



21世纪高等教育财经津梁丛书

个人信息安全

孙毅 郎庆斌 杨莉\著



FE 东北财经大学出版社
Dongbei University of Finance & Economics Press

D913.04
S973

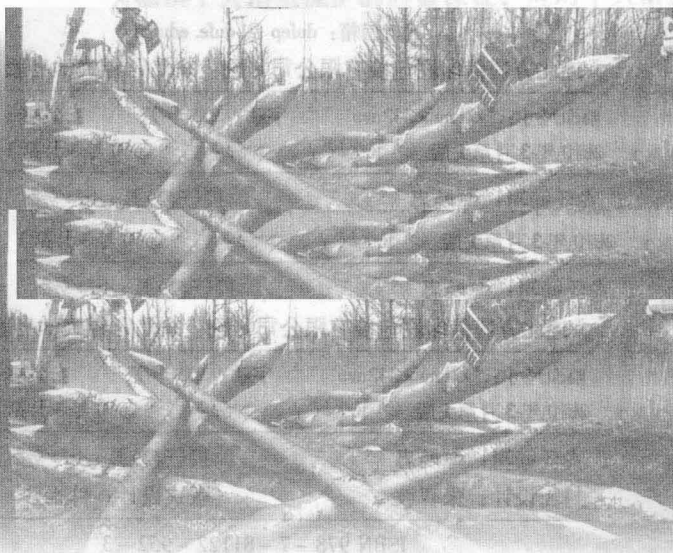


策划

21世纪高等教育财经津梁丛书

个人信息安全

孙毅 郎庆斌 杨莉\著



FE 东北财经大学出版社
Dongbei University of Finance & Economics Press
大连

© 孙毅 郎庆斌 杨莉 2010

图书在版编目 (CIP) 数据

个人信息安全 / 孙毅, 郎庆斌, 杨莉著. —大连: 东北财经大学出版社, 2010. 3

(21 世纪高等教育财经津梁丛书)

ISBN 978 - 7 - 81122 - 952 - 3

I. 个… II. ①孙…②郎…③杨… III. 隐私 - 人身权 - 高等学校 - 教材 IV. D913.04

中国版本图书馆 CIP 数据核字 (2010) 第 037620 号

东北财经大学出版社出版

(大连青黑石礁尖山街 217 号 邮政编码 116025)

教学支持: (0411) 84710309

营 销 部: (0411) 84710711

总 编 室: (0411) 84710523

网 址: <http://www.dufep.cn>

读者信箱: dufep@dufe.edu.cn

大连北方博信印刷包装有限公司印刷 东北财经大学出版社发行

幅面尺寸: 172mm × 242mm

字数: 300 千字

印张: 13 1/2

2010 年 3 月第 1 版

2010 年 3 月第 1 次印刷

责任编辑: 谭焕忠

责任校对: 王 娟 那 欣

封面设计: 张智波

版式设计: 钟福建

ISBN 978 - 7 - 81122 - 952 - 3

定价: 22.00 元

序一

随着信息技术的发展,个人信息的收集、处理愈加方便、容易,大量涉及个人隐私的信息,可以轻易地随时通过网络获取。对个人信息的侵害愈加频繁,愈加呈现多样性,从而引发新的个人隐私的安全危机。

由于几千年传统文化的影响,公民在经济、社会活动中普遍缺乏个人信息安全意识,在全球经济一体化、社会生活信息化的今天,缺少个人信息安全专门法规、行业间自律规范的约束,个人信息不合理地公开甚至滥用成为常态。

为了规范个人信息收集、处理、使用行为,保证个人信息的有序、合理、合法流动,大连市率先发布了《大连市软件及信息服务业个人信息保护规范》,并开始实施个人信息保护认证工作,并在此基础上,发布了辽宁省地方标准《辽宁省软件及信息服务业个人信息保护规范》。2008年6月19日大连软交会期间,辽宁省正式发布了全社会各行业可遵循的地方标准《辽宁省个人信息保护规范》。

