冯占英,张　玉,段美珍,等. 大数据环境下个人信息泄露路径及其保护策略研究[J]. 中华医学图书情报杂志,2020,29(9):7-12.

DOI:10.3969/j.issn.1671-3982.2020.09.002

· 研究与探讨 ·

大数据环境下个人信息泄露路径及其保护策略研究

冯占英[1],张　玉[1],段美珍[1],陈　锐[2],王玉洁[1],吴方怡[1],姚　敏[1],王　璇[1],王宇光[1],左夏露[1],祝　茜[1]

[摘要]对个人信息泄露的途径和原因进行总结和归纳,并从政策制度、技术设施和相关个人等多个方面提出构建完善的个人信息安全保障体系。其中,政策制度方面应建立健全信息安全保障制度,技术设施方面要着力提升信息安全保障技术和能力,相关个人方面应全方位提升个人信息安全意识和保护能力。

[关键词]大数据;信息安全;信息泄露;信息保护

[中图分类号]G203;D922.16　　[文献标志码]A　　[文章编号]1671-3982(2020)09-0007-06

Divulging paths and protecting strategies of personal information in big data environment

FENG Zhan-ying[1], ZHANG Yu[1], DUAN Mei-zhen[1], CHEN Rui[2], WANG Yu-jie[1], WU Fang-yi[1], YAO Min[1], WANG Xuan[1], WANG Yu-guang[1], ZUO Xia-lu[1], ZHU Qian[1]

(1. Library of Academy of Military Sciences, Beijing 100039, China; 2. Information Research Center of Military Sciences, Beijing 100036, China)

[**Abstract**]After the divulging paths and causes of personal information were summarized, the idea was given for developing a well-equipped personal information security protection system in aspects of its political system, technical facilities, and relevant persons, namely the information security protection system should be established and amplified in view of its political system, the information security protection techniques and competence should be strengthened in view of its technical facilities, and the personal information security awareness and protective ability should be improved in view of its relevant persons.

[**Key words**]Big data; Information security; Information divulgement; Information protection

大数据的迅猛发展和广泛运用引领了全球范围内的科技革新,推动了整个社会的进步。以信息技术为基础,信息及信息化的发展已经渗透到人类生活和生产的方方面面,成为当前推动社会进步的关键要素,也逐渐成为世界各国和各机构之间博弈和竞争的核心。然而,在大数据技术和信息化发展的同时,因数据挖掘和利用等导致个人信息泄露的途径和范围进一步扩展,从而引发一系列个人信息安全问题,进而更广泛地危害组织和国家信息安全的现象已屡见不鲜。为最大限度地减少信息泄露及其带来的危害,必须充分了解大数据技术环境下隐藏的信息安全隐患,明确个人信息泄露的各种途径,做到防患于未然。

1　研究背景

“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题”[1],个人信息尤其是那些关系机构和国家安全的关键性个人信息的安全问题已经得到了国家各级政府和各行业的重视。如在国家层面,备受关注的《中华人民共和国个人信息保护法(草案)》已完成,

[基金项目]国家社会科学基金项目(16GJ003-158)

[作者单位]1. 军事科学院图书馆,北京　100039;2. 军事科学信息研究中心,北京　100036

[作者简介]冯占英(1973-),女,山西繁峙人,博士,研究馆员,研究方向为图书馆学、计算机,主持、参加课题 20 余项,发表论文 20 余篇。

并将提请全国人大常委会会议审议[2]，这标志着我国第一部专门针对个人信息安全的法案即将正式出台；在各行业机构层面，现行的《关于加强网络信息保护的决定》[3]《电信和互联网用户个人信息保护规定》[4]和《关于进一步加强军队信息安全工作的意见》[5]等相关文件也对个人信息安全问题进行了规定。这些政策文件的出台在一定程度上有利于防范个人信息泄露现象，并为个人信息保护实践提供指导。但从现实情况来看，由于相关政策体系和内容不完善、针对性和可行性不强以及多方利益相关者对制度的执行不到位等原因，我国个人信息安全还存在很多问题，信息泄露问题仍然频繁发生。

