财经法学 No. 4，2023
pp. 118 - 133

网络空间中信息安全守门人的刑法义务

喻浩东*

内容提要：拒不履行信息网络安全管理义务罪的增设为网络空间中信息安全守门人的刑法义务提供了实定法根据。鉴于司法实务所遭遇的困境，有必要对信息安全义务的目的、性质和范围展开教义学上的体系化解读。在目的构建上，无论用户信息专有权说还是信息网络安全管理秩序维护说都存在难以克服的缺陷。应当提倡一种系统耦合的法益观，将该义务的目的界定为保障信息共享的互惠性风险分配机制，以实现法律系统与数字经济系统间的有效沟通。在性质界定上，义务犯论错误地理解了积极义务的产生根据，将支配犯与作为犯、义务犯与不作为犯不当混同。信息安全义务的本质是对网络服务提供者数字生产权力的纠偏，因而应当归属为基于组织管辖产生的消极义务而非基于制度管辖产生的积极义务。在明确保护目的和义务性质的基础上，对该义务保护范围的确定，既要实现保障信息共享的互惠性风险分配机制的规范目的，也应对其中内含的危险给予正当性控制。

关键词：网络服务提供者　信息安全守门人　系统耦合的法益观　拒不履行信息网络安全管理义务罪

一、问题的提出

在信息网络世界中，数据的收集、处理、利用等环节均控制在占据技术主导优势的各类网络服务提供者之手，因此在风险管辖方面，网络服务提供者实际扮演着“守门人”的关键角色。基于此，国际社会普遍要求作为数据控制者或处理者的网络服务提供者承担数据保护的法律义务。我国亦不例外，十余年来经由《中华人民共和国网络安全法》（以下简称《网络安全法》）、《工业和信息化领域数据安全管理办法（试行）》、《中华人民共和国数据安全法》等多部法律法规的颁行逐步构建起一套有关平台数据安全保护义务的制度体系。

为了稳定规范化预期、发挥积极一般预防的刑法功效，我国立法机关在《中华人民共和国刑

* 喻浩东，复旦大学法学院讲师。

法修正案（九）》中增设了286条之一，规定网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户信息泄露，造成严重后果的，应当追究刑事责任。不过，该条自颁行以来几乎未曾得到实际适用。〔1〕个中原因除了行政前置性程序的设置导致很多案件未进入刑事程序之外，主要还在于信息网络安全管理义务究竟为何模糊不清。〔2〕

在首起电信运营商因拒不履行这一信息安全义务被判处刑罚的案件中，法院认定被告人李小全负有查验、评估、审核行业卡使用情况的职责，明知远特公司曾三次违反实名制的管理规定，仍将大量带有个人信息的回收卡交给亚飞达公司，违反用户实名制进行挑卡，造成严重后果，且在两年内经监管部门多次责令改正而拒不改正，构成拒不履行信息网络安全管理义务罪。〔3〕可是，法院并未明确被告人的上述行为到底违背了哪部法律、行政法规中的哪一义务。本案中远特公司曾被三次责令改正的法律根据是《电话用户真实身份信息登记规定》，但该规定并未达到法律或行政法规的层级，而且，法院并未论证用户信息泄露造成的严重后果能够归责于被告人违反法律、行政法规义务的行为。

由此看来，解读网络服务提供者的信息安全义务理应构成信息刑法的重要议题。本文将试图在追求数据安全保护与数据有序流动相对平衡的价值理念下，从以下三个方面展开体系性论述：首先需要明确这一安全义务的目的何在。目的是全部法律的创造者，〔4〕科处义务必须回答“这样做意在保护什么”的问题。其次需要界定立法者为实现这一目的采用了何种规制方式，也即安全义务的性质。这种义务究竟归属义务犯的积极义务还是支配犯的消极义务，对于归责原理的适用而言具有显著影响。最后在明确该义务的目的和性质的基础上，体系化地构建其实体内容并划定其合理边界。

二、信息安全义务的目的重构

既有学说对保护目的的界定无论在方向还是结论上都存在难以克服的缺陷，其共同症结在于，未能意识到并发挥法益作为法律系统与其他社会子系统间媒介的作用。

（一）既有学说的缺陷所在

1. 对“用户信息专有权说”的批评

有论者认为，信息法益就是信息主体所享有的信息权利。信息专有权的核心是基于法规范明确授权的对数据处理的“允许”。同时，又因为立法者将该罪设置在《中华人民共和国刑法》（以下简称《刑法》）第六章第一节“扰乱公共秩序罪”中，所以要将法益进一步限缩为具备公共利益属性的信息专有权。〔5〕

但无论在事实还是规范层面，都谈不上用户的信息专有权。在事实层面上，用户信息是用户

〔1〕 相关实证研究报告，参见杨新绿：《拒不履行信息网络安全管理义务罪司法适用问题及化解》，载《湖北警官学院学报》2020年第5期。

〔2〕 参见李世阳：《拒不履行网络安全管理义务罪的适用困境与解释出路》，载《当代法学》2018年第5期。

〔3〕 参见云南省昆明市盘龙区人民法院（2020）云0103刑初1206号刑事判决书。

〔4〕 Vgl. Rüthers/Fischer/Birk, Rechtstheorie mit Juristischen Methodenlehre, 10. Aufl., 2018, § 15 Rdn. 520.

〔5〕 参见敬力嘉：《论拒不履行信息网络安全管理义务罪——以网络中介服务者的刑事责任为中心展开》，载《政治与法律》2017年第1期。

在社会交往中产生的，是用户与各类智能设备互动的产物，本身就具有公共属性，严格来说只能是“与用户有关的信息”。海量的用户信息被控制在各类网络平台的手中，而用户个体根本无法像控制财产那样控制这些信息。〔6〕从规范层面来说，强调用户对信息的专有，人为地在法律上制造资源的稀缺，无异于禁锢思想、阻吓交流，本质上是不受限制地限制他人的自由。〔7〕且单就其中个人信息的保护而言，不同领域中的个人信息应当受到保护的程度也不相同，要根据信息的利用可能性、信息利用的目的以及经由信息科技所开启的处理可能性等因素来区分不同的保护层级。〔8〕

另外，该论者将“信息网络安全管理”不当限缩到网络信息传播治理的范畴，但不论是就用户信息的保护，还是就刑事证据的保存而言，其都难以归入该范畴之中。我国有学者曾对网络信息传播犯罪的类型进行了概括：类型一是该信息传播行为本身就是《刑法》所禁止的构成要件或构成要件行为的一部分；类型二是发布或传播不法信息本身并非构成要件的实行行为，只有当该类信息的发布或传播与行为人自己或他人在现实世界的行为结合才会造成法益侵害。〔9〕显然，网络服务提供者不履行对用户信息或刑事证据的保护或保存义务造成法益侵害的，并不属于上述两类传播犯罪中的任何一类。

