基于信息生态理论的个人数据保护策略研究

——由英国下议院《网络安全:个人在线数据保护》报告说开去

Personal Data Protection Strategy Research Based on the Theory of Information Ecology

——Take the *Cyber Security*: *Protection of Personal Data Online* by British House of Common Culture, Media and Sport Committee as an Example

韩秋明

(中国科学技术发展战略研究院,北京,100038; 南开大学经济与社会发展研究院,天津,300071)

[摘要] 介绍信息生态理论的核心思想,通过包含信息人和信息环境在内的信息生态理论框架分析英国下议院文化、媒体和体育委员会近期发布的报告《网络安全:个人在线数据保护》,剖析涉及其中的英国信息专员办公室、TalkTalk 公司及其用户、第三方合作机构、公共安全部门等信息人在个人数据保护生态系统中的角色和生态位,概括《报告》中对以上信息人提出的建议,总结相关经验和做法;在此基础上,分析在线个人数据保护生态系统中存在的生态链割裂、生态位失位、生态系统失衡等问题,从信息人和信息生态环境等方面剖析产生问题的可能原因,并构建个人数据保护的宏观机制和提出解决问题的微观策略。

[关键词] 大数据 个人数据保护 信息安全 信息生态 数据泄露 《网络安全:个人在线数据保护》报告

[中图分类号] G351 [文献标识码] A [文章编号] 1003-2797(2017)02-0094-11 DOI:10.13366/j.dik.2017.02.094

[Abstract] This paper introduces the core ideas of the information ecological theory, analyzes the report recently released by British House of Commons Culture, Media and Sport Committee named *Cyber Security*: *Protection of Personal Data Online* by information ecological theory framework including information man and information circumstance, elaborates the roles and ecological niches of the UK's Information Commissioner's Office, TalkTalk and its users, third-party partner agencies, and public safety agencies in the personal data protection ecosystem, summarizes it's experiences and practices in this theory frame; On this basis, the article analyzes the existing problems of online personal data protection ecosystems, such as ecological chain fragmentation and ecosystem imbalance; Then this work tries to find the possible cause of the problem, establishes personal data protection macro mechanism and proposes appropriate countermeasures.

[Key words] Big data Personal data protection Information security Information ecology Data branches *Cyber Security*: *Protection of Personal Data Online*

1 引言

近年来,从电影明星、大学教授再到刚入学的大学生,因个人信息泄露产生的欺诈案件层出不穷,造成的社会影响极其恶劣。在云计算时代,大部分信息服务者都会将客户的数据存储在云服务器中,这给日渐增多的网络攻击带来了机会,也为用户个人数据的保护带来了挑战。为保证合法、价值最大化且安全地

[基金项目] 本文系国家社科基金项目"虚拟社区中的信息交流与导控机制研究"(11CTQ026)的成果之一。

[作者简介] 韩秋明,男,助理研究员,博士后,研究方向:信息服务、技术预测与评价,Email:hanqiuming2222@gmail.com。

使用用户个人数据,平衡信息服务者、用户、信息技术、第三方服务商等多个主体的价值利益,以追求更高的"数据红利"[1],需要多方协作,共同构建健康、合理的个人数据保护信息生态。

信息生态是指在某一环境下,由信息人、社群、组织、信息行为、价值和信息技术共同构成的有机整体[2]。2016 年 7 月 27 日,中共中央办公厅、国务院办公厅印发了《国家信息化发展战略纲要》,在其第五部分中特别强调要加强网络生态治理,"维护公民合法权益……全面规范企业和个人信息采集、存储、使用等行为,防范信息滥用。加强个人数据保护,依法打击网络违法犯罪。"[3]

个人信息保护问题也是世界各国共同面临的问题之一。2016 年 6 月 15 日,英国下议院(House of Commons)文化、媒体和体育委员会(Culture, Media and Sport Committee)发布了一份报告,主题是《网络安全:个人在线数据保护》(Cyber Security: Protection of Personal Data Online)(以下简称报告)[4]。该报告对各利益相关者所做的有关个人数据保护的一系列工作做了详细阐述,并提出了许多建议。报告中涉及到政府部门、公安部门、企业、第三方服务商、客户,以及社会大众等诸多信息生态系统组成要素。从这个角度来说,该报告为个人数据保护生态系统的构建和优化提供了一些指导,总结其经验将会对我国网络生态治理提供参考,为个人数据保护的措施提供借鉴,为即将于 2017 年 6 月开始实施的《中华人民共和国网络安全法》增砖添瓦。

2 个人数据保护生态系统研究的理论基础

信息生态理论是研究信息生态系统构建及其应用研究的理论基础,其核心思想是强调信息人与信息环境之间的关系,主张合理分化信息生态位,正常发挥信息生态系统功能,达到某种平衡的状态[5]。

对信息生态系统的构成,David[6]、Nardi[7]、Malhotra[8]等不同学者都做出过相关界定。总的来说,信息生态系统由信息人和信息生态环境构成,其中信息人包括信息生产者、服务者、消费者和监管者,信息生态环境包括信息本体、信息技术、信息时空和信息制度[9]。

2.1 个人数据保护生态系统中的信息人

(1)信息生产者。大数据时代下的信息生产者与传统信息生产者有所不同。传统信息生产者主要是图书馆、科研机构、科研人员等[10],在新媒体环境下,用户已经成为信息生产者中的一员,他们生产自己的社交信息、地理位置信息、个人喜好信息等。