在个人信息安全相关标准编制、地方法规研究和个人信息保护认证实践中,涉及个人信息的定义、个人信息的特征、个人信息主体的权益、个人信息保护的原则、个人信息管理、个人信息安全,以及个人信息保护认证机制、个人信息保护认证质量等诸多问题。经过多年未曾间断的持续阅读、研究、分析、吸收、思考,形成个人信息安全规范的精炼的条文、认证机制及质量保证体系,并完成了全国首部基于丰富实践经验,系统、理论地阐述个人信息安全机理的专著——《个人信息保护概论》^①。

为了更好地认识、理解个人信息安全,推进个人信息保护工作的普及、深入,在《个人信息保护概论》的基础上,我们重新梳理了个人信息安全体系构建、实施、运行和个人信息安全认证机制的基本概念、流程、过程、基本理论和实践、质量控制等诸多问题,基于最新的研究成果和实践经验,修正了《个人信息保护概论》中不明确、不清晰,甚至错误的观点,保证在个人信息安全实践中正确、清晰地理解和学习。如在实践中,能获得个人信息安全理论和实践的初步认识并在以后的工作中付诸实施,则本书的初衷得以实现。

本书共分10章,由东北财经大学孙毅组织撰写,大连交通大学郎庆斌设计全书架构并总纂、定稿。第1、3、10章由孙毅撰写;第2、4、5、6、9章由郎庆斌撰写;第7、8章由杨莉撰写;附录部分由孙毅编写。

大连软件行业协会的孙鹏、王开红、郭玉梅、曹剑、常伟、尹宏等,为本书的撰写,收集、提供了大量资料,提出了许多有益的思路,在此向他们表示深深的谢意!

^① 郎庆斌、孙毅、杨莉:《个人信息保护概论》,北京,人民出版社,2008。

本书在编写过程中，得到大连市经济和信息化委员会、大连软件行业协会、大连个人信息保护工作委员会和工作委员会教育培训组的大力支持，在此一并表示感谢！

本书得以顺利出版，特别感谢大连市西岗区信息产业局及王义杰局长，对他们付出的努力，表示深深的谢意。

由于个人信息安全是我国新兴的研究领域，因此，本书中许多观点还值得商榷，也难免存在许多不足之处，欢迎同仁共同探讨，并加以斧正。

东北财经大学 孙毅
2009 年 12 月

序二

个人信息安全，正在形成信息安全领域一个新的分支，成为全球瞩目的焦点。它深刻影响着人们在经济、社会、生活中的活动，已经成为不容忽视的安全因素。

遍观世界，个人信息安全事件频出，2008年，英国涉及2 500万人、725万个家庭的资料泄露，2009年英国1.9万张信用卡信息泄露，日本陆上自卫队14万人及家属信息泄露，美国生命保险日本分公司个人信息泄露，日本住友生命保险横滨子公司1 600名员工信息泄露……不一而足。中国的个人信息泄露，更是泛滥成灾。环顾宇内，随着科技发展、社会进步，更凸显个人信息的商业价值和经济利益，特别是虚拟空间的迅速膨胀，使个人信息炙手可热，作为社会个体的个人几无隐私可言。

欧盟及其各成员国，建立了严格的个人信息安全相关的法律体系。然而，层出不穷的个人信息安全事件严重考验着法律体系的遵从度。英国于2009年6月2日发布了第一个个人信息保护规范——*Data Protection – Specification for Personal Information Management System*，以提高和维持1998年英国数据保护法的遵从度。可见，仅仅依靠法律的严谨是不能保证个人信息的相对安全，需要辅之行业自律相应标准。

在个人信息安全实践中，如何保障个人信息安全和个人信息主体权益，没有统一的模式、成熟的理论和同一的经验。个人信息安全是新兴的研究领域，概念、模式、过程、服务、质量、标准与法律的协调等，有大量课题需要认真、深入研究。在个人信息安全研究中，注重将已形成的观点诉诸文字，以供实践检验、同行交流、教授学子，推进个人信息安全意识的普及进程，是本书的宗旨。

个人信息保护体系（个人信息管理体系更趋严谨和科学）是保证个人信息管理活动科学、规范、有效、充分，约束个人信息管理者行为的管理系统。本书从个人信息保护体系入手，剖析了体系机制、构成、过程和质量保证等，以及体系评价机理、过程、质量。基于个人信息保护体系总体架构，分别阐述了管理机制、保护机制、安全机制、过程改进机制及保证体系充分、有效、适宜的评价机制，也阐述了基于实践形成的若干基本概念。