2. 对“信息网络安全管理秩序说”的质疑

更多论者基于体系解释的原理，将法益界定为信息网络安全的管理秩序。〔10〕对此本文也难以认同，提出如下质疑理由：

其一，特定领域的管理秩序是否为适格的集体法益，并非不言自明。对此，德国学者格雷科给出了三个消极性标准：（1）循环性测试，即如果不假定某种集体法益存在，就无法将特定的刑罚法规正当化，这一事实并不是认定这种集体法益确实存在的理由；（2）分配性测试，即很多个体都有意愿分享某种利益，这一事实并不是认定一个集体法益存在的理由；（3）非特定性测试，即如果侵害某一所谓的集体法益总是同时以侵害个人法益为前提，那么就不允许将这种集体法益认定为特定刑罚法规的保护利益。〔11〕信息网络安全管理秩序无法通过这三个标准的检验：首先，并不是非要假定该秩序利益的存在，才可以对信息安全义务予以正当化。秩序利益的形成反倒以保障个人权益为前提。其次，尽管社会成员都对信息网络安全秩序享有利益，但这并不是将该秩序本身作为法益保护的理由。再次，由于拒不履行信息安全义务总是以侵犯用户的人身和财产权益为前提，因此无法将更为抽象的管理秩序作为该义务的保护法益。

其二，将特定领域的管理秩序界定为法益，是对规范与法益的混淆，会致使单纯的行政不服从被认定为犯罪。社会秩序，意指社会进程中存在某种程度的一致性、连续性和确定性。人们在生活安排方面对连续性的诉求与他们要求在相互关系中遵守规则的倾向之间是存在联系的。只要人的行为受到法律规范的控制，重复规则性这一要素就会被引入社会关系之中。遵循规则化的行

〔6〕 参见欧阳本祺：《侵犯公民个人信息罪的法益重构：从私法权利回归公法权利》，载《比较法研究》2021 年第 3 期。

〔7〕 参见杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，载《比较法研究》2015 年第6 期。

〔8〕 Vgl. Thilo Weichert, Datenschutzstrafrecht-ein zahnloser Tiger? NStZ 1999, 490.

〔9〕 参见王莹：《网络信息犯罪归责模式研究》，载《中外法学》2018 年第 5 期。

〔10〕 参见谢望原：《论拒不履行信息网络安全管理义务罪》，载《中国法学》2017 年第 2 期；前引〔2〕，李世阳文；杨新绿：《论拒不履行信息网络安全管理义务罪的法益》，载《北方法学》2019 年第 6 期。

〔11〕 Vgl. Luís Greco, Gibt es Kriterien zur Postulierung eines kollektiven Rechtsguts? FS-Roxin, 2011, S. 208.

为方式，为社会生活提供了很高程度的有序性和稳定性。〔12〕所以，这里的秩序体现了规范运作的实际状态，但法益则是行为规范所保护的客体，是秩序所要保护的价值，这说明秩序与法益不能混同。〔13〕强调某一特定社会秩序需要加以维护，仅仅是表达了国家想要运用公权力对该领域进行行政管理的意愿之事实，并没有交代管理的目的何在。将特定领域的社会管理秩序界定为法益，无疑是站在政府的一端，其追求的管理秩序无非就是该领域参与者服从行政管理的有序状态。〔14〕这样的法益观容易导致将管理法规等同于管理秩序的套套逻辑，而且将单纯违反行政法规的行为认定为犯罪，也不符合变动社会中法益理论的应然走向。杨仁寿在《法学方法论》中指出，倘若社会急剧变迁，法律目的与社会目的不同，就应当以社会目的来解释法律。〔15〕信息网络领域由一元化的国家管制逐渐迈向多元主体共治的局面，也正要求法律与时俱进，改变其“压制的性格”，转而成为社会各个子系统自我运作与自我治理的协调机制。

（二）保护目的的重新界定

1. 系统耦合的法益观之提倡

既有学说共通的弊病在于，无论是从《刑法》条文规定的行为对象来确定法益，还是从具体犯罪所属的类罪来确定法益，〔16〕均只是在刑法体系内部对《刑法》条文保护目的的逻辑推导。这样做的消极后果有二：其一，以预设目的为导向的解释，无非是朝着解释者想要达致之结论的循环论证。〔17〕其二，完全侧重于方法论意义的法益理论，致使法益概念逐渐丧失了批判立法的机能，因为除非相应的道德观念土崩瓦解，否则刑法保护就很容易获得正当性。〔18〕由刑法体系内部确定的法益不仅在价值取向上可能与他系统中应当保护的利益南辕北辙，且据此所进行的构成要件解释很可能导致将他系统中原本应予鼓励的行为不当认定为犯罪，实质上是法律系统粗暴干预他系统自主运作的表现。

想要走出当前法益理论深陷的泥潭，就不得不将现代社会建立在二阶观察基础上的社会沟通模式纳入法益的构建当中。现代社会分化为若干自创生的子系统，这些子系统均是封闭运行的实体，它们借助其要素的递归式生产自我创生和自我维持。〔19〕尽管如此，封闭运作的系统又具有开放的面向，系统对其环境保持着认知上的开放性和敏感度。在环境为系统自创生的延续制造问题时，系统就会以自己固有的方式产生激扰。〔20〕虽然系统与其环境之间没有直接的接触，但却通过其自身运作对环境形成观察。这种观察是系统内部的活动，它以区分系统和环境为前提，同时具有自我指涉和外部指涉的面向，通过与外部环境的沟通实现认知上的开放。〔21〕其中，法律

〔12〕 参见〔美〕E·博登海默：《法理学：法律哲学与法律方法》，邓正来译，中国政法大学出版社 2010 年版，第 228、239 页。

〔13〕 参见马春晓：《经济刑法的法益研究》，中国社会科学出版社 2020 年版，第 127 页。

〔14〕 参见蓝学友：《互联网环境中金融犯罪的秩序法益：从主体性法益观到主体间性法益观》，载《中国法律评论》2020 年第 2 期。

〔15〕 参见杨仁寿：《法学方法论》（第 2 版），中国政法大学出版社 2013 年版，第 72 页。

〔16〕 参见张明楷：《刑法分则的解释原理》（第 2 版）（上），中国人民大学出版社 2011 年版，第 350－352 页。

〔17〕 参见〔德〕英格博格·普珀：《法学思维小学堂》，蔡圣伟译，元照出版公司 2010 年版，第 96 页。

〔18〕 参见〔德〕伊沃·阿佩尔：《通过刑法进行法益保护？——以宪法为视角的评注》，马寅翔译，载赵秉志、宋英辉主编：《当代德国刑事法研究》（第 1 卷），法律出版社 2017 年版，第 57 页。

〔19〕 Vgl. Georg Kneer, Armin Nassehi, Niklas Luhmanns Theorie sozialer Systeme: eine Einführung, 2000, S. 65.