(2)信息服务者。个人数据保护生态系统中的信息服务者负责将信息生产者产出的信息向社会传递、传播和扩散,并将收集、整理后的信息通过一定的策略向用户提供相应的产品和服务。

(3)信息消费者。在信息生产者、服务者多元化发展的环境下,信息消费者也呈现出多元的特点。用户无疑是信息消费者之一。此外,随着信息服务种类的精细化,一些服务机构在提供增值扩展服务的同时,还会与第三方服务机构开展合作,共同使用和消费用户信息。

(4)信息监管者。信息监管者主要是对信息活动进行监督和管理的个人或组织。宏观层面上,主要是服务信息服务监管的政府机构,如我国的网信管理部门,英国的信息专员办公室等。微观层面上,信息服务者也应承担部分信息监管的责任,特别是针对第三方合作机构对用户信息的访问和使用等。

2.2 个人数据保护生态系统中的信息生态环境

(1)信息本体。个人数据保护生态系统中的信息本体主要是用户的信息内容和承载信息内容的载体,如存储在信息服务平台服务器中的用户的姓名、性别、年龄、电子邮件、联系方式、家庭住址、银行卡号、通信账号、服务使用记录等。

(2)信息技术。这里的信息技术主要指信息安全技术。随着大数据、云计算等技术的普遍应用,移动终端、云端、社交平台产生的数据彼此紧密相连。要保护用户个人信息,需采取一定的信息安全技术,如云端代理访问、适应性访问管控、端点侦测及回应等。特别还要注意 SQL 攻击,信息安全公司 Infosec 表示,SQL 的易感染性是"在网络程序中最常见的漏洞之一"[11]。

(3)信息时空。对于个人数据保护生态系统来说,随着移动互联网和移动终端的飞速发展,用户个人信息活动的时间空间壁垒都基本被打破,因此信息

时空泛化为存在网络连接的任何时空。

(4)信息制度。信息制度是在个人数据保护生态系统中,用来约束信息人行为的导向性文件、伦理、规则、标准、法律及政策的集合。世界上主要国家或地区组织都出台过相关信息制度或法律,如欧盟的《有关个人数据自动化处理之个人保护公约》及其修正案、英国的《数据保护法案》、美国的《网络环境下消费者的数据隐私保护》法案和日本的《个人信息保护法》等[12]。

3 《网络安全:个人在线数据保护》报告分析

信息生态理论认为,信息人是信息生态系统中的核心要素[13],起着主导作用,信息生态环境是为信息人及其信息活动提供支持和保障的,如信息本体是信息人生产、扩散、流转的关于信息人的信息,信息技术则是为信息人的活动提供便捷、安全、高效的技术保障,信息时空是为信息人提供的时间和空间,而信息制度则是引导、管理、规范信息人行为的规则体系。因此,本节在具体分析过程中,将以《网络安全:个人在线数据保护》报告中的信息人为主线,介绍涉及的多种信息人,以及对信息人的相关建议,其他信息生态系统环境要素将融合在分析之中,不再单独列出。

3.1 该报告出台的背景

2015 年 10 月 21 日,一起针对电子通信和互联网服务提供商 TalkTalk[注1][14] 的网络攻击事件,导致该公司的用户网站在当日下线。10 月 23 日,TalkTalk 表示此次"重大且持续的网络攻击"事件正在由伦敦警察局网络犯罪调查科(Cyber Crime Unit)展开调查(因为用户遭到了网络诈骗),并且用户姓名、地址、出生日期、电话、电子邮件、账户信息、信用卡以及银行卡详情都有可能被盗用。10 月 26 日,TalkTalk 数据泄露成为英国下议院紧急会议的主题。该委员会表态将会紧密跟踪与网络攻击事件相关的进展。

TalkTalk 公司的信息泄露只是此次调查报告的直接原因。从宏观层面来看,由于互联网的国际化,个人数据保护的形势日益严峻,这起事件只是众多已经发生并且仍在持续发生的信息泄露事件中的一件。由英国文化、媒体与体育部(Department for Culture, Media and Sport,DCMS)最新发布的 2016 年网络安全漏洞调查发现,90%的大型组织已经经历过至少一次信息泄露,且有 25%的公司一个月最少经历一次网络信息泄露[15]。英国信息专员办公室(Information Commissioners Office,ICO)的调查表明,数据泄露并不止存在于通讯行业,医疗卫生才是发生数据泄露最多的领域,其次是当地的政府。技术英国(TechUK)估算因网络犯罪导致的数据泄露一年给英国带来约 340 亿欧元的损失,而 2010 年时这个数字是 270 亿欧元[16]。

由此可见,此次报告出台的背景是在全球公共服务"数字化"进程下,越来越多的公共服务都将海量的个人数据存储在网络上,而一旦网络安全受到侵犯,个人数据的泄露将会给经济社会带来巨大的损失。

3.2 该报告涉及的信息生态要素

报告对 TalkTalk 数据泄露事件做了详细的调查,涉及多个信息人。总的来看,主要信息人有政府管理部门、数据泄露的公司及用户、第三方公司、公共安全部门等。该报告对各个信息人发挥的作用进行了描述,并有针对性的提出了建议。