本书通过一个虚拟的企业环境，描述了构建、实施、运行个人信息保护体系的全过程，是实际使用本书的总结，有一定的现实指导意义。

本书的撰写，是个人信息安全研究、实践近10年的结晶，是大连软件行业协会个人信息保护工作委员会、个人信息保护评价办公室集体智慧的成果，凝结了大连市从事个人信息安全事业全体成员的心血和劳动。本书作者谨致诚挚的谢忱。

大连交通大学 郎庆斌
2009年12月

目 录

第1章 绪论	1
1.1 网络应用中的个人信息侵害	1
1.2 博客与隐私	3
1.3 现实生活中的个人信息侵害	4
1.4 个人信息安全的影响	5
1.5 个人信息安全范畴	7
第2章 基本概念	9
2.1 信息	9
2.2 个人信息相关概念	12
2.3 个人信息拥有者	27
2.4 个人信息处理	29
2.5 个人信息数据库	31
2.6 个人信息保护体系	32
2.7 个人信息安全	33
第3章 个人信息管理机制	35
3.1 管理概述	35
3.2 个人信息保护体系	37
3.3 个人信息保护管理机制	39
3.4 个人信息数据库管理	45
3.5 个人信息管理的目标和原则	46
第4章 个人信息保护机制	49
4.1 个人信息管理	49
4.2 个人信息保护原则	50
4.3 个人信息收集	52
4.4 个人信息处理	58
4.5 个人信息利用	60
4.6 个人信息的后处理	63
第5章 个人信息安全管理机制	64
5.1 信息资源	64
5.2 信息安全简述	65
5.3 信息安全防护体系	66
5.4 个人信息安全	68
5.5 信息安全与个人信息安全	74

5.6 社会工程学管理	75
第6章 过程改进机制	80
6.1 PDCA 模式	80
6.2 个人信息保护体系的 PDCA 模式	81
6.3 监察	82
6.4 内审	83
6.5 过程改进	84
第7章 外包服务业个人信息安全	87
7.1 服务外包的基本概念	87
7.2 服务外包机理	90
7.3 政府对服务外包产业的支持	96
7.4 服务外包中的个人信息安全	97
第8章 个人信息安全保护模式	103
8.1 美国保护模式	103
8.2 欧盟保护模式	106
8.3 日本保护模式	108
8.4 德国保护模式	110
8.5 我国的个人信息保护模式	111
第9章 个人信息安全认证体系	115
9.1 评价体系的发端	115
9.2 评价的基本概念	116
9.3 评价体系管理	118
9.4 评价流程	120
第10章 个人信息安全实践	135
10.1 企业模型	135
10.2 个人信息安全需求	136
10.3 个人信息管理机制	137
10.4 风险管理与保护机制	139
10.5 安全管理机制	147
10.6 过程改进机制	149
10.7 申请个人信息安全认证	151
附录1 手机“偷窥”隐私	152
附录2 部分管理规章示例	155
附录3 辽宁省地方标准	191

第1章 绪 论

个人信息伴随着社会发展和市场经济的建立,凸显人格利益的商业价值和经济利益。人格要素的商品化、利益多元化,更凸显了在现代社会经济活动中,个人信息的无形的物质性财产权益。

随着网络技术的发展,改变了传统的生活形态,社会生活更加便利和快捷。同时,通过网络收集、处理和利用个人信息也更容易。号称全球最大的中文搜人引擎 Ucloo,只要输入姓名,就可检索到非常详尽的个人信息。在信息技术飞速发展的今天,几无个人隐私可言。

个人信息无形的商业价值,特别是网络空间信息资源共享的特性,使个人信息被不合理使用、收集、篡改、删除、复制、盗用、散布的可能性大大增加,个人信息主体的个人信息控制权面临失控的危险。

1.1 网络应用中的个人信息侵害

计算机技术,特别是网络技术的飞速发展,在带来便利和快捷的同时,也更易于个人信息的收集和利用,因而产生了个人信息滥用、泄漏、公开和传播的隐患,如 Cookie 的利用。