〔20〕 参见前引〔19〕，Georg Kneer 书，第 61 页。

〔21〕 参见前引〔19〕，Georg Kneer 书，第 98 页。

系统依照“合法/非法”的符码形成封闭的自我运作，以区隔于以“支付/不支付”为符码的经济系统和以“有权/无权”为符码的政治系统。

法律系统的唯一功能在于稳定规范性预期，违法事实的发生并不会导致法律无效，因为法律系统会反事实地坚持预期，拒绝做出相应调整。正是由于该系统的沟通排斥“合法/非法”以外的所有第三种价值，脱离外部的社会脉络而维持反事实的“规范性”，其他社会子系统才得以自主运行。在此意义上，法律具有保障经济发展、政治稳定、科学繁荣、宗教自由等多种成效。〔22〕但符码本身并不具有单纯凭借自身而生存的能力，唯有在法律系统的纲要层次上展开悖论，它们才能以自我再制的方式具有生产性。这里的纲要补充符码的语意和使用符码的条件，分派“合法/非法”价值的判断标准。在这一层次上，法律系统认知环境，汲取非法律价值，从而保障自身的学习能力，使之不至于在获得“自主性”的同时丧失对环境的适应性和敏感度。〔23〕经由纲要的运作，环境的变动被建构为“法律事件”，对法律系统内部的既有状态形成激扰，迫使该系统自身做出相应的调整。〔24〕由此，法律系统与经济、政治系统间形成“结构耦合”的关联模式。在这一过程中，法益充当了系统间沟通的媒介，它将刑法体系外部的信息也即各种价值判断、政策因素和利益衡量纳入系统自我指涉的介质。基于此，无论认定哪种犯罪，都需要对行为特定领域的运作逻辑和沟通模式进行考察，在此基础上进行刑法构成要件的判断。〔25〕

2. 目的重构：信息共享的互惠性风险分配机制

根据系统耦合的法益观，确定具体罪刑规范的保护目的，需要首先关注该规范外部指涉的他系统中的利益诉求，然后思考将这种利益诉求在刑法系统内部转化为何种法益。

古典社会的经济理论假设个人对私利的追求是驱动经济增长的唯一有效方式。个人追求私利的根本原因在于对稀缺资源的竞争压力及对是否能够获得合理的稀缺资源的不确定性。彼时隐私权保护意识的兴起，就来源于对社会成员之间不当竞争的必要限制。私权利制度赋予了社会成员足够的理性，使其可以根据自身意愿来自我决定并为相应后果负责。然而，有机社会的成员针对稀缺资源将会是合作分享取代竞争占有，“共同创造—共享—按需分配”取代了“分工—私权—交易”模式。〔26〕在大数据时代，个人数据信息具有充裕性，对数据的挖掘、开放和处理产生出众多衍生信息或结果，很多都是一开始无法预测的。因此，早在 1996 年，互联网先驱佩里·巴洛就在《网络空间宣言》中倡导信息的自由分享。美国维基百科计划的实施、我国网络上的字幕组、戏仿和知识共享等在线社群努力创造的开放式环境，反映了信息分享和协作的模式受到关注。而后，从 Web 2.0 时代去中心化的信息交互到 Web 3.0 时代的网际和数据互通，技术的升级和应用创新都在不断促进信息分享和盈余扩大。〔27〕核心交互既是网络平台出现的根本原因，也是其所追求的基本目标。平台想要促进有价值的核心交互，就必须将生产者和消费者吸引过来，为之提供方便且易于联系和交换的工具与规则，同时还要利用相互之间的信息有效匹配生产

〔22〕 参见高鸿钧、赵晓力主编：《新编西方法律思想史（现代、当代部分）》，清华大学出版社 2015 年版，第 328 页。
〔23〕 参见前引〔22〕，高鸿钧、赵晓力主编书，第 329－330 页。
〔24〕 参见前引〔22〕，高鸿钧、赵晓力主编书，第 341 页。
〔25〕 参见刘涛：《系统理论下刑法与社会关系研究》，中国法制出版社 2023 年版，第 326－329 页。
〔26〕 参见吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016 年第 7 期。
〔27〕 参见梅夏英：《在分享和控制之间：数据保护的私法局限和公共秩序构建》，载《中外法学》2019 年第 4 期。

者和消费者，使其互惠互利。〔28〕

对于信息共享这一他系统中的利益诉求，必须经由刑法纲要转化为法律系统内部的具体法益。实际上，民法和刑法上有关信息保护的规范，其最终目的都指向了信息共享，但各自的侧重面向并不相同：民法上对个体的赋权和对信息处理者的赋责，更多地为了提升信息利用的效率和平衡相关主体间的利益。例如有论者指出，倘若以财产权方式来保护个人信息并规范其使用，因为受制于信息主体的意志，往往会使主体陷入要么全部同意要么全部拒绝的两难境地，不利于提升信息使用的质量和效率。〔29〕与此不同，刑法对信息权益的保护，则更侧重于防范信息共享中的负外部性效应，其关注的是风险如何公平分配、谁应当对风险的实现负责的问题。经济学中的外部性，是指有人承担了他人行为引起的成本或获得别人行为创造的收益。如果社会成本大于个人成本，这时有人承担了行为人带来的伤害，我们就称其为负外部性。〔30〕而在信息时代的法律规制中，刑法主要侧重防范由网络服务提供者等信息控制者和处理者的行为导致的隐私侵害等负外部性效应。〔31〕对于刑法系统的运作而言，必须确立并保障一套指向信息共享的风险分配机制，以形成“合法/非法”的判断符码，通过制裁破坏该风险分配机制的行为来确证规范的效力。

公平的风险分配机制的核心在于互惠原则。该原则要求个人的利他必须带来足够合作的盈余，而且群体成员在他人没有给予互惠行为的回报时，可以在未来不再做出利他行为。在有限的群体和空间中，对于这一原则可以通过查明和惩罚非互惠者并将其踢出群体的方式来加以维护。〔32〕而在超越时空的网络空间中，社群规范的互惠约束机制或许不再能够适用，通过法律对违反互惠分享规范的行为进行规制就必不可少。信息的互惠分享也是数据生产论的题中之义：如果把数据比作小麦，网络平台就是小麦被收集、研磨、精炼为面粉的加工厂。对于用户来说，数据只是他们浏览互联网的副产品，但对于平台来说，这些就是重要的生产资料。只有平台才能够将个人信息与行为数据加工提取为生产要素。〔33〕然而，如果任由他人侵犯用户的信息权益，最终致使用户对于平台的整体信任崩塌，不再放心将自己的信息提供给网络服务提供者，就会像釜底抽薪一样剥夺作为生产者的平台最为基本的生产原料。〔34〕所以，对于违背互惠原则、强制用户承担其不应承担的信息风险的行为，刑法就应当予以制裁，以保障公平的风险分配机制的效力。当然，互惠的风险分配也要求刑法将保护目的最终指向信息的共享，也即，对信息处理者的风险分配也应当有利于促进信息共享目的的实现。倘若将数据收集、利用与流转的决定权完全置于用户之手，不仅事实上不可能，而且也不利于生产者充分挖掘数据潜藏的巨大价值。如此也就不难理解，为什么个人数据的私权保护理论遭遇了猛烈抨击。〔35〕

---

〔28〕 参见〔美〕杰奥夫雷·G. 帕克等：《平台革命》，志鹏译，机械工业出版社 2017 年版，第 39－47 页。

〔29〕 参见郑维炜：《个人信息权的权利属性、法理基础与保护路径》，载《法制与社会发展》2020 年第 6 期。

〔30〕 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 65－67 页。

〔31〕 参见〔德〕克劳斯·施瓦布、〔澳〕尼古拉斯·戴维斯：《第四次工业革命——行动路线图：打造创新型社会》，中信出版集团 2018 年版，第 11 页。

〔32〕 参见前引〔27〕，梅夏英文。

〔33〕 参见张凌寒：《数据生产论下的平台数据安全保障义务》，载《法学论坛》2021 年第 2 期。

〔34〕 世界经济论坛的一篇报告指出，个人和数据控制机构间存在的严重信息不对称，造成了严重的信任危机，影响数据的真实产生和自由流动，阻碍创新和大数据潜力的发挥。参见个人信息保护课题组：《个人信息保护国际比较研究》，中国金融出版社 2017 年版，第 44 页。