(1)政府管理部门。在英国,英国通信管理局(Office of Communications)是电子通讯以及网络服务的监管者。对于信息泄露事件来说,最主要的管理部门是信息专员办公室(ICO),它由数据保护法案(Data Protection Act)授权监管。隐私与电子通信条例(Privacy and Electronic Communications Regime,PECR)要求电信公司和通信服务提供商要在 24 小时之内向信息专员办公室报告任何一个信息泄漏事件。

(2)数据泄露的公司及用户。数据泄露的公司及其用户是数据泄露事件的直接受害者。该报告中写到,在数据泄露事件发生之后,TalkTalk 用户接到了一些诈骗的邮件和电话,造成了经济损失,并声称遭到了黑客的持续跟踪。实际上 TalkTalk 在泄露事件发生前采取过一些防范手段,如在 1 年内定期写信给用户,告知他们当客户服务代理人员代表公司给他们打电话时会搜集哪些信息以及不会搜集哪些信息。网络攻击之后,TalkTalk 也联系了银行,让其监管客户账户,并且给消费者团体和公民咨询局(Citizens Advice Bureau)提供建议。客户服务研究协会(Institute of Customer Service)认为 43%的用户担心网络攻击会危及他们的个人信息并带来财产损失。

(3)第三方公司。第三方公司包含第三方咨询公司、承包商和供应商。第三方咨询公司比如普华永道,它曾代表代表英国商务、创新和技能部(Department for Business, Innovation and Skills)执行 2015 年信息安全漏洞调查,并且在 TalkTalk 数据泄露事件发生之后还受到委托来进行系统安全审计。承包商和供应商是企业供应链中不可或缺的组成部分,但也是数据泄露的潜在威胁。Intel 公司的调研显示,43%的威胁是由雇员、承包商以及第三方供应商引起的[17]。

(4)公共安全部门。公共安全部门主要负责数据泄露之后的犯罪调查。对于警察局来说,为尽快捕获罪犯而希望将事件控制在一定范围内,不希望对外公布太多信息以影响刑事调查;而数据泄露的公司则出于对用户负责的态度和义务,希望第一时间将事件通报给客户以及与客户利益相关的单位(如银行),这种复杂的矛盾关系目前尚未得到有效解决。

(5)网络黑客或网络诈骗犯。网络黑客会在窃取用户数据之后,有针对性的通过模拟用户或者诱骗用户授权的方式侵入用户的电脑系统,并进一步获取存储在电脑中的各种信息。网络诈骗犯则会冒充信息服务者或第三方服务商,通过邮件、电话等方式与用户取得联系,获取用户信任,并套取用户的银行卡、信用卡等信息,或诱导用户进行不合理消费和电信诈骗等犯罪活动。这些行为在 TalkTalk 数据泄露事件后都得到验证。

3.3 该报告对保护个人数据的建议

针对数据泄露过程中的各个信息人,该报告也提出了一些建议。

3.3.1 政府管理部门

ICO 是主要的信息保护管理部门。报告对该机构的建议主要有:

(1)对事件、已有资源的优先级做出评估。ICO 的管理事务很繁重,但执法人员仅有 30 余人,每年大约要处理约 1000 起案件和近 20 万个公共咨询,尽管有些案件不需要深入调查,但很明显人力资源是缺乏的,因此需要对事件和资源的优先级做出合理评估。

(2)提高事件瞒报漏报的罚款金额,并提升对数据拥有者的处罚力度。目前 ICO 对数据泄露事件的瞒报漏报只收取 1000 英镑的罚款,并对那些没有给客户提供通信安全指导且造成用户损失的组织的罚款最高额为 50 万英镑。这对大公司来说并不是有效的威慑,该报告建议从目前的最大额 50 万英镑扩展到该组织全球营业额的 4%,或者 2000 万欧元。报告还建议 ICO 开始编制指导文件来提高英国的数据控制者的自控意识,如在数据管理法案中增加有效威吓的语句(如判处监禁等),以此让法院对个人信息的非法使用进行有效裁决。

(3)牵头相关部门,强化对用户损失的赔偿。当前对于信息泄露带来的损失,个人只能通过上法院起诉才能够索赔,而且没有直接经济损失证据的赔偿则更加困难。报告建议 ICO 联合有关机构(如公民咨询局和警察局受害者支援部门等)为客户通过简单申诉程序获取赔偿提供咨询和建议,为其成员在遭受数据泄露影响之后寻求赔偿时提供指导和帮助。

(4)创建隐私保护标签。ICO 将推出隐私保护标签(Privacy Seal)计划。这个标签将授予那些展示了良好隐私保护实践和实现了高度数据保护遵从性标准(high data protection compliance standards)的组织。它可以帮助客户了解哪些公司采取了数据保护标准,哪些公司取得了进步,哪些公司则还没有重视数据保护。

(5)联合相关机构发布信息通报的最佳实践。ICO 应该发布进一步的通知相关主管部门的指导意见和包含如何以合适的方式通知受害者的最佳实践案例,以此来维持保护对警察调查十分重要的信息和尊重消费者/客户对泄密警示的需求之间的平衡。

3.3.2 有潜在数据泄露风险的公司

针对数据拥有者和控制者,报告提出的建议如下:

(1)与客户建立联动机制。报告建议信息服务机构定期写信(或电子邮件)给用户,告知他们当客户服务代理人员代表公司给他们打电话时会搜集哪些信息以及不会搜集哪些信息。如果出现信息泄露事件,则尽快核实有多少用户受到影响。如果对个人或用户来说有很大的受损风险,则应尽快告知用户相关事件,防范进一步的损失。