本文以“SU=个人信息泄露+个人隐私泄露”为检索式在 CNKI 数据库中进行检索，检索时间范围截至 2020 年 8 月 1 日，共获得 618 条记录，包括学位论文 30 篇、学术期刊论文 344 篇，涉及计算机网络、行政法律、经济、新闻传媒、教育与图书情报等多个领域。期刊文献中仅有 54 篇来自中文社会科学引文索引（Chinese Social Sciences Citation Index, CSSCI）、《中文核心期刊目录总览》（即“北大核心”）及中国科学引文数据库（Chinese Science Citation Database, CSCD）。由此可见，个人信息泄露问题已经得到了各领域的广泛关注，但核心文献数量分布较少，研究成熟度还不够。从研究方法和主题内容来看，现有研究主要通过逻辑归纳和演绎的方法开展，研究内容主要涉及个人信息泄露危害及其保护的重要性、个人信息及隐私保护的法律问题[6]、个人信息及隐私泄露的原因及其保护策略等方面[7]。总体来看，相关研究对现有案例的挖掘还不够，研究方法的科学性和规范性还有待提升，所提对策建议的系统性、普遍性和针对性还有待加强。

因此，本文立足于当前的信息技术环境，以个人信息泄露为核心研究内容，通过案例分析法和文献归纳法，对个人信息泄露途径进行分析，并从事物发展的自然规律和构成要素的角度出发，从政策制度、技术设施和相关个人方面提出保障个人信息安全的可行性建议和策略，具有一定的创新性和实践指导价值。

2 大数据时代个人信息泄露的途径与原因

大数据时代，伴随着人工智能、云计算和物联网等技术的不断发展，智慧社会、智慧城市和智慧社区等一系列智慧化工程逐步实施，人们日常的生活和生产方式也由此产生了翻天覆地的变化，几乎大部分的个人信息及社会活动行为都会被互联网记录下来，形成具有特色的个人或组织的“档案”[8]。这些数据的存储与利用为提升社会生产和生活的效率与效能创造了良好的条件。但由于网络信息安全监管力度不够、信息安全保护意识和能力不足等多种原因，个人信息数据泄露问题也日渐凸显，信息泄露事件的数量不断攀升，给公民的个人生命财产安全乃至机构组织和国家的安全等带来了极大的威胁。因此，明确个人信息的内容类型，分析其泄露的途径和原因，对今后个人信息的保护至关重要。

2.1 个人信息的内容类型

明确个人信息的内容类型及其边界是防止其泄露的前提和基础。个人信息是指与个人相关的、能够直接或间接识别的个人数据，所包含的内容十分广泛，不仅包括个人姓名、身份证号码、肖像、DNA 和指纹等直接识别身份的信息，也包括家庭信息、社会生活信息、教育信息、工作信息、健康信息、财务信息、行政司法信息、表达性信息等可间接识别身份的其他信息[9]。

从信息的产生过程和稳定程度来说，个人信息可分为身份证号码和 DNA 等固定的静态信息，以及社交行为信息和财务信息等会随着时间的推移不断变化的动态信息；从信息的内容属性来说，个人信息可分为属人的个人信息和属事的个人信息[10]。事实上，随着信息技术的不断渗透和公众在信息社会中参与度的不断提升，信息的属性边界变得越来越模糊，绝大多数反映主体自然属性和自然关系的信息的社会属性也在不断增强[11]。

2.2 个人信息泄露的典型案例

通过国内外个人信息典型案例（表 1）可以发现，个人信息泄露事件并不是某一个国家和地区的个案问题，而是困惑全球各国和各领域的普遍性问题。尤其是在大数据环境下，互联网普及程度较高、网络安全保障意识和能力较弱的主体，其信息泄露的风险越大。个人信息泄露现象不仅发生在普通公民中，还波及军人等对国家和社会经济安全有重大影响的特殊人群。通常情况下，普通公民个人信息