〔35〕 参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期；前引〔6〕，欧阳本祺文。

因此，不但刑事立法者不应当忽视数字经济发展中的利益诉求，网络运营者实施的有利于促进数据共享的行为不应当纳入刑事处罚的范围，而且刑事司法也应参照同样的思路来区分“合法/非法”，如后文所述，应通过目的性对“用户信息”“泄露”等构成要件要素予以解释，合理地确定网络服务提供者的信息安全义务之边界。

三、信息安全义务的性质界定

《刑法》第 286 条之一实际规定了三种类型的信息网络安全管理义务，而其中针对用户信息的安全管理义务，应当从数字生产权力纠偏的维度对其性质予以界定。

（一）义务类型：消极义务和积极义务

有论者援引了罗克辛关于义务犯成立的根据——对行为人所承担的社会角色和规范义务的违反——认为拒不履行信息安全管理义务罪属于典型的义务犯。该论者据此指出，作为犯以积极制造法益风险的方式支配犯罪进程和法益侵害结果，而不作为犯主要体现为违背义务导致原本可以不发生的结果发生，两者分属存在论和规范论的范畴。〔36〕

但这种观点恐怕将支配犯和作为犯、义务犯和不作为犯不当混同。作为与不作为的区分显然是存在论意义上对行为人之行为形态的客观描述，与之相反，支配犯和义务犯的区分则是规范论意义上关于哪一行为人构成正犯的规范性评价。在存在论层面上，人们观察某行为是否体现为一种积极的能量投入，而在规范论视域中，基于“从实然中不能推导出应然”的方法二元论，某一存在结构（作为或不作为）并不能决定规范评价（犯罪支配或义务违反）的结论。在规范论的意义上，有论者甚至宣称，所有犯罪的成立都必须满足义务违反的前提要件。〔37〕至少对于过失作为犯来说，注意义务的违反是法定的构成要件要素，而过失结果的归责还必须满足注意义务违反与结果之间的规范关联。对于故意作为犯来说，如果认为其和过失作为犯仅是位阶关系，那么也可以说前者是具备更高不法程度和责任程度的后者。〔38〕

值得注意的是，我国学者曾提出的支配维度和义务维度的结果归责的二分模式，与这里所说的支配犯与义务犯的二元划分并不能同日而语。支配维度的结果归责，基本上对应于行为人对导向结果的因果流程拥有事实性操控的作为的情形，而义务维度的结果归责，则主要用来解决行为人对结果并未施加现实作用力的场合如何归责的问题。〔39〕但对结果是否施加了现实作用力，并不是义务犯成立与否的判准。只有当行为人所负担的义务是具有人身专属性的特别义务时，才有讨论义务犯的余地。

实际上，只有将犯罪划分为基于组织管辖和基于制度管辖的二元类型，才能真正为判断信息安全义务是否属于义务犯的特别义务提供实质判准。雅各布斯提出以“管辖”来统摄全部犯罪行

〔36〕 参见周光权：《拒不履行信息网络安全管理义务罪的司法适用》，载《人民检察》2018 年第 9 期。

〔37〕 Vgl. Otto, Grundkurs Strafrecht-Allgemeine Strafrechtslehre, 7. Aufl., 2004, § 5 Rdn. 10 ff.

〔38〕 Vgl. Puppe, Strafrecht Allgemeiner Teil: im Spiegel der Rechtsprechung, 4. Aufl., 2019, § 7 Rdn. 1 ff.

〔39〕 具体的论述，参见劳东燕：《事实因果与刑法中的结果归责》，载《中国法学》2015 年第 2 期。

为的归责判断，〔40〕至于行为人根据什么对某一事件负有管辖义务，既可能基于自由行动所带来的组织圈的扩张，也可能基于社会制度所附加的团结义务。对管辖义务做这样区分的理由在于，人们可以组织世界，当然也一直生活在一个被组织了的世界（带有制度的世界）中，因此对于社会交往得以可能必不可少的是稳定人们的规范性期待，这种期待关联到两种不同的对象领域：其一，应当可以期待，所有人都会组织好自己的交往圈，从而不会导致他人遭到来自外部的伤害。这种期待仅仅具有消极性的内容。其二，同样可以期待，原初的社会制度可以正常运转。这种期待具有积极性的内容。〔41〕为了稳定这两种规范性期待，人们必须分别履行消极义务和积极义务。

消极义务要求人们不要无视他人的组织圈而安排自身的活动。17 世纪的德国学者普芬道夫就曾说道，在所有的绝对义务中，首先是不侵犯他人的义务。这是最基本的义务，没有它就根本不会有人类的社会生活。〔42〕不过，不去侵犯他人的义务并不等同于不能做什么的禁止规范，因为当行为人负有义务去阻止一个侵害他人法益的因果流程时，他显然是要积极地做点什么（作为义务）。不作为犯中对危险源的管理（基于先行行为、交往安全义务等）义务就要求行为人为防止危险源的扩散而采取积极举动。这种作为义务的产生根本上还是基于行为人自由组织自身的活动，而不需要特殊的制度理由。

积极义务不仅要求人们避免自己的组织行为侵犯他人，还要求人们为保障某种状态的完好或促进他人的组织行为，即共同建设一个美好世界而做点什么。〔43〕对此，普芬道夫也曾指出，为了共同的社会性而承担的第三个普遍义务是，每个人都应尽其所能有益于他人。仅仅不伤害他人、不轻视他人是不够的。我们还必须给予（至少是分享）他人能增进相互间善意的东西。〔44〕人们之所以能够感受到法律赋予他们的自由，前提是为法律所承认的社会关系暨制度的长久存在。父母与子女的关系，婚姻关系，国家的统治关系，对安全和秩序的维护以及立法和行政等等，均属此类。只有在法律上被纳入该制度的人，才负有积极义务。〔45〕

（二）数字生产的权力纠偏与原初义务

那么，信息安全义务究竟属于消极义务还是积极义务？本文认为，基于网络服务提供者在知识和技术上的绝对优势，信息安全义务的科处是对其从事数字生产活动的权力纠偏，因而是一种原初义务，并不需要制度提供特殊的理由。

随着经营体量和经济实力的迅速扩大，网络平台的身份特征和法律形象也在转变，早已不是仅具中立性质的网络接入、存储或宿主服务的技术提供者。与这种去中立化、复杂化相伴而来的是网络平台控制力的明显增强。〔46〕如果将网络空间比喻成生态系统，谁掌控了平台，谁就是开

〔40〕 Vgl. Jakobs, Die Strafrechtliche Zurechnung von Tun und Unterlassen, 1996, S. 32 ff. 转引自何庆仁：《义务犯研究》，中国人民大学出版社 2010 年版，第 142 页。

〔41〕 Vgl. Jakobs, Strafrecht Allgemeiner Teil, 2. Aufl., 1991, § 5 Rdn. 7.

〔42〕 参见〔德〕塞缪尔·普芬道夫：《人和公民的自然法义务》，鞠成伟译，商务印书馆 2009 年版，第 79 页。

〔43〕 Vgl. Jakobs, System der strafrechtlichen Zurechnung, 2012, S. 83.