基于网络的个人信息收集和利用主要包括:

1. 当用户获得网上服务,包括网上购物、获取信息、电子邮箱、个人主页、网上浏览等时,网络服务商通常会要求用户提供部分个人信息,如姓名、性别、年龄、家庭住址、工作单位、住宅电话或手机号码、身份证号码,以至婚姻状况等,甚至要求提供更加详细的个人信息,内容可以广泛到无所不包;
2. 用户在电子商务活动中形成的个人财产和信用信息,包括登录账号和密码、信用卡、电子消费卡、网上交易的相关信息、个人收入状况等;
3. 游戏玩家在网络游戏过程中形成的个人信用信息,包括网络游戏账号和密码、QQ 号和密码、游戏虚拟物等;
4. 用户的网上行为,包括访问网站时使用的 IP 地址、网上活动轨迹、活动内容、兴趣爱好等;
5. 个人的电子邮箱和电子邮箱地址等。

网络服务商可以基于网络在短时间内收集到大量的、多种类型的个人信息,基于商业目的进行整合,并建立相应的数据库。网络服务商利用个人信息数据库,可以直接面向用户进行有针对性的广告宣传和销售服务,以降低传统销售方式的成本,提高经营效率。

个人信息为个人信息主体唯一拥有,利用个人信息,必须经过信息主体授权。

但是,基于网络的个人信息利用和收集,存在侵犯个人信息主体隐私权的威胁。这种侵权行为常常表现为:

1. 个人为主体的侵权行为。主要表现为:

(1) 未经个人信息主体同意或授权,擅自在网上公开、宣扬、散布、泄漏、转让他人的或与他人之间的个人信息;

(2) 未经个人信息主体同意或授权,窃取、复制、收集他人传递过程中的电子信息;

(3) 未经个人信息主体同意或授权,擅自侵入他人的电子邮箱、发送垃圾邮件、邮件炸弹或恶意病毒等;

(4) 未经个人信息主体同意或授权,擅自侵入他人的个人信息系统,收集、破坏、窃取他人的个人信息等。

如在 BBS 或公共聊天室中公布、散布、张贴他人的个人信息,就是一个典型的例子。

2. 网络服务商为主体的侵权行为。网络服务商向公众提供网络技术、设施和服务等信息交流所需的基础条件,不论是有偿服务,还是无偿服务,均应采取必要的管理措施和相应的技术手段,保证用户的个人信息安全。但是,用户的个人信息具有无形的价值属性,一些网络服务商为谋取巨大的经济利益,肆意侵犯用户的权益。主要表现为:

(1) 用不合法的手段、不合理的目的,收集、保存用户的个人信息;

(2) 以不合理的目的,过度收集、使用个人信息;

(3) 未经个人信息主体同意或授权,不合理利用或超目的、超范围滥用个人信息;

(4) 未经个人信息主体同意,擅自篡改、披露个人信息,发布错误的个人信息;

(5) 未经个人信息主体同意或授权,擅自将所保存的、经合法途径获得的个人信息提供给商业机构,造成个人信息的不合法公开、泄漏或传播。

号称全球最大的搜人引擎 Ucloo,可以搜索到近 9 000 万华人详细的个人信息资料,包括个人的家庭、生活、工作等各个方面,而只需花费一元钱、输入姓名即可。Ucloo 服务商在未得到个人信息主体同意或授权的情况下,以获取最大经济利益为目标,保存和收集个人信息,用于不合理的目的;不合理或不合法地利用或滥用个人信息,造成个人信息的泄漏、传播或不合法的公开。Ucloo 服务商的行为是典型的侵犯个人隐私的行为。

3. 生产厂商为主体的侵权行为。生产厂商在制造销售的网络基础设施中设计了专门的功能,以收集用户的信息;或存在漏洞,为某些专业人员窃取用户的信息提供了便利,使用户的个人信息资料受到侵害,如微软操作系统、INTEL 奔腾产品等。

