组织义务已经确立。《民法总则》第 111 条规定，任何组织和个人负有依法取得他人个人信息并确保信息安全的义务。对所收集信息的安全保障义务是所有收集主体的基本义务。《消保法》和《网络完全法》对于信息安全保障义务做出了进一步的规定。其中，《消保法》第 40 条规定，经营者及其工作人员对收

〔49〕 参见张怀岭：“德国法董事合规义务的司法适用逻辑——基于对‘西门子诉纳伯格案’的分析”，《中德私法研究》2015 年第 2 期，第 238～258 页。

〔50〕 LG München I，NZG 2014，345（346）.

〔51〕 参见王军：《中国公司法》，高等教育出版社 2017 年版，第 389 页。

集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。《网络安全法》第 40 条规定了网络运营者“建立健全用户信息保护制度”的组织义务。该法第 42 条第 2 款中规定：“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息的安全。”从这些规定可以引申出，企业作为信息的（合法）收集者时，为了履行法律所规定的信息保护义务，必须在企业内部采取妥当的、符合客观必要安全标准的措施。为履行上述事前预防和事后补救义务，公司管理者自然应当设立相应的信息安全保障部门，配备与其处理信息规模相适应的专业人员。

2. 鉴于实践中大规模信息窃取、泄露、出卖等侵害个人信息的行为是源于“内部人”，[52] 董事、高管对公司所负的组织义务还涵盖了建立内部运行良好的监督机制。在“西门子诉纳伯格”案中，法院认定，尽管西门子公司设立了专门的合规部门并且配备了相关专业人员，但是这一合规监督机制未能有效运行，事前预防违法事件（诸如，反复在集团内部出现向海外政府官员和个人行贿的事件）和事后处罚措施（尤其是对相应员工的人事处罚）都未能达到预期效果，从而违反了董事的合法义务。基于这一法律适用逻辑，合法义务要求收集用户个人信息的企业必须建立对内部员工的培训和监督制度。而且，如果在个案中表明该制度存在不足之处，必须及时采取补救措施。这也可以从我国《消保法》第 40 条（补救措施的规定）和《网络安全法》第 42 条第 2 款（个人信息泄露、毁损、丢失的情况下应采取补救措施并履行告知和报告义务）中找到法律依据。以 58 同城数据泄露事件为例，该公司全国用户个人简历遭到大规模泄露。无独有偶，招聘网站普遍存在个人数据保障程度低下，安全漏洞众多且长时间没有得到修补，易于遭恶意爬虫软件利用平台漏洞爬取信息的问题。根据对智联招聘工作人员的采访，该企业内部信息保护制度不严格，即便权限较低的员工也可以轻易、无限制地获取企业数据库中的用户个人信息。[53] 这也表明了以董事、高管合法义务为基础，建立内部完善合规制度的迫切性。

五、个人信息保护义务内化机制构建的关键环节：举证责任的分配与诉讼主体资格

（一）举证责任分配

司法实践中，实体权利在多大程度上以及以何种成本可以得到维护和实现，主要依赖于举证责任的分配。比较法上的公司治理中，董事的经营活动受到商业判断规则（Business Judgment Rules）的保护。而商业判断规则则是通过实体法的形式确定举证责任的分担。基于这一比较法经验，个人信息保护纠纷中的举证责任分配应当通过实体法

〔52〕 例如，京东的用户信息泄露事件。在最高人民检察院最近发布的六起侵犯公民个人信息犯罪典型案例中，造成损害最大的都是“内部人”的违法行为。

〔53〕 该事件具体经过参见 http：//industry.caijing.com.cn/20170324/4251509.shtml，最后访问时间：2017 年 11 月 27 日。

的规范予以特殊规定，从而实现利益保护的平衡。具体而言，针对发生的个人信息侵害纠纷，例如，信息的泄露、不当使用等情形，只要信息的权利人举证证明发生了其权利受到侵害的后果，就由对个人信息负有保护义务的主体对其履行了法定的信息保护义务或者特定损害后果即便在其合法履行义务的情况下依然会发生（因果关系）承担举证责任。

比较法上的考察表明，为了避免司法机关对于商事决策采取事后审查从而不正当地抑制经营者从事具有一定风险的商业活动的积极性，引入商业判断规则是必然之举。德国法的制度沿革便佐证了这一点。20 世纪 90 年代，德国联邦最高法院的判例规则主张，[54] 公司应当对董事违反注意义务的客观要件承担说明与举证责任（Darlegungs-und Beweislast），而董事则仅对其不具有主观过错承担举证责任。这就意味着，在例外情形下，诸如公司财产由于相关董事未能履行职责的原因（收银数额不足、存货短缺）而无法确定时，公司的权利可能就无法实现。但是，如今联邦最高法院已经通过一系列新的判决极大地以有利于公司提起诉讼的方式进行了改革。[55] 公司作为原告，仅需要证明其在多大范围内由于董事义务范围内的行为而遭受了损害。[56] 这很大程度上是基于对《股份法》和《合作社法》相关规范的类推适用。例如，通过移植美国法的制度，《德国股份法》首先在第 93 条第 1 款第 1 句规定了董事会成员应当负有注意义务的标准；其次，第 93 条第 1 款第 2 句规定："如果董事会成员在进行商业决策时，基于妥当的信息基础可以合理地相信其行为有利于公司的利益，则不构成注意义务的违反。"商业判断规则的引入既降低了公司作为原告的举证责任，同时也为董事对商业决策所享有的自由裁量提供了制度保障。这也可以为我国《公司法》以及司法实践所借鉴，从而实现董事在商业决策上的自由裁量权与履行法定个人信息保护义务的良好平衡。因为公司及其董事"距离"证据最近，其承担自身已经履行组织义务的举证责任并非是不成比例的风险负担。