(2)限制数据的集中访问。额外数据汇集的脆弱性是信息服务机构需要迫切解决的重要问题。应对

的办法之一可能是提升安全要求,并对需要访问大量个人数据的机构进行背景检查,并应该设法控制和限制特别集中的数据访问。

(3)CEO 的薪酬与网络安全挂钩。公司日常的网络安全责任应该很明确地与某一具体人员相关,例如,首席信息官或是安全总管。一次重大的网络攻击很适合考察 CEO 应对危机的能力。为了保证 CEO 能对信息安全高度重视,CEO 薪酬的一部分应该与其有效挂钩。

(4)进行网络安全情景演练。尽管 42%的大公司有至少一项网络突发事件管理规划,但只有 29%的公司有正式的书面网络安全政策,且仅有约 10%的被调研公司有相关规划。因此,报告强调了"全力推行企业或组织机构的网络安全情景训练和实战演习"的重要性。

(5)服务合同中增加相关条款。目前通信服务商的合同里没有清晰地说明由于数据泄露而造成用户经济损失可以作为提前终止合同的必要条件。通信和电信公司应该用简单易懂的文字在服务合同中对这一点进行告知和阐明,这样客户在选择服务和产品时就可以做出明智的选择。

(6)加大信息安全技术投资。考虑到电子商务对全球经济的重要性和电子化服务的普及,以及日渐增加的网络攻击威胁,报告认为企业需要在网络安全防护方面不断的投资,来保证他们的技术领先于犯罪分子和黑客。

(7)信息安全情况年报机制。除了加强投资,还需要论证这些资金投入是否有效。因此,报告建议持有大量个人数据(员工、客户、患者、纳税人等)的组织每年应该向 ICO 报告以下情况:①员工网络安全意识培训;②上一次安全流程审计的时间,审计人是谁,采用的什么标准;③是否拥有事件管理计划,以及上次测试的时间;④对现有的和潜在的客户及供应商提供了哪些验证通讯真实与否的渠道和指导;⑤从客户处获得核实通讯真实性的请求数量;⑥意识到的遭受攻击的次数,以及攻击是否成功(造成真正的数据泄露)。

报告还建议应该鼓励企业或者组织在提交的报告中附上年度账目数据,表明他们已采取有效的流程和严格的安全举措,以此来给予客户、股东和供应商信心。

3.3.3 第三方合作公司

在 2016 年网络漏洞调研中,只有 34%的大公司为他们的供应商设定了网络安全标准[18]。报告建议所有电信公司和在线零售商,以及其他易受网络攻击的组织,都应该采取措施来确保它们符合数据保护条例的规定。另外在选择第三方供应商时将网络要素计划(Cyber Essentials)作为主要标准。

3.3.4 社会大众

由于网络诈骗犯对消费者的攻击不断增加,有效的回应措施是提高用户识别欺骗的方法以及自我保护的意识。报告认为有必要提高用户防范网络、电话诈骗以及电话骚扰的意识,因为用户也有在网络上保护自身的责任。政府应该发起一个公共宣传活动,并在活动中进行相应的测试。

4 个人数据保护存在的信息生态问题

通过对上述数据泄露事件和《报告》的分析,可以看出当前阶段个人数据保护信息生态系统的构建还存在着诸多普遍性问题。

4.1 个人数据保护生态系统中的存在的问题

(1)个人数据保护生态链割裂。在信息活动过程中,用户的信息需求和信息人的价值追求共同作用,会形成连接不同类型信息人的信息生态链。自然界的食物链是依靠能量流来连接,而信息生态链则是由信息流来连接。

正常的信息生态链中,四类型的信息人之间存在着信息流转与反馈的平衡,信息生产者信息流向信息服务者和信息监管者,信息服务者信息流向信息监管者、第三方合作者和用户,用户信息流向信息服务者,并且与第三方合作者之间有间接信息流动,每条信息流都包含相应的反馈,如图 1 所示。从《报告》中反应的现实来看,目前个人数据保护存在着信息生态链割裂的问题。信息生产者和信息服务者出于维护自身名誉和信息监管者对相应责任惩罚力度不大的考虑,有时会对信息泄漏事件进行瞒报和漏报,且不会通知用户和第三方合作者(如银行等)进行防范,信息监管者因此无法及时对社会发布相关措施,无法惩治网络

犯罪分子，也无法为避免损失制定相应的政策。这时，由于信息链的割裂，各主体间信息流转速度减慢、流转方向阻断、流转功能减弱，信息消费者与信息服务者之间唯一的信息流中断，却与网络犯罪分子建立起一条犯罪信息流，网络犯罪分子会通过电子邮件、电话等方式与用户取得联系，利用盗窃的信息和数据骗取用户的信任，取得用户的“反馈”，造成用户经济和财产损失，如图 2 所示。