还有许多形式的侵权行为,如以商业机构为主体的侵权行为,以网上调查、市

场调查为名,跟踪、记录用户的网上行为,收集用户的个人信息资料,并转让、出卖,以获取利润,或用于其他商业目的等。

网络服务商在个人信息收集和利用中,存在信息不对称问题,是引发网上个人信息侵害愈加严重的原因之一:

1. 地位不对称。网络服务商在收集和利用个人信息时,在个人信息的使用目的、范围、方法等方面处于主导地位,可能提出一些不合理的要求,强迫用户接受。用户则处于被动地位。

2. 信息不对称。网络服务商在收集、利用个人信息时,用户被告知的信息是有限的,个人信息的使用目的、范围、方法等使用情况,并未完全通知用户,用户也缺乏对相应技术的了解。

1.2 博客与隐私

在网络应用中,博客,由于其特殊的网络交流方式,是发展最为迅猛的。2008年11月,在上海召开的第二届中美互联网论坛上,中国个人博客数量的迅猛增长受到特别关注。中国国务院新闻办公室副主任蔡名照向与会精英披露,“去年,中国个人博客有4 000多万,今天中国的博客数量已达到1.7亿,网民拥有博客的比例高达42.3%。”

另据中国互联网协会理事长胡启恒透露的另一项排名则显示,目前中国互联网的十大应用领域中,博客及个人空间,位列第八,排名超过了论坛、BBS、网络购物。

博客是继E-mail、BBS、ICQ之后出现的又一种网络交流方式,代表新的生活方式和工作方式,甚至成为新的学习方式。它是一种表达个人思想、网络链接内容,按照时间顺序排列,并且不断更新的出版方式,综合了多种原有的网络表现形式。通常由简短且经常更新的帖子构成。其内容和目的可以有很大的不同,从其他网站的链接和评论、有关公司或个人构想,到日记、照片、诗歌、散文,甚至科幻小说的发表或张贴,林林总总,包罗万象。

然而,博客的开放性,如果与搜索引擎结合,将使普通人无所遁形,引发个人隐私泄露的危险。通过博客和搜索,就可以随便搜索到普通人的生活琐事、喜怒哀乐。可能博客(写手)不会在博客中公布真实的个人信息,但绝不可以无视这一问题。无论怎么谨慎,总会无意中透露些微个人隐私。根据这些个人隐私,可以轻易收集到博主的个人信息。

《深圳青年》2009年第15期的一篇文章,讲述了一则在博客上看到的故事。小标题是“信息危机:小心你的博客”,文章大意如下:

一位在美国工作的同胞,因为性格比较内向,怯于社交,单身一人。为了排遣独在异乡的寂寞,向来极度低调的他终于在一年多以前开始写博客解闷(博客博主)。虽然他感觉自己所写的日志无非就是日常起居的流水账,但在偶然闯进他博

客的人看来,竟充满了别样的吸引力。因而,他的博客不久就游荡起一小帮同样身在美国且为孤独所困的博友。

一天,博主打开电脑,收到一封陌生女孩的邮件。女孩自称为博客读者,将在第二天飞到博主所在城市,与博主相见。邮件称,她已知道博主住址,可以轻易找到。博主自知从未在博客中公布过个人信息,因而以为是恶意玩笑,并未在意。

然而,第二天下班回到住所,竟真有一个女孩等在门口。女孩进屋就开始炫耀“人肉搜索”技能:利用博主在博客中透露的点点蛛丝马迹,经过无数次 GOOGLE 搜索和地面人脉打探,最终确定了博主的电子邮箱和住址……

同样,利用博客泄露他人隐私也不乏其例。如苏州“博客门”事件:据《检察日报》报道,一位苏州工业园区管委会招商局副局长把自己同时与4个男性领导保持不正常关系的事情以日记方式公布在博客中,网民经“人肉搜索”,曝光了事件所涉及的人员;杭州一女子因被人以连续98篇博客曝光个人隐私而诉至法院……

备受关注的“中国博客第一案”,原告陈堂发是南京大学新闻传播学院的一名副教授,他发现在中国博客网的一个网页上,一篇名曰《烂人烂教材》的博客日志里,博客主人“K007”指名道姓地辱骂他,诸如什么“猥琐人”、“流氓”、“烂人烂教材”等,并已在网页上保留了2个多月。原告协商无效后诉至法院。虽然,“中国博客第一案”以原告的胜诉告终,但暴露了网民、网站经营者法律意识淡薄,法律的有效制裁措施欠缺,个人隐私权在博客面前的脆弱。