就个人数据保护而言，德国《数据保护法》的立法例可供借鉴。该法第 7 条第 1 款规定了企业违反法律规定，因其信息收集、处理或利用行为给用户造成损害的应当承担赔偿责任。但是，该条第 2 款又规定："企业尽到根据具体情形所必要的注意义务的，不承担损害赔偿责任。"法律体系上，该规范被作为德国《股份法》（AktG）第 93 条第 1 款、《有限责任公司法》（GmbHG）第 43 条第 1 款抑或《合作社法》（GenG）第 34 条第 1 款的特殊规范。这意味着由信息处理者对其自身已经履行了法律规定应尽的注意义务承担举证责任，从而大幅降低了用户等主体提起诉讼的举证责任和风险。[57]

---

〔54〕 BGH v. 26. 11. 1990-II ZR 223/89，GmbHR 1991，101 ff；BGH v. 21. 03. 1994-II ZR 260/92，GmbHR 1994，459 ff.

〔55〕 诸如 BGH v. 04. 11. 2002-II ZR 224/00＝GmbHR 2003，113～117。

〔56〕 参见前注〔47〕，Zhang H. 书，第 66 页。

〔57〕 例如，奥地利法律人和活动人士马克斯 史莱姆丝（Max Schrems）曾通过投诉和诉讼的方式迫使 Facebook 公布其账户的用户信息以及在欧洲关闭其脸部识别功能。以欧盟新条例的通过为契机，他作为创始人新近成立了非政府机构 Noyb，旨在针对企业违反信息保护义务的行为向监管机构进行投诉以及向法院提起诉讼。

（二）诉讼主体资格

就诉讼主体资格而言，与德国现行法类似，欧盟《通用数据保护条例》第 80 条第 1 款规定了“集体诉讼”条款，允许非政府组织代表个人信息受到损害的个人向监管机构采取法律行动。该条第 2 款进一步授权成员国可以就“集体诉讼权”进行规定。尤其值得注意的是，该条例第 82 条第 1 款明确规定损害赔偿的范围涵盖“精神损害赔偿”。在损害赔偿额度的计算上，欧盟法院（EuGH）判例依据“有效性原则”，[58] 认为损害赔偿额应当具有“威慑性”。[59] 这将大幅增强私法执行机制在个人数据保护方面的有效性。我国《消保法》已经引入了惩罚性的损害赔偿制度，尽管该法本身具有“规制法”的色彩。基于降低私权利行使成本，鼓励权利保护的目的，可以扩大惩罚性损害赔偿的适用范围。

参考文献

[1] 范为. 大数据时代个人信息保护的路径重构 [J]. 环球法律评论，2016（5）.

[2] 赵秉志. 公民个人信息刑法保护问题研究 [J]. 华东政法大学学报，2014（1）.

[3] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心 [J]. 现代法学，2013（4）.

[4] 陈甦. 民法总则评注 [M]. 北京：法律出版社，2017.

[5] Niedobitek M（Hrsg.）. Europarecht-Grundlagen der Union [M]. Berlin/Boston：De Gruyter，2014.

[6] Schanz. Die Datenschutz-Grundverordnung-Beginn einer neuen Zeitrechnung im Datenschutzrecht [J]. NJW 2016.

[7] [德] 鲁道夫·冯·耶林. 为权利而斗争 [M]. 郑永流，译. 北京：法律出版社，2012.

[8] 洪延青. 以管理为基础的规制——对网络运营者安全保护义务的重构 [J]. 环球法律评论. 2016（4）.

[9] 徐丽枝. 个人信息处理中同意原则适用的困境与破解思路 [J]. 图书情报知识. 2016.

[10] 张维迎. 理解公司：产权、激励与治理 [M]. 上海：上海人民出版社，2014.

[11] Kraakman R. etc. The Anatomy of Corporate Law-A Comparative and Functional Approach [M]，New York：Oxford University Press，2009.

[12] Davies P，Worthington S. Principles of Modern CompanyLaw [M]，London：Sweet & Maxwell，2012.

[13] [德] 卡尔·拉伦次. 法学方法论 [M]. 陈爱娥，译. 北京：商务印书馆，2004.

[14] [美] 弗兰克·伊斯特布鲁克. 公司法的经济结构 [M]. 罗培新，张建伟，译. 第 2 版. 北京：北京大学出版社，2014.

[15] Zhang H. DieRechtspflichten der Leitungsorgane der geschlossenen Kapitalgesellschaften [M]，Hamburg：Dr. Kovac Verlag，2017.

[16] 张怀岭. 德国法董事合规义务的司法适用逻辑——基于对“西门子诉纳伯格案”的分析 [J]. 中德私法研究，2015（2）.

[17] 王军. 中国公司法 [M]. 北京：高等教育出版社，2017.

[18] Yahoo now says all 3 billion of its accounts affected by massive hack [EB/OL]. [2017-11-24]. http：//mashable. com/2017/10/03/yahoo-hack-bigger/#Y6kUXV1Duaq2.

[19] Google collects Android users' locations even when location services are disabled [EB/OL]. [2017-11-24]. https：//qz. com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/.

（责任编辑：朱晓峰　赵建蕊）

〔58〕 EuGH，EuZW 2016，183 Rn. 44-Arjona Camacho.

〔59〕 参见前注〔18〕，Schanz 文，第 1847 页。