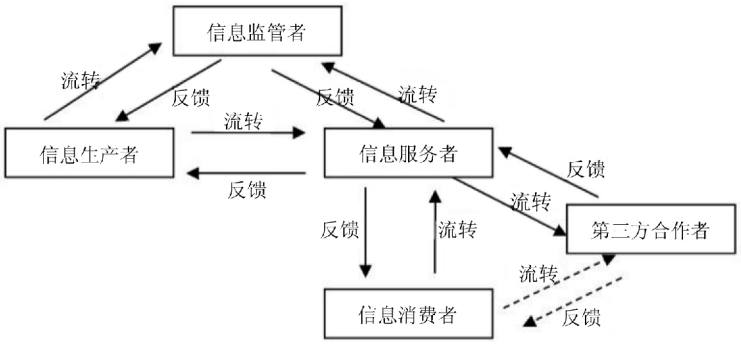

图 1　健康的个人数据保护信息生态链

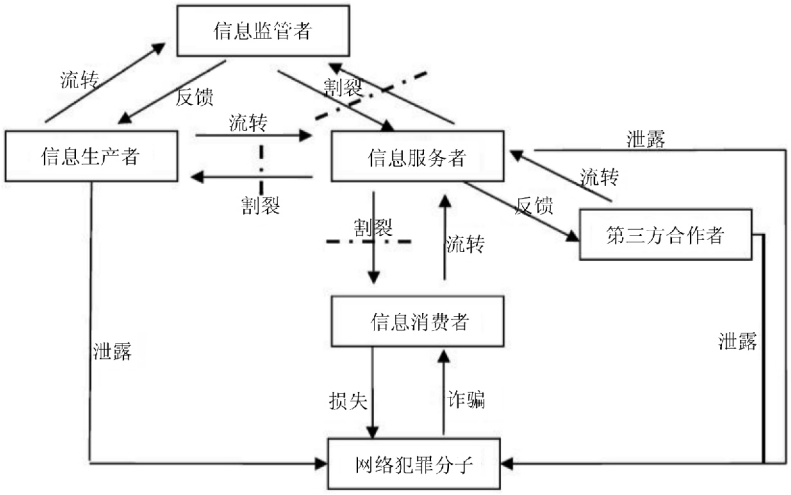

图 2　割裂的个人数据保护信息生态链

(2)信息监管生态位失位。信息生态位主要是信息人在信息生态环境中的位置[19]，由功能、资源和技术决定。前文已经提到，尽管在分析信息人时，将其分为四种类型，但随着大数据、云计算以及移动互联网的发展，信息人之间的界限也相对模糊，时代赋予信息人更高的使命，并提出了更高的要求，如信息服务者也应承担信息监管的职责，与信息用户也会成为信息生产者一样。因此原有信息生态位不可避免的会与时俱进的进行调整，在调整过程中会出现失位的情况，即生态位扩大、缩小，或与其他信息人生态位重叠等，如图 3 所示。信息生产者、服务者和第三方合作者凭借互利共生关系，本可实现优势资源互补的“共生放大效应”，但由于信息链的割裂以及彼此之间的竞争，导致为维持各自的竞争力，只希望将所掌握的用户信息资源价值最大化，而忽视了对用户数据应有的保护，生态位出现重叠或偏移。信息监管者因为

信息链的断裂,很多信息无法获取,执法和监管生态位被压缩。信息消费者的信息生态位由于信息服务和产品的互动性增强,会出现生态位扩大的情况,既是消费者,还是生产者;在数据保护方面,由于与信息服务者信息流转的不通畅,信息消费者接受信息时会有延迟和丢失,信息位还会缩小,难以保持稳定。

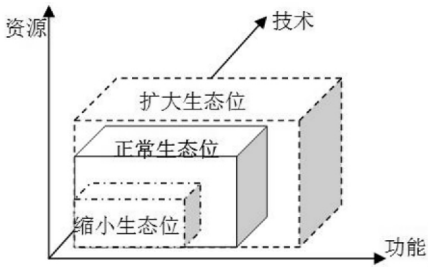

图3 信息生态位失位

(3)个人数据保护信息生态系统失衡。个人数据保护生态系统由信息人、信息环境以及错综复杂的信息链共同构成。要想保持平衡,则需要信息人与信息生态环境各要素之间相互协调、合理匹配、高度适应,建立共生关系、互动关系、合作关系甚至适度的竞争关系。对于个人数据保护生态系统,由于信息生态链的割裂和信息位的失位,造成信息人之间无法合理匹配、信息生态环境各因子无法相互协调、信息人与信息环境无法高度适应等问题,导致个人数据的泄露,如图4所示。

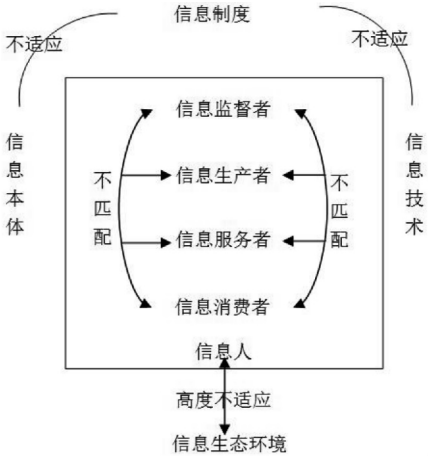

图4 信息生态失衡

4.2 引发个人数据保护生态系统问题的可能原因

在剖析个人数据保护生态系统结构要素的基础上,进一步分析目前存在的生态问题和可能的原因。通过对信息生态要素的梳理,并结合《报告》的内容来看,引发个人数据保护问题的原因主要有以下几个方面。

4.2.1 信息人方面的原因

(1)信息监管者。管理意识滞后。客观来说,管理意识需要在长期的管理活动中形成,而个人数据安全的保护是一项相对较新的工作职能,与以往网络内容管理和安全管理不完全相同。从实践来看,信息监督者存在着管理意识滞后的问题,无法提前通过政策制定来引导和规范相关行为,实施的管理措施相比个人信息安全实践也相对滞后。