博客中凸显的个人隐私隐患,是网络应用中个人信息侵害的典型事例。

1.3 现实生活中的个人信息侵害

现实生活中,个人信息随意传播、公开、泄露、滥用的现象随处可见。人们可能会有意或无意地泄漏自己的个人信息,泄漏形式是多种多样的:一次抽奖活动、申报某项事务,如申请信用卡、订阅杂志、一个电话、应聘、住宿等,个人信息就可能进入商家预先设计的数据库中,成为商家获取利益的筹码。当某个人或某商家对你的姓名、工作单位、电话号码、身份证号码、生活信息等个人信息资料了如指掌时,而你对此却一无所知。

很多人可能有过这样的经历:刚刚购买一套商品房,就不断收到装修公司,甚至是房屋中介公司的电话或短信,他们知道房子的户型、面积等详细信息;一个孩子刚刚出生,婴幼儿用品广告就做到了家门口,他们知道孩子的性别、出生时间等;刚办理了新车入户,保险公司会立即打电话推销;如果在某个公共场合接受了市场调查,就可能收到许多莫名的广告宣传或“骚扰”电话……

大量的个人信息合法地掌握在许多公共机构、政府行政机构、提供公共服务的公司:学校有学生的个人资料、医院有病人的病历档案资料、司法公安机关有当事人的个人隐私资料,以及工作单位、银行、移动通信……某些个人或商家可以轻易

地与管理个人信息的权利机关结合, 监听、获取个人信息资料, 如2006年11月, 中央电视台、深圳电视台曝光的“深圳市车管所将车主资料出卖给套牌制造分子”、2007年4月中央电视台《新闻调查·约会新7天》“我们的隐私是否被侵犯”、2009年3·15晚会曝光的公开叫卖个人信息的海量信息科技网, 全国各地的车主信息、各大银行用户数据, 甚至股民信息等一应俱全, 且价格极其低廉, 很清楚地说明了这个问题。

在现代社会、经济活动中, 个人信息的无形的价值属性, 驱动人们不遗余力地攫取。对商家而言, 谁拥有更多的个人信息, 谁就拥有更大的潜在的经济利益, 并由此催生了一些以买卖个人信息资料为业的商家和个人。

在我国, 人们对个人隐私的认识比较模糊, 重视不足, 与历史的文化遗产有关。在实际生活中, 人们可能公开谈论涉及个人隐私的话题, 已是司空见惯。为某些商家或个人收集个人信息资料提供了便利条件。这些收集方式可能包括:

1. 通过已公开的信息, 或在平常的人际交往、工作关系中收集并累积个人信息;
2. 通过在公共场所进行市场调查、问卷调查等形式, 获取个人信息;
3. 采用某种方式, 与具有大客户群的单位, 如医院、学校、酒店、商场、楼盘销售处等, 建立联系, 获取、累积个人信息。
4. 其他方式, 如窃取的个人资料: 身份证或复印件、应聘资料、登记表等, 造成个人信息的任意传播或滥用, 甚至对个人信息主体构成威胁等, 多种多样。

在个人信息的经济价值日益凸显, 信息处理成本愈来愈低的情况下, 个人信息泄漏、滥用的危险也日益严重。

附录1是《南都周刊》2009年11月9日刊载的一篇文章, 披露了透过手机“偷窥”个人隐私的示例。

1.4 个人信息安全的影响

信息技术的发展使信息传递和处理更加方便、快捷, 特别是网上金融交易、网上购物、网络聊天、网络游戏等基于网络行为的实现, 大量的以个人为主体的信息在网间流动, 使个人信息的侵害行为, 成为新的信息公害。

个人信息主要体现在信息服务业、金融保险业、医疗服务业、政府机关、电信业、教育、广告及印刷、劳动服务业、制造业等行业中, 随着现代信息服务业的深入, 正逐渐向全社会展开。社会、政治、经济等各个行业在计算机网络系统、相关软件及数据处理、社会生活的各个方面经常涉及个人信息的使用和处理, 因此, 凸显个人信息安全的重要性。