〔44〕 参见前引〔42〕，塞缪尔·普芬道夫书，第 86 页。

〔45〕 Vgl. Kindhäuser/Hilgendorf, Lehr-und Praxis Kommentar, StGB, 8. Aufl., 2020, § 13 Rdn. 38.

〔46〕 参见王华伟：《德国网络平台责任的嬗变与启示》，载《北大法律评论》第 19 卷第 1 辑，北京大学出版社 2019 年版，第 134 页。

放、共享幕后的生态系统的支配者。即便是同样作为私主体参与到网络空间的活动中，网络平台与其他私主体间也分属“枢纽节点”和“普通节点”，由此颠覆了网络空间乌托邦的幻梦。〔47〕这种不平等关系意味着支配和权力。这种权力体现在其他私主体的身上，则是面临“要么接受，要么离开”的格式选项。

在网络平台收集、处理用户的个人信息时，用户除了能在形式上对最初的环节表达同意之外，根本无权在充分知情的情况下参与数据处理的过程，而网络平台不仅免费获取了法律上的特权，且声称自己就是数字生产要素的创造者。在平台服务提供者看来，正是基于其所拥有的庞大的计算能力和尖端算法，孤立的个人信息和行为数据才被组合起来，并被充分挖掘其中潜在的巨大价值。用户个体则不可避免地沦为数字生产的资源，丧失了自我控制和主体性。〔48〕对此，各国大多以立法形式明确了知情同意制度，企图解除平台对个体权利的威胁。然而，数据处理的极度专业性与处理过程的非透明性，往往致使用户根本无法事实上做出“同意”：相比于一般产品而言，用户在收集、理解与运用隐私政策中披露的相关信息时，不仅面临时间、精力、专业、能力方面的难题，也面临系统性风险与不确定性的难题。〔49〕如果说用户对于自身信息被处理的过程中可能遭受何种风险都无法预测，那也就谈不上做出了真正的同意。同时，网络平台所拥有的这种权力也使得拥有公权力的政府难以对其进行有效约束。政府不仅无能力介入数据加工、流转等流程，亦无能力检测平台的数据安全质量，这导致网络平台对于数字公共安全也形成了威胁。〔50〕

要求网络服务提供者承担信息安全的刑法义务，正是力图对其基于技术优势所形成的权力进行纠偏。毫无疑问，这种基于“行动自由—后果责任”而生成的义务是一种基于组织管辖的原初义务。这是一种最低限度的安全保障义务，其具有以下两个特点：其一，这项义务不同于网络服务提供者对国家或个体负有的如一般经营主体的其他义务，不以任何具体主体作为履行义务的对象。其二，该义务内生于网络服务提供者成立之时，贯穿于其为网络用户提供网络服务的全过程，即便是在其退出该领域之时，也需为该义务的履行进行最为妥当的安排。〔51〕基于这种界定，私法保护路径中所提倡的信息信托理论在此就无法适用，该理论主张，网络服务提供者与用户之间应被类比于律师之于用户、医生之于病人、雇主之于雇员的关系，前者相较后者占据专业知识优势且相互间具有委托与信赖关系。网络服务提供者作为受托人必须为了委托方的利益尽到谨慎义务与忠诚义务，但同时受托人也有权利和义务进行自由裁量。〔52〕可是一方面，这种谨慎义务与忠诚义务一般仅在特定主体之间存在，因此与信息安全义务的普遍性不相符合；另一方面，在刑法中，诸如背信犯罪人就是违背基于信赖关系产生的谨慎义务与忠诚义务，但往往被界定为典

〔47〕 参见〔美〕巴拉巴西：《链接：商业、科学与生活的新思维》，沈华伟译，浙江人民出版社 2013 年版，第 85 页。

〔48〕 参见前引〔33〕，张凌寒文。

〔49〕 参见丁晓东：《个人信息保护：原理与实践》，法律出版社 2021 年版，第 98 页。

〔50〕 参见前引〔33〕，张凌寒文。

〔51〕 参见梅夏英、杨晓娜：《网络服务提供者信息安全保障义务的公共性基础》，载《烟台大学学报（社会科学版）》2014 年第 6 期。

〔52〕 参见前引〔49〕，丁晓东书，第 98－99 页；Jack M. Balkin，*Information Fiduciaries and the First Amendment*，49 University of California Davis Law Review 1183（2016）.

型的义务犯，〔53〕理由在于，这种义务并非原生于义务主体，而是基于制度的要求。

相反，对于拒不履行信息网络安全管理义务罪中的另外两项义务，即违法信息的管控义务和刑事证据的保存义务，则应当界定为基于制度管辖所负担的积极义务。尽管立法者将这三项义务全部规定在了同一个法条中，但正如有学者反思的那样，多罪一名是我国刑法罪名体系的显著特征。也即，在我国《刑法》条文当中常有一个罪名实际包含多个犯罪构成的现象。但是其指出，讨论刑法问题的基本平台只能是犯罪构成而不是罪名。〔54〕的确，上述三项义务的对象不同，保护目的指向不同，违反义务所造成的后果也不同，事实上分别对应三种不同的犯罪构成。这个结论也可以在比较法上获得论据。

以德国立法为例，基于“核心刑法—附属刑法”二元分立的立法体例，网络服务提供者的法律责任被规定在1997年的《电信服务法》中，其中第5条就已经明确采取了限缩责任的立场。受到欧盟颁布的《电子商务指令》的影响，德国联邦议会先后多次修订该法并最终于2007年通过新的《电信媒体法》，其中第7条规定了网络服务提供者责任的一般原则，即网络服务提供者对于所传输和存储之信息原则上不负有监督义务。而在第8—10条中，立法者又具体地给三种不同类型的服务提供者规定了免责条件。〔55〕这实际就是避风港原则在德国立法中被采纳的体现。与之相反，有关数据保护的法律条文则规定在《联邦数据保护法》中：该法第42条为刑事罚则，分别针对故意将个人数据向不特定多数人公布的行为、未经许可加以处理或者通过错误信息骗取的行为设置了相应的刑罚后果；第64—66条则分别规定了数据处理中的安全义务、个人数据遭损害时向联邦官员报告的义务和向受害者报告的义务。〔56〕与此类似，我国也早在2006年颁布的《信息网络传播权保护条例》中就引入了避风港原则，即力图限缩网络服务提供者对于违法信息内容的监管义务。但对于数据保护则在《网络安全法》等法律法规中详细明确了数据控制者、处理者的信息安全保障义务。

综上所述，可以认为，我国《刑法》第286条之一所规定的信息安全义务是一种消极义务，适用支配犯的归责原理。

四、信息安全义务的范围划定

在明确信息安全义务之目的与性质的前提下，对该义务保护范围的确定，一方面是厘定保护对象的范围，另一方面则是合理地划定保护边界。

（一）保护对象的厘定

在确定何种用户信息处于该保护义务的范围之内时，应当以信息共享的互惠性风险分配为这一保护目的作为构成要件解释的基点。

---

〔53〕背信犯罪在我国《刑法》中体现为第161条违规披露、不披露重要信息罪，以及第169条之一背信损害上市公司利益罪。参见前引〔40〕，何庆仁书，第124页。

〔54〕参见丁胜明：《以罪名为讨论平台的反思与纠正》，载《法学研究》2020年第3期。

〔55〕参见王华伟：《避风港原则的刑法教义学理论建构》，载《中外法学》2019年第6期；Hilgendorf/Valerius，Computer-und Internetstrafrecht：Ein Grundriss，2. Aufl.，2012，Rdn. 193.