的泄露仅对自身产生不良的影响,轻则干扰生活,重则危害生命;而军人等特殊群体是国家秘密的关键组成部分,一旦其个人信息泄露,就会给个人和组织带来不可估量的损失。

表 1　个人信息泄露典型案例

案例	时间	国别	事　件	泄露方式
案例 1	2018 年	美国	美国国防部国防旅行系统因敏感邮件分发至错误的电子邮件,导致 21426 名海军陆战队队员、舰队水手以及雇员的高度敏感信息泄露,邮件附件列出了包括截短的社会安全号码、信用卡信息、银行路线号码、电子资金转账详情、住宅位置、邮寄地址及紧急联系信息等个人敏感数据	被动泄露
案例 2	2018 年	中国	支付宝年度账单泄露信息事件	被动泄露
案例 3	2018 年	中国	滴滴、美团外卖等多家互联网平台被曝利用用户大数据“杀熟”	被动泄露
案例 4	2016 年	中国	顺丰荆州某网点仓管汪某售卖客户信息,涉及的群体包含快递代理商、文化公司、无业游民、诈骗犯罪分子等,形成了多方参与的产业链条	被动泄露
案例 5	2016 年	俄罗斯	“彼得大帝”号核动力巡洋舰上服役的一名俄罗斯水兵在社交网络上上传了数张在甲板上自拍的照片,美国根据社交网络显示的地理位置获取到俄罗斯舰队的航行位置,“彼得大帝”号核动力巡洋舰是和俄罗斯唯一的航母“库茨涅佐夫”号一起行动的,该举导致航母的位置信息被直接泄露	主动泄露
案例 6	2016 年	美国	美国海军发布公开声明称其拥有的一台笔记本电脑遭到了黑客的入侵,超过 13 万现役及已退休海军士兵的个人信息因此遭到外泄	被动泄露
案例 7	2016 年	美国	成人网站 xHamster 用户数据遭公开售卖,账号涉及英美政府官员	被动泄露
案例 8	2016 年	–	“口袋妖怪”(Pokemon Go)游戏基于谷歌地图开发,游戏会持续更新用户所在位置,被指或可能侵犯用户隐私,泄露机密信息,游戏在多国被下架	主动泄露
案例 9	2016 年	美国	美国最大的有线电视公司“时代华纳”公开表示,公司旗下近 32 万用户的邮件和密码信息已被网络黑客窃取	被动泄露
案例 10	2016 年	中国	徐玉玉案件:不法分子倒卖高考考生信息,并通过诈骗电话从考生处骗取钱财,导致受害人遭受经济损失并因此失去了生命	被动泄露
案例 11	2007 年	美国	当一架载有一队士兵的直升机飞往达伊拉克某基地时,一些士兵在飞行路线上拍照,并将相关照片上传到互联网上。伊拉克叛乱分子利用图片中可识别的地标,确定了直升机的确切位置并进行迫击炮攻击,摧毁了 4 架 AH-64 直升机	主动泄露

结合当前人们日常的行为习惯等情况,从被泄露信息的个人角度对表 1 中的泄露案例进行分析,发现个人身份信息、运动轨迹和地理位置信息、财务和消费信息、网页浏览行为等社交行为信息是个人信息泄露的主要内容类型。其中,身份信息是识别特定个人最直接的信息类型,该类信息与其他个人信息直接相关。通过对身份信息的识别,可以迅速锁定并挖掘到其他所有的个人信息。因此,身份信息尤其是关键性身份信息的泄露,会让个人信息暴露在互联网中,一览无余。利用用户画像技术,通过网络浏览行为等社交行为信息、财务和消费信息及位置信息等基本属于动态的个人行为信息,可全面掌握和了解用户情况。这些信息一旦被非法获取和利用,会对用户个人及其家庭等造成不良影响。