人力资源欠缺。网络攻击和数据泄露事件是呈指数增长的发展态势,而在监管部门任职的人员增长规模不可能与待处理的事件成正比,且核心成员一般都是管理学的背景,较少有技术背景,这就造成有限的管理人员知识结构相对不均衡。

技术水平落后。个人数据保护管理的相关信息技术与网络攻击技术仿佛DNA的双螺旋结构,“你增我长”共同发展,但客观上,防护技术的发展要落后于攻击技术的发展。受制于信息监督者的知识结构,采取最新的管理技术很难实现。

(2)信息生产者和服务者。数据红利的过度追求。因信息环境的进化,信息服务者之间的信息生态位或面临相互重叠的窘境,必须要进行调整,提高自身的竞争能力。信息服务者之间的竞争除了自身定位和功能以外,更重要的就是用户资源的竞争,用户数据在某种程度上已经成为非常重要的资源。在此情境下,信息服务者会更多地考虑如何将用户数据资源价值最大化,其重要性要高于用户数据的保护。

网络安全投资较少。信息的生产和服务毕竟是市场行为,需要投入和回报呈正比关系。但是用于网络安全的投资回报不明显,或者显效较慢,需要较长的时间,因此信息生产者和服务者对网络安全的投资也不会是第一位的考虑方向。

主要负责人网络安全责任不明晰。对于信息生

产者和服务者来说,用户数据资源的安全需要明确的负责人来负责,负责人级别越高则影响越大,效用越明显,同时要明确数据安全泄露的责任,做到"主"与"责"相匹配。实践中这一点存在着问题,《报告》也对此提出了相关的建议。

对第三方合作者审计不严格。因业务拓展和共同发展的需要,信息生产者和服务者在信息生产和传递过程中不可避免的要与第三方合作者进行联合。在现实中,个人数据拥有者在共享数据资源的同时对第三方合作者的安全审计存在漏洞,也缺乏相应的安全标准。

(3)信息消费者。信息消费者最大的问题还是自我保护意识不足。客观来说,信息用户在信息活动中有自我保护的责任,特别是移动互联网环境下,手机等移动终端通过各类型信息服务者基本可以做生活中的任何事情,这样来个人的数据不可避免的存储在移动终端、信息服务者服务器、云端等机器当中,这其中不乏大量与经济利益相关的信息,如银行卡号和密码、移动支付账号密码等,还有自己社交的一些信息,这些如果泄露都会给自己和社交圈中的主体带来损失。

4.2.2 信息生态环境方面的原因

(1)信息载体易受侵犯。由于物理存储的限制,大多数信息服务者都将数据存在云端服务器。而云端服务器一般不会自己搭建,而是采取租用的方式。在多租户环境下,存储者无法直接控制数据,甚至无法知道数据存储的确切位置,也使得恶意盗窃行为或攻击更难以控制。也正由于云服务器存储大量用户数据,才会更加吸引网络黑客或者网络攻击者。当然,一般云服务提供商都会采取一定的保护措施,但是仍无法改变云服务器对犯罪分子的吸引力。

(2)网络攻击技术的不断翻新。随着云计算技术的使用,很多新型的攻击技术出现。如针对云计算的拒绝服务攻击和旁通道攻击等。以拒绝服务供给为例,当攻击者与正常的云用户被分配到同一个子网内时,如果攻击者发送大量数据包将该子网与外界相连的瓶颈链路堵塞,那么就会对正常用户造成网络服务的拒绝服务攻击[20]。一般来说,网络安全技术的发展总是落后于攻击技术的发展。

(3)信息时空的无限制。前文已述及,信息活动的时间和空间壁垒已被打破。传统的信息活动需要一定的场域,而目前基本可以实现随时随地从事任何信息活动。对于用户是如此,对于网络犯罪分子也同样如此。

(4)信息制度不健全。制度滞后于技术发展。前文已述及,个人数据保护的外部形势日新月异,而管理的制度、技术标准等方面要滞后于技术的发展,网民数量虽然规模越来越大,但良性、健康的网络秩序尚在形成之中。

相关法律量刑过轻。根据《报告》中的内容可以看出,当前发达国家的信息安全管理制度也有约束力不够的问题,一些法案中对数据泄露事件惩罚不严,量刑过轻。我国《刑法》、《居民身份证法》对泄露个人信息行为规定了相关法律责任,但并没有广泛适用于各行各业,对一些个人行为,也难以起到约束作用。可见这是全世界都面临的一个问题。

缺乏相应的配套制度。制度制定的滞后也造成了一些制度的空缺,如《报告》中提到的缺少用户的赔偿制度;拥有用户数据的企业或组织缺乏相应的数据保护最佳实践的指南,也没有定期向信息监管者汇报信息安全情况的机制;新信息系统开发过程中也很少有企业或组织将安全原则贯彻始终,此外对开发人员的安全培训也不到位等问题。

5 个人数据保护的策略选择

在以上分析的基础上,有必要参考发达国家的先进经验,对个人数据保护生态系统中存在的问题进行防范和治理。为保持信息链的通畅和信息位的适当,信息人之间需要密切配合,保障信息流转,融合共同的价值追求,与信息生态环境相适应,才能更好地保护个人数据。因此,应该建立一种宏观保护机制,引导实现信息人的共同价值诉求,以及采取微观保护策略,在实践中切实保护个人数据信息。