〔56〕Vgl. Schlösser-Rost/Koch，in：Wolff/ Brink，BeckOnline Kommentar，Datenschutzrecht，36. Aufl.，2021，§ 42，§ 64－66.

1. 用户信息与非用户信息

在《刑法》第 286 条之一中，立法者将保护对象限定在用户信息上，在本文看来可以作以下两方面的合理解释：

第一，只有当信息的收集、处理、利用是发生在网络服务提供者和享受服务的用户之间时，两者才处于一个利益与共的共同体关系中。如前所述，数据经济潜力的发挥，必须依靠数据的自由流动、融合以及进一步的创新。因此从数字生产论的角度，社会公众失去对数据保护体系的信任，是一个非常危险的信号。〔57〕但是，只有利益与共的网络服务提供者与用户之间才谈得上相互的信任和依赖，并基于此来巩固互惠分享的关系。

第二，从支配的角度来看，网络服务提供者对于用户信息基于其组织管辖的行为而形成了保护性的支配关系，而支配的另一面则是答责（verantworten）。因此，对于那些非用户的信息，既然网络服务提供者并没有实施收集、处理、利用和流转的组织行为，也就并不负有基于保护性支配而产生的原初义务。除非，对于第三人侵犯该非用户的信息权益或滥用其信息实施违法犯罪的行为，网络服务提供者基于外部制度的要求而履行积极的管辖义务。

以意大利的“谷歌案”加以说明。2006 年 9 月 8 日，谷歌网站上的一段视频展示了一个残疾的大学生被三名同学虐待的过程（其中一个同学正在用他的手机录音，而另外十几个同学则眼睁睁地看着这一幕而无动于衷）。这个残疾学生遭受着自闭症的折磨，其听力和视力也遭到损害，完全成为心理和身体暴力的客体。这个持续 3 分钟的视频被超过 5000 人次大批量地观看。在某一特定时间点上，这个视频甚至位列最受欢迎的娱乐视频。谷歌的用户对该视频评论颇多，其中有一些认为该视频的内容不合适，甚至发邮件给谷歌要求删除该视频。从该视频被放到网上开始，它可供观看的时间已经超过了 2 个月。〔58〕根据《意大利数据保护法》的规定，四名谷歌领导层成员涉嫌非法处理敏感信息却未经过被害人的同意，而且没有得到数据保护机构的授权。法官认定谷歌领导层成员有罪的理由在于，谷歌在处理这些视频的时候，并没有采取足够谨慎的措施去避免对他人隐私的侵犯，尤其是并没有提醒视频上传者要履行消极义务（也就是不要上传这样的视频的义务）。有论者对此批评道，这样的提醒义务与告知数据主体有关数据处理范围和目的的义务并不相同，后者才是可能引发刑事制裁的义务。网络服务提供者的确应当避免侵害第三方的隐私权利，但是其承担赔偿责任的理由在于侵权法上的严格责任原则。因此，该案的审查重心应当转向：上传包含第三方健康信息的视频是否属于违法内容的传播，而谷歌作为网络服务提供者是否有义务来阻止这样的传播过程。〔59〕

2. 用户信息与个人信息

对于“致使用户信息泄露，造成严重后果”的解释，2019 年最高人民法院、最高人民检察院关于《办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第 4 条全面沿用了 2017 年“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

〔57〕 参见前引〔34〕，个人信息保护课题组书，第 44 页。

〔58〕 See Giovanni Sartor & Mario Viola de Azevedo Cunha, *The Italian Google-case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, 18 International Journal of Law and Information Technology 356, 357 (2010).

〔59〕 参见前引〔58〕，Giovanni Sartor、Mario Viola de Azevedo Cunha 文，第 368 页。

释》第5条的规定，特别注意与后者保持衔接和协调，将用户信息区分为高度敏感、敏感和一般信息，数量标准则按照侵犯公民个人信息罪入罪标准的十倍来掌握。〔60〕对此，最高人民法院喻海松法官提醒道，用户信息与公民个人信息存在交叉竞合，但不能等同，除了公民个人信息之外，还应包括账号、密码、数字证书等用于确认操作权限的身份认证信息，上网轨迹、交易记录、浏览记录等网络行为信息，通信信息等，而且基于全面保护的原则，用户信息不限于不能被公开获取的信息。〔61〕但对此还需要进一步予以限定。《刑法》第286条之一不可能旨在保护所有的用户信息，其保护范围要受保护目的的制约。

首先，用户信息肯定包含了公民个人信息，但在保护范围上有必要与侵犯公民个人信息罪有所区分，因为后者主要着眼于个人信息在公法上的受保护权，而前者则更加强调促进数据的互惠分享。对于高度敏感信息和敏感信息而言，对公民个人信息的保护与对数据互惠分享的保护具有一致性，因为这两类信息毫无疑问对于公民个人具有重大利益上的关联性，一旦遭到泄露、滥用而造成严重的人身或财产损害，自然人用户整体上将会丧失对网络服务提供者的信任，必定阻碍数据的提供和共享。但对于其他个人信息或与个人有关的信息是否要纳入用户信息义务的保护范围，则需要考虑该信息之于用户个人重大利益的相关性以及该信息是否主要具有公共属性和流通属性：(1) 对于没有公开且对个人的人身、财产安全至关重要的一般信息，例如网银账号和密码等，应当纳入保护范围。(2) 对于没有公开但对个人的人身、财产安全并无直接影响的一般信息，例如上网轨迹、交易记录等，考虑到这些信息之于数字经济的潜在价值，不应当纳入保护范围。(3) 对于已经公开的个人信息，应当按照情境原理考察其后续利用是否会显著违背信息主体的合理期待。不过原则上来说，由于第三方是否会滥用已公开的个人信息从事侵害权利人等违法犯罪活动，已经脱离了网络服务提供者的支配范围，不应当强制其履行保护义务，但是，一旦网络服务提供者已经明显认识到个人信息会被用于违背信息主体合理期待的目的，就不能被免除阻止该信息滥用过程的义务。(4) 单纯的数据财产权交易，尽管并未征得用户同意，但由于交易双方对该用户数据的使用场景相同、目的也一致，不会带来额外的隐私风险，也不会打破用户的合理预期，〔62〕所以也不应当被纳入到信息安全义务的范围之中。

其次，用户信息还应当包括企业信息。在文义上，相较于个人信息而言，将用户信息解释为包括企业信息实际面临更少的障碍。〔63〕在合目的性上，对企业信息权益的保护也有助于促进数据的互惠分享：对于企业拥有的半公开或者未公开数据，如果法律提供了足够保护，避免数据的公开与获取对企业形成竞争劣势，那么企业就会选择更多地公开此类数据或信息。相反，如果法律没有对企业的商业秘密或者涉及竞争利益的数据提供足够保护，那么就会促使企业采取更为严格的保密措施或设置反爬虫等技术壁垒，〔64〕这显然不利于数据的互惠分享。当然，相较于个人信息而言，