从信息泄露主体的主客观态度来看,案例中信息泄露的方式主要有被动信息泄露和个人主动信息泄露两种。

被动信息泄露主要包括非法监控、信息系统和平台的技术漏洞、黑客攻击及信息窃取等多种类型(如案例 6)。通常情况下,大部分的个人信息泄露都属于被动泄露,即个人信息被他人或机构泄露。

个人主动信息泄露包括主动无意识泄露和主动故意泄露两种。主动无意识泄露指的是个人主动进行了信息发布,但在发布信息时可能并不明确所发布信息属于涉密信息且认为不会泄密,个人主动信息泄露多数情况下是无意识的(如案例 11);主动故意泄露指的是个人明确所发布信息属于涉密信息或发布此类信息会产生泄密风险,但为了牟利等原因

依旧发布相关信息的行为(如案例 4)。

2.3 个人信息的泄露途径

基于以上案例分析,结合当前的时代环境和人们的日常行为特征,本文认为大数据环境下个人信息的泄露途径主要有以下几种。

一是个人信息被网络服务平台自动采集。大数据在服务业、电子商务业及金融信息业等领域的应用可以帮助商家分析消费者需求,便于其提供更精准的广告推介,开展商业服务。但部分服务平台的运营者或管理者会通过倒卖个人信息进行牟利,造成个人信息的泄露。

二是个人信息被第三方实体进行网络非法抓取。大数据时代,人们经常在各种社交媒体上发布自己的动态和信息,并且很多人并未意识到信息泄露风险,在发布或分享信息的同时会不经意暴露自身敏感信息,这使个人信息泄露变得更加容易。第三方实体通过大范围网络抓取并配合数据挖掘技术,便可以较容易地掌握用户个人信息,构建用户画像,并针对目标用户进行进一步的信息挖掘。

三是个人信息被移动位置应用程序采集和泄露。目前,各类在线社交网络软件在人们的生活中占据了不可或缺的位置。人们通过社交网络活动产生的绝大部分数据与位置信息相关,随着定位技术的高速发展,专注位置服务的各类地图 App、具备定位功能的应用软件日渐成为手机客户端必不可少的组件。这些应用软件通过获取终端用户的位置信息,将虚拟网络与现实物理世界连接起来,依靠地理信息系统的支持,为用户提供相对应的增值服务。此外,无论微博、微信、QQ 等网络社交应用,还是涉及人们衣食住行的其他相关应用,均可用 GPS 随时随地分享用户的当前位置并搜寻路线,还可搜索到周边位置的朋友。然而,用户开启位置定位服务,并与不同的朋友和服务供应商“共享”位置,就会导致自己的日常行踪外泄。信息技术在方便个人生活的同时也隐藏着泄露个人信息的风险[12]。

四是个人信息因信息系统本身的漏洞和恶意攻击等原因被泄露。随着物联网、大数据和人工智能等技术的不断发展和应用,互联网和智能设备等已是人们日常生活中必不可少的工具。这些技术设备在网络安全、数据安全、密码安全、应用安全、终端安全、位置安全和云存储安全等方面的不足和缺陷会增加个人信息泄露的风险[13]。

除以上信息泄露途径外,电子设备报废和网络媒体过度报道等引发的信息泄露事件也时有发生。随着信息技术和设备的升级发展,以及用户行为模式的变化,个人信息被收集和泄露的方式还会不断更新变化。虽然相应的安全措施也会不断出现,但新的破解方法也会随之而来。因此个人信息一直都会处于被恶意收集的风险中,只有提高自身的防范意识,才能尽量避免重要的信息被他人恶意获取,才能保证个人信息的安全。

2.4 个人信息泄露的原因

通过对个人信息泄露案例的分析,结合已有研究结果,发现信息泄露的原因主要包括以下几点。

一是我国在个人信息保护的立法及监管层面上存在不足,缺乏系统性和针对性且可行性较强的政策,对于个人信息保护方面的立法和执法经验还不够丰富,对突破红线、知法犯法的恶劣行为惩罚力度不够,从而导致信息泄露事件不断发生。