5.1 个人数据保护的宏观机制

个人数据的泄露最直接的原因是信息生产者和服务者在满足信息消费者信息需求的过程中,由于价值追求不同而出现的社会问题,因此要想从根本上保

护用户个人数据,信息人之间需要建立共同的价值追求。在满足用户需求和追求共同价值的驱动下,信息生态环境会发生进化,更好地适应和反向影响信息人的信息行为。信息人与信息生态环境相互作用,共同维护个人数据保护生态系统间各要素的平衡状态,如图5所示。

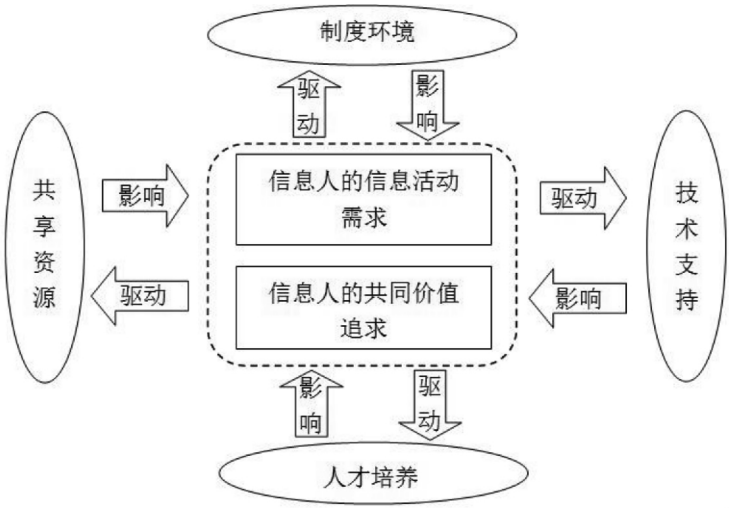

图5 基于信息生态理论的个人数据保护宏观机制

优化个人数据保护的制度环境。制度环境对个人数据保护的意识构建、行为规范的影响不言而喻。尽管各国都有相关的法律,但是很多法律法规都相对片面,如有的是规范电子商务领域的,有的是规范电子通信领域的,从个人数据生命周期(个人数据收集、记录、储存、传播、使用或销毁等)为基点考虑的很少。

提升信息保护技术的广泛应用。通过教育、培训等方式来提高不同层次的信息人对信息保护技术的掌握,拓展信息价值链,在追求数据红利的同时提高信息素养。通过补贴、评优等活动激励各信息生产者和服务者不断引入信息保护技术,在保护用户数据的同时还可以大幅提升抗网络攻击的水平。

加强用户信息资源的共享共责。在大数据时代,信息人希望独自依靠用户信息资源的开发获得发展壮大几无可能,信息人要想可持续发展,就要更加重视共同生存,组成利益共同体,相互促进,分工协作,互利互惠,共享用户数据。但与此同时,需要加强"共责"的意识,划定个人数据泄漏的"红线"。

培育多元数据保护人才。无论新技术的采用,还是新型信息服务的创新,以及对信息活动的监督和执法,都需要人来做保障。因此培育具备安全管理知识、安全技术能力、服务创新意识等的多元信息安全人才就显得十分重要。

5.2 个人数据保护的微观策略

个人数据保护的微观策略选择如图6所示。在信息本体方面,信息监管者应进行政策引导和法律规制,明确信息和载体的安全义务、责任,科学合理的引导信息及载体资源配置,在共同开发用户信息资源的同时,保障信息内容合法、合理的在一定范围内流转;信息生产者和信息服务者应秉持用户个人数据资源安全第一的理念,不仅仅将用户数据信息作为需要价值最大化的资源之一,更应该以用户为导向,以用户利益和价值最大化为发展方向,并注重网络攻击的防范,以及严格控制第三方合作者对数据资源的大量访问;信息消费者则应该提升自我保护的意识,在信息服务平台上减少与自身利益直接相关的信息生产,如银行卡、信用卡等信息,并对所要相关信息的不明来历电话、电子邮件等保持警惕,不轻易泄露。

在信息技术方面,信息监管者应顺应信息技术发展趋势,主动了解与信息安全有关的技术发展情况,

为制定相关政策夯实基础。此外，还应联合信息服务者共同推出个人数据保护的最佳实践，并为在数据保护方面有突出贡献或提供宝贵经验参考的信息服务者设立安全标签，作为信息服务者信誉的明确标识；信息生产者和信息服务者应加强信息安全技术的投入力度，紧跟网络攻击防御技术发展脚步；对系统开发人员和第三方合作者进行安全培训，提高内部员工的防范意识和技术手段，并在制定数据泄露应急规划的基础上，择机进行实战演练，把用户个人数据保护从口头转化为实际行动；信息消费者要对信息技术保持安全意识，不要轻易相信服务者所宣传的最新技术的普适性、功能性和安全性，对涉及自身数据信息的新技术保持谨慎，等技术逐渐发展成熟之后再逐步采纳，避免当信息技术使用的“小白鼠”。

	信息监管者	信息生产者 信息服务者	信息消费者
信息本体	政策引导 法律规制	安全理念 防范攻击 访问控制	提升意识 自我保护
信息技术	主动了解 最佳实践 安全标签	加强投资 人员培训 实战演练	安全意识 保持谨慎 逐步采纳
信息时空	公共宣传 加强监管	妥善配置 增加提醒	少用公网 保护账户
信息制度	合理布局 优先定序 加大处罚 赔偿政策	客戶联动 应急规划 明确条款 用户赔偿	学习体会 参与宣传 遵守制度