〔60〕 参见缑杰、吴峤滨：《〈关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释〉重点难点问题解读》，载《检察日报》2019年10月27日，第3版。

〔61〕 参见喻海松：《网络犯罪二十讲》，法律出版社2018年版，第88页。

〔62〕 参见张忆然：《大数据时代“个人信息”的权利变迁与刑法保护的教义学限缩——以“数据财产权”与“信息自决权”的二分为视角》，载《政治与法律》2020年第6期。

〔63〕 参见王肃之：《论法人信息的刑法保护》，载《中国刑事法杂志》2020年第3期。

〔64〕 参见丁晓东：《论企业数据权益的法律保护——基于数据法律性质的分析》，载《法律科学（西北政法大学学报）》2020年第2期。

企业信息具有更多的公开性和公共性，因此需保护性应有所降低。对于第三方抓取开放数据的网络爬虫等行为，既然其本身不构成侵权和犯罪，那么网络服务提供者自然没有义务予以阻止；相反，对于未经授权抓取限制访问、获取数据的行为，网络服务提供者原则上负有阻止义务。〔65〕

（二）保护边界的划定

保护义务边界的确定应兼顾目的性和正当性的考量：一方面，履行保护用户信息的义务能够保障信息共享的互惠性风险分配机制；另一方面，也要防止该义务的过度科处给义务主体的基本权利带来不当侵蚀，因此，义务的科处必须具有事实上的可能性和规范上的可期待性。

1. 保护边界的目的性划定

如前所述，刑法通过保护用户信息权益来实现信息互惠共享的终极目的。问题在于，网络服务提供者拒不履行保护义务导致用户信息出现何种程度的损害后果时，才会被认为破坏了信息共享的互惠性风险分配机制呢。这里涉及两项构成要件要素的解释：一是用户信息泄露，二是造成严重后果。

用户信息泄露，一般是指信息被未经授权地访问、窃取或公开，涉及对信息的机密性和完整性的破坏。〔66〕但是，保障信息互惠共享的规范目的会将破坏信息可用性的行为同样视为破坏互惠性风险分配机制，从而应当将其纳入“泄露”的定义中来。例如个人、企业的信用记录被第三方出于报复目的而更改或者删除，导致个人、企业遭到歧视或遭受名誉和经济上的损失，其危害性绝不亚于狭义上的数据遭泄露或者丢失的后果。因此，《欧盟数据保护条例》第 4 条定义的第 12 项就明确写道，“个人数据泄露”是指个人数据在传输、存储或进行其他处理时的安全问题引发的个人数据被意外或非法破坏、丢失、更改、未经授权披露或访问。〔67〕

对于严重后果的解释，2019 年“两高”颁布的《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第 4 条划分了以下几类情形：一是用户信息的大量泄露，二是用户信息泄露导致人身伤害，三是用户信息泄露导致重大经济损失，四是用户信息泄露导致社会秩序的严重混乱。这反映了信息泄露后果兼具实体性和非实体性的类型：实体性后果诸如人身伤害或者经济损失容易被识别和量化，而非实体性后果包括信息泄露导致未来实体性侵害的风险显著增加、个体因此焦虑不已、社会因信息大量泄露而动荡不安。〔68〕基于信息泄露的损害特点，对于义务违反与损害结果间因果关系的要求可以做出适当缓和，从而更加周延地保护法益：其一，对于因信息泄露导致的自伤、自杀等原本应当由被害人自我答责的后果，应当纳入严重后果当中；〔69〕其二，网络服务提供者的义务违反并不一定单独导致了损害后果，对此可以采纳累积犯的法理，让网络服务提供者为自身义务违反所导致的信息泄露负责。例如在人肉搜索案件中，某个体的多类敏感信息被从不同的网站上非法获取，最终形成损害该个体名誉并造成其自杀后果的用户画像的，〔70〕网络服

〔65〕 参见杨志琼：《数据时代网络爬虫的刑法规制》，载《比较法研究》2020 年第 4 期。

〔66〕 See Clara Kim, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2 Columbia Business Law Review 544, 548 (2016).

〔67〕 参见中国信息通信研究院互联网法律研究中心、京东法律研究院编：《欧盟数据保护法规汇编》，中国法制出版社 2019 年版，第 56 页。

〔68〕 参见解正山：《数据泄露损害问题研究》，载《清华法学》2020 年第 4 期。

〔69〕 有关“缓和的结果归属”的学理论述，参见张明楷：《论缓和的结果归属》，载《中国法学》2019 年第 3 期。

〔70〕 Vgl. Kubiciel/Großmann, Doxing als Testfall für das Datenschutzstrafrecht, NJW 2019, 1050 ff.

务提供者应当为自己违反规范的累积危险行为个别性地承担刑事责任。〔71〕

为防止以上损害后果的发生，理应在法律和行政法规的框架之内，从技术性措施和管理性措施两个面向全面构建网络服务提供者的信息安全义务。根据《网络安全法》第42条、《中华人民共和国民法典》第1038条以及《中华人民共和国个人信息保护法》第51条的规定，信息处理者应当对个人信息进行分类管理并采取加密、去识别化等技术措施，防止未经授权的访问、泄露、篡改、丢失。在实际的信息安全等级保护制度中，不同分级配套的管理规范和技术标准构成了安全保护义务的主要内容，而保护等级则由两个定级要素决定：保护对象受到破坏时侵害的客体和对客体造成侵害的程度。只要根据保护等级要求落实了所有项的要求，就被认为履行了安全保护义务。但是，仅仅以侵害后果为着眼点采取保护措施，忽略了动态变化的侵害频率，而且，静态式的合规措施并未考量网络安全攻防技术的进步，仅仅达到安全底线也并不意味着保护了用户安全的实质需求。〔72〕对此，应当更加重视以管理为基础的规制以避免刻舟求剑式的技术措施导致的漏洞，具体来说：（1）在事前的风险预防阶段，网络服务提供者应当以风险评估机制的建立为中心，制定对用户信息的保护策略，按照最先进的保护标准定期对风险变化进行评估并适时调整保护策略。在此过程中，尤其要考虑到与第三方主体的交往过程中是否履行了必要的谨慎义务，以避免黑客等侵入者借助第三方通道来达到非法获取用户信息的目的。（2）在事后的实害阻止阶段，网络服务提供者应当及时采取补救措施防止损害的发生或扩大，同时应当履行法定的对监管部门和权利主体的通知义务，以便后者及时采取补救或自救措施。除非其所采取的措施能够确保用户信息即便泄露也不会导致损害后果。（3）在全过程的风险防控中，互联网公司领导层需要制定组织计划，将数字生产所应承担的危险识别、观察及消除的义务分配给数据合规官以及公司执行层成员。〔73〕较为清晰地划分各成员间的负责范围，有助于反制现实中责任意识稀薄化的现象。领导层成员还负有义务对组织计划的可靠性进行持续监管，因此其应当谨慎选任有资质的监管人员，持续向成员充分讲解与其履职相关的法律法规，并为担负相应职责的成员提供足够的配备。〔74〕

2. 保护边界的正当性基础

按照支配犯的法理，只有创设风险的行为人才负有义务消除风险。同时，为了控制义务的目的性追求所内含的危险，有必要从事实和规范两个层面对其加以限定：一方面，义务的履行必须在事实上具有可能性，也就是说采取保护措施能够有效避免损害后果的发生；另一方面，义务的履行在规范上应当具有可期待性，行为规范的设立应使得相关主体间的利益取得相对平衡。

首先，只有当信息泄露风险是由网络服务提供者共同创设时，其才有义务消除风险。如果该风险是由侵害方和用户通过互动过程共同创设的，那么只要网络服务提供者在技术和管理措施上没有失职行为，就不应当为损害后果的发生承担责任。例如，在著名的“机票款项诈骗案”中，

〔71〕 参见张志钢：《论累积犯的法理——以污染环境罪为中心》，载《环球法律评论》2017年第2期。

〔72〕 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》，载《环球法律评论》2016年第4期。

〔73〕 Vgl. Dannecker/Dannecker, Fahrlässigkeit in formalen Organisationen, in: Knut Amelung (Hrsg.), Individuelle Verantwortung und Beteiligungsverhältnisse bei Straftaten in bürokratischen Organisationen des Staates, der Wirtschaft und der Gesellschaft, 2000, S. 217.