二是相关系统平台和网站的防范能力有限,常因技术问题和漏洞等引发信息泄露风险。除程序系统设计不规范、规划不合理问题外,也可能存在代码注入漏洞、弱密码漏洞、路径遍历漏洞、缓冲区溢出漏洞、跨站脚本攻击(XSS)漏洞和拒绝服务攻击(DOS)漏洞等。这些漏洞本身并没有太大威胁,只会影响软件的使用和用户的体验,然而一旦被网络黑客发现和利用,就可能带来极大的安全威胁。

三是我国社会各界尤其是普通民众对个人信息安全问题的重视程度不足。21 世纪以来,大数据等信息技术得以广泛应用并惠及每一个参与互联网的普通民众。在享受信息技术带来的极大便利的同时,民众对互联网也形成了较强的依赖性,再加上个人信息的隐私保护意识和维权意识薄弱、个人信息和隐私保护能力不足等原因,导致个人信息安全问题日渐增多。

综上所述,随着新技术、新应用和新模式的出现,用户信息泄露的方式及内容愈加繁多,想从海量的数据中监测到被利用的漏洞也变得困难重重。因此解决因多方面原因导致的信息泄露问题,将是未来个人信息安全领域的重要研究方向。

3　个人信息安全保障对策

通过对大数据环境下我国个人信息泄露途径和原因的分析,本文认为今后可从政策法律、技术设施和相关个人等多个角度出发,按照从宏观部署和指导到微观执行和落实的思路,构建完善的个人信息安全保障体系。

3.1　政策制度方面:建立健全信息安全保障制度

政策制度是促进实践发展的关键指导和重要推动力,因此必须坚持制度先行。个人信息安全和保护问题需从政策制度方面加以重视,坚持从上至下的顶层设计与底层设计相结合的思路,按照事前预防、事中控制和事后问责的发展流程[14]建立体系化的法律法规和政策制度,明确个人信息的法律界定,加强个人信息保护力度,切实维护个人的合法权益和组织利益。

事前预防就是要求提前制定科学完善的个人信息和隐私保护政策和制度、信息监管制度和惩戒制度及防泄密安全机制等。目前国内从政府到机构和组织对个人信息和隐私保护问题的关注度不断上升,备受关注的《中华人民共和国个人信息保护法》也即将出台。

事中控制就是要求相关机构和部门在具体实践的过程中,根据实际情况从个人信息控制者、处理者与其他个人信息行为主体等不同的利益相关者的角度出发,明确各类型活动中可能会涉及的信息安全问题,制定规范的网络管理和使用制度,明确相关人员的权利义务和其他要求。

事后问责就是要求建立强有力的问责机制和惩戒机制,通过行政和法律处罚督促相关人员进行不断的反思和改进。

3.2　技术设施方面:提升信息安全保障技术和能力

大数据时代的个人信息泄露始于信息技术的应用,也应终结于信息安全技术的应用。构建并维护强有力的网络安全体系,能从根本上解决因互联网技术问题带来的个人信息泄露风险。从国家和社会发展的大环境来说,国家和政府应关注信息安全问题及其对国家和社会发展的影响,鼓励信息安全领域的创新研究,把国家信息安全能力的提升和相关技术设施的开发及信息安全人才的培养作为重点关注领域并加以支持。从行业和组织机构层面来说,一方面要注重网络安全系统等软硬件设施的自主研发,另一方面要强化防泄密的安全保护技术的应用,加强对个人数据及其他关键数据的技术监控和自动处理。对因技术问题引发的泄密问题应通过自主研发和外部引进等相结合的方式提升信息安全保障技术,减少个人信息泄露的风险,尽早发现信息的变化状态,及时预警,尽量使损失最小化。