图 6　基于信息生态理论的个人数据保护策略

在信息时空方面，信息监管者要根据网络的具体情况（内网、外网、公网、私网、PC 端、移动端等），合理布局网络安全保护的相关资源，并把相关的政策、制度、案例、实践等向全社会宣传；信息生产者和信息服务者也要根据网络情况妥善部署自身的服务架构，并应用在容易发生数据泄露的公共网络空间或 Wifi 载体中，用户接入服务后要增加相应的风险提示信息，唤起用户自我保护的意识；信息消费者也要尽量减少与公共空间提供的免费网络链接，尽管这会方便用户的信息活动体验，但也会使数据泄露风险剧增。如果必须使用公网，则要注意不提供个人的账户（通讯工具账户、社交工具账户、个人财产账户等）信息。

在信息制度方面，信息监管者应根据技术发展状况，对存在问题较多的行业、领域、技术方向等问题合理布局政策，如类似发达国家一样针对个人数据保护制定《个人数据保护法》，针对其他领域的问题制定相应的法律；在面对海量需要处理的监管事件时，突出重点，明确优先级和处理次序，保证重要的事情优先处理；此外，还需要加大对个人数据泄露责任方的惩罚力度，包括提升罚款金额和增大量刑程度，并牵头各有关部门建立用户个人数据泄露的相应赔偿、补偿机制。信息生产者和信息服务者应该设置用户联动机制，保障在一定时间范围内与客户的沟通，告知用户获取信息的正确途径、方法，防范非法诈骗；还要制定应急处理方案，并在服务条款中增加造成数据泄露的风险和责任说明，且将主要负责人的薪酬与网络安

全挂钩,提高主要负责人的重视程度;在数据泄露事件发生后积极配合调查,在清晰划分责任的基础上,主动进行用户赔偿,最终形成行业自律。信息消费者则应对国家和消费过程中服务者的相应制度主动学习体会,并参与社会性的宣传活动,寓教于乐,增强意识和体验,并遵守相应的制度,避免个人信息的有意或无意泄露和可以避免的经济损失。

6 结语

个人数据安全是网络安全的重要组成部分,是网络生态治理的主要对象,是国家信息化发展的重要战略目标,也是亿万网民在网络世界从事信息活动的重要保障。本文从信息生态系统理论出发,以英国最新发布的《网络安全:个人在线数据保护》报告为例,分析了各主体在个人数据保护生态系统中的位置和作用,并针对存在的诸多问题提出有针对性的对策建议。不过,本文更偏向于《报告》的个案分析,并未涉及更多的现实案例,希望以后相关学者或研究人员可以对此进行更准确的实证分析。

注释

1 TalkTalk是一家为用户提供近距离交友、群组语音聊天、观看直播、组织游戏玩家、订阅游戏视频,以及享受电子竞技乐趣等的信息服务平台。它将注册用户的信息进行智能匹配,提供个性化智能服务,并与第三方服务者合作,开展支付、通信等服务。

参考文献

1 汪梦.数据红利下须加强个人数据保护[J].中国发展观察,2016(4):60-61
2,7 Bonnie A., Nardi. Information Ecologies. Reference & User Services Quarterly[M]. Chicago: Fall,1998(4):49-50
3 中共中央办公厅,国务院办公厅.国家信息化发展战略纲要[EB/OL].[2016-07-27].http://news.xinhuanet.com/fortune/2016-07/27/c_1119291902.htm
4,11,18 Cyber Security: Protection of Personal Data Online[EB/OL].[2016-06-25].http://www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/14802.htm
5 肖希明,唐义.信息生态理论与公共数字文化整合[J].图书馆建设,2014(3):1-4
6 L.A.David.An Ecology of Communication: Cultural Formats of Control[M] . Hawthorne:Aldine de Gruyter, 1995
8 Yogesh Malhotra.Information Ecology and Knowledge Management: Toward knowledge ecology for hyperturbulent organizational environments[EB/OL].[2016-07-20]. http://www.Yogeshmalhotra.com
9 娄策群,等.信息生态系统理论及其应用研究[M].北京:中国社会科学出版社,2014:37
10 T.H.Davenport, Laurence Prusak. Information Ecology:Mastering the information and knowledge environment[M]. New York:Oxford University Press,1997:22
12 北京大学互联网法律中心.国外网络法律文件选编[M].北京:学习出版社,2014:2-5
13 K S Baker, G C Bowker. Information Ecology: Open system environment for data, memories and knowing[J]. Journal of Intelligent Information System,2007(1):127-144
14 TalkTalk,The Ultimate Entertainment Platform[EB/OL].[2016-08-15].http://talktalk.sg/
15 Cyber Security Breaches Survey 2016[EB/OL].[2016-08-02].https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf
16 Written evidence submitted by UK[EB/OL].[2016-08-02].http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/cyber-security-protection-of-personal-data-online/written/24966.html
17 Written evidence submitted by Intel Security[EB/OL].[2016-08-02].http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/cyber-security-protection-of-personal-data-online/written/24950.html
19 娄策群.信息生态位理论探讨[J].图书情报知识,2006(5):23-27
20 俞能海,郝卓,徐甲甲,等.云安全研究进展综述[J].电子学报,2013(2):371-380

(收稿日期:2016-11-08)