〔74〕 Vgl. Eidam, Unternehmen und Strafe, 5. Aufl., 2018, § 7 Rdn. 107 ff.

被害人通过某订票网提供的电话预订机票，被客服人员要求用网银汇款。被害人汇款后虽查询扣款成功，但对方称钱未到账，还需要通过 ATM 联网操作使付款生效。被害人按照其引导在 ATM 上输入所谓 18356 的激活码（实际输入到转账数额一栏），之后相应数额随即被转入诈骗人的账户。〔75〕 在本案中，信息泄露或数据丢失的风险是由诈骗行为人而不是网络服务提供者创设的，因为没有证据表明后者在系统安全上存在漏洞。而且，银行系统本就是为了帮助用户实现自主利益而设立，既然用户基于“自愿”主动向对方提供自己银行账户的信息，那么银行系统的运营者就不可能反过来审查该交易的真实性和合法性。

其次，只有当网络服务提供者有能力履行义务以避免结果的发生时，才应当为损害结果的发生负责。遵守规范的前提是拥有遵守规范的能力，不能超越规范接收者的实际能力对其设定义务。因为作为义务的规范只是告诉行为人应当采取何种方式避免结果的发生，但它没有表明行为人在何种程度上受到义务的约束，也就是说，在何种程度上，行为人必须为了实施合义务的行为而将他的能力维持在必要的水平之上。对于这一问题的回答属于刑法中制裁规范的任务，也即，在何种条件下，要将刑罚施加于一个违反规范的行为。〔76〕 某一行为是否合乎规范，是一个应从事后予以回答的逻辑的推演问题。但只有当行为人本可以实施与当为命令相符且能够阻止结果发生的合法替代行为时，他所实施的违反规范的行为才能被作为义务违反归责于他。因此，只有在具备足够的行为能力的范围内，一个规范接收者才受到规范的约束。〔77〕 所以，必须在具体情境下检验作为义务的履行是否能够有效避免损害结果的发生。事前风险预防义务的履行，如果能够在很大程度上避免损害后果的发生，就应当认为义务具备履行可能性。事后实害阻止义务尤其是通知义务的履行，由于涉及通知对象之自由决定的介入，在判断合义务的替代行为能否避免结果发生时，应当采取规范论的思维，假设监管人员等负有处置义务的主体会按照义务的要求履行监管职责，〔78〕 在此基础上来判断通知义务对于阻止结果发生的实效。此外，只有当义务的设置充分考虑了义务主体的社会角色及其相应的利益需求，使得义务主体为履行该义务不必过度牺牲行动自由时，该义务的履行才具有规范上的可期待性。对于网络服务提供者而言，保护义务的承担应当以合乎比例的经济利益的损失为前提，〔79〕 只能要求其将信息安全风险降低到一个相对可接受的范围之内，而不是绝对地消除风险。当其保护措施足以实现这一目的时，不应当要求其承担更高的注意义务。

五、结　论

网络信息犯罪的治理绝不只是在封闭的法律体系内部进行，而必须是在法律系统与其他社会

〔75〕 参见秦新承：《认定诈骗罪无需“处分意识”——以利用新型支付方式实施的诈骗案为例》，载《法学》2012 年第 3 期。

〔76〕 Vgl. Kindhäuser, Erlaubtes Risiko und Sorgfaltswidrigkeit, GA 1994, S. 200.

〔77〕 Vgl. Kindhäuser, Gefährdung als Straftat: rechtstheoretische Untersuchungen zur Dogmatik der abstrakten und konkreten Gefährdungsdelikte, 1989, S. 50.

〔78〕 Vgl. Puppe, Brauchen wir eine Risikoerhöhungstheorie? FS-Roxin, 2001, S. 287；徐凌波：《义务违反的竞合与结果可避免性》，载《南京大学学报（哲学·人文科学·社会科学）》2018 年第 2 期；喻浩东：《不作为因果关系判断中的自由意志与规范假设》，载《政治与法律》2022 年第 4 期。

〔79〕 Vgl. Georg Freund, Strafrecht Allgemeiner Teil, 2. Aufl., 2009, § 1 Rdn. 20.

子系统的有效沟通中进行。信息安全守门人刑法义务的构建，首先应当关注数字经济系统的保护需求，在此基础上确定刑法规范的保护目的与规制需要，进而确定该义务的具体内容。通过以上体系化的论述，本文得出以下结论：

其一，信息安全义务的目的既不是保障用户信息专有权，也不是维护信息网络安全管理秩序，而是保障信息共享的互惠性风险分配机制。

其二，信息安全义务的性质是支配犯的消极义务，而不是义务犯的积极义务。该义务的科处是对网络服务提供者的数字生产权力的纠偏。

其三，信息安全义务的范围基于该义务的保护目的和义务性质得以实质地厘定。对该义务的保护对象和保护范围的确定，既应当促成规范目的的实现，也应当为其提供正当性的基础，从而对目的追求所内含的危险进行必要控制。

Abstract: The addition of the crime of refusing to fulfill the obligations of information network security management provides a basis for the criminal law obligations of information security gatekeepers in cyberspace. In view of the dilemma encountered in judicial practice, it is necessary to carry out a systematic interpretation of the purpose, nature and scope of information security obligations in doctrine. In terms of purpose construction, both the exclusive right to user information and the maintenance of information network security management order have insurmountable defects. A systematic coupling view of legal interests should be advocated, defining the purpose of the obligation as a reciprocal risk allocation mechanism to guarantee information sharing, in order to achieve effective communication between the legal system and the digital economy system. In terms of nature definition, the obligatory offense theory misunderstands the basis for the creation of positive obligations, and improperly confuses dominant offenses with acting offenses, and obligatory offenses with inaction offenses. The essence of information security obligation is the correction of the digital production power of network service providers, so it should be classified as a negative obligation based on organizational jurisdiction rather than a positive obligation based on institutional jurisdiction. Based on the clarification of the purpose of protection and the nature of the obligation, the scope of protection of the obligation should be determined in order to achieve the normative purpose of guaranteeing the reciprocal risk allocation mechanism of information sharing, and also to justify the control of the dangers inherent in it.

Key Words: internet service provider, information security gatekeeper, systematic coupling view of legal interests, crime of refusing to fulfill the information security management obligations

（责任编辑：简　爱　赵建蕊）