3.3　相关个人方面:全方位提升个人信息安全意识和保护能力

信息的产生、管理和利用等与每个参与人类信息交流和信息管理生命周期的个体密切相关,信息安全意识和保护能力的提升是防止个人信息和隐私泄露的关键。因此,无论是个人信息的所属者、管理者还是使用者,都需要顺应大数据时代的特点与要求,改变传统的安全观念与认知,了解个人信息安全相关法律法规,提升信息安全意识与素养,掌握信息安全保护知识,不断培养防护技能。具体来说,一是要积极参加网络安全、信息管理、隐私保护的普及课程,了解互联网的运作模式和信息泄露途径,了解网络使用过程中可能会面临的威胁及处理手段[15];二是要注意培养良好的上网习惯,慎重对待智能产品和免费 Wi-Fi 等,定期对关键数据进行更新和处理,以减少个人信息泄露[16];三是要了解和掌握一些简单的信息安全保护技能,持续学习和了解新的技术环境和手段,以便在个人信息安全面临威胁时能够通过自我救助和外部救援等途径解决问题。

4　结语

随着时代的进步和信息技术的升级,人们生产、管理和利用信息等的方式和手段会更加多元化,信息泄露防不胜防,个人信息和隐私保护的难度也会越来越大,因此个人信息安全保护将是未来很长一段时间内需要持续关注的重点课题。个人信息安全保障体系的构建不能一蹴而就,需要多方利益相关者的广泛关注和参与。只有这样,才能有利于社会的长治久安,才能促进社会和谐发展。

【参考文献】

[1]　习近平谈网络安全:没有网络安全就没有国家安全[EB/OL]. (2018-08-17)[2020-08-13]. http://cpc.people.com.cn/xuexi/n1/2018/0817/c385476-30234135.html.

[2]　全国人大常委会法工委:个人信息保护法正在研究起草中

[EB/OL]. (2020-05-14)[2020-08-13]. https://www.chinacourt.org/article/detail/2020/05/id/5220984.shtml.

[3] 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[EB/OL]. [2020-08-13]. http://www.npc.gov.cn/wxzl/gongbao/2013-04/16/content_1811077.htm.

[4] 电信和互联网用户个人信息保护规定[EB/OL]. (2012-07-29)[2020-08-13]. http://www.cac.gov.cn/2012-07/29/c_133142088.htm.

[5] 经习近平主席批准 中央军委印发《关于进一步加强军队信息安全工作的意见》[EB/OL]. (2014-10-07)[2020-08-13]. http://www.81.cn/sydbt/2014-10/07/content_6167089.htm.

[6] 刘 璐,潘鸿圆. 大数据时代个人信息法律保护的思考[J]. 新闻传播,2020(13):18-19.

[7] 鲁佑文,马亚鑫. 信息源与风险源:大数据时代个人信息安全困境及应对[J]. 现代传播:中国传媒大学学报,2019,41(11):81-85.

[8] 杜小红. 大数据背景下的个人信息保护[J]. 法制与社会,2020(12):14-15.

[9] 侯永刚. 黑客攻防[M]. 北京:人民邮电出版社,2016.

[10] 张才琴,齐爱民,李 仪. 大数据时代个人信息开发利用法律制度研究[M]. 北京:法律出版社,2015.

[11] 郭明龙. 论个人信息之商品化[J]. 法学论坛,2012,27(6):108-114.

[12] 赵 璐. 我国移动社交网络中的用户个人信息保护研究[D]. 太原:山西大学,2019.

[13] 徐 澄. 面向企业信息安全的网络攻击防范手段研究[J]. 中国电子科学研究院学报,2020,15(5):483-487.

[14] 郭 军. 大数据环境下图书馆用户个人信息保护研究[J]. 图书馆工作与研究,2020(1):11-19,28.

[15] 王 丰. 论对个人信息安全素养的培养[J]. 电子世界,2020(2):93-94.

[16] 徐小亭. 对大数据时代军人个人信息安全的思考[J]. 国防,2018(7):65-67.

[收稿日期:2020-08-15]

[本文编辑:黄思敏]