个人信息安全早已引起许多国家的关注, 并采取了相应的措施。国际上已有50多个国家和地区制定了相关法规和标准, 以图保证个人信息在政治活动、经济

活动、虚拟空间中的安全。这些国际组织、机构和国家建立的个人信息安全方面的主要法规有:

- 1973 年瑞典颁布《数据法》;
- 1974 年美国颁布《隐私法》;
- 1976 年联邦德国颁布《联邦数据保护法》;
- 1978 年法国颁布《数据处理、档案与自由法》;
- 1980 年欧盟颁布《关于保护自动化处理过程中个人数据的条例》;
- 1980 年 OECD 发表《隐私保护和个人数据跨国流通指导原则》;
- 1982 年加拿大颁布《隐私保护法》;
- 1984 年英国颁布《数据保护法》;
- 1986 年美国颁布《电子通信隐私法》;
- 1995 年欧盟通过《个人数据保护指令》;
- 1996 年欧盟通过《电子通讯数据保护指令》;
- 1999 年欧盟制定《Internet 个人隐私保护的一般原则》;
- 1999 年美国公布《互联网保护个人隐私的政策》;
- 2005 年日本颁布实施《个人信息保护法》。

其中,世界经济合作发展组织 (Organization for Economic Co-operation and Development, OECD) 1980 年颁布的《隐私保护和个人数据跨国流通指导原则》中有关个人信息保护的八项原则,成为各国一致遵循的原则,许多国家在此基础上制定或不断补充、完善本国的个人信息保护法规。OECD 八项原则是:

1. 收集限制原则。个人信息的收集必须采取合理合法的手段,必须征得个人信息主体的同意。
2. 信息质量原则。个人信息必须在利用目的范围内保持正确、完整及最新状态。
3. 目的明确化原则。个人信息收集目的要明确化。
4. 利用限制原则。对个人信息资料不得超出收集目的范围外利用。
5. 安全保护原则。对个人信息的丢失、不当接触、破坏、利用、修改、公开等危险必须采取合理的安全保护措施加以保护。
6. 公开原则。个人信息管理者必须用简单易懂的方法向公众公开个人信息保护的措施。
7. 个人参加原则。个人信息主体的权利,包括:确认个人信息的来源、个人信息的保存等;收集、利用的质疑;修改、完善、补充、删除等。
8. 责任原则。个人信息管理者有责任遵循有效实施各项原则的措施。

八项原则体现了对人的尊重和对个人信息的规范管理,在保护个人信息的同时,让个人信息能真正实现自身价值和更好地为公众服务。个人信息的安全防护不是为了限制个人信息的流动,而是对个人信息流动进行正规的管理和规范,以保证能够符合个人信息主体同意的目的,保障个人信息的正确、有效和安全,保证个人

信息能够在合理、合法的状态下流动。

我国与个人信息安全相关的法律条文,散见于宪法、民法、刑法等法规中,没有专门的保障个人信息安全的法规;公民和社会普遍缺乏个人信息安全意识,个人信息经常性被不合理地公开甚至滥用。这种状况由于国际上对个人信息的关注直接影响到我国的对外交流。随着国际交流的增加和国际业务的增多,与实行个人信息保护的国家进行项目合作和交流时,这些国家会考虑我国个人信息安全情况,而且将优先选择实行个人信息安全防护的国家。因此,个人信息安全已成为国际业务交流中一项重要的制衡条件。

软件外包业务是我国的重点产业之一,大量软件及信息处理业务来自国外。国外客户对个人信息安全的要求,已经对承接软件及信息外包业务造成了影响。特别在对日外包业务中,由于日本颁布、实施了个人信息保护法,特别是自1998年4月1日创建针对日本信息处理企业的P-AMRK认证制度,对软件外包企业意义深远。

大连是我国软件外包基地之一。从个人信息安全对大连软件与信息服务业的影响可以窥见一斑:

1. 产业整体表现为:信息服务业客户对加工信息发包谨慎,软件加工业客户不提供真实测试数据。

2. 客户向承接外包项目的企业提出个人信息安全的具体要求,并在合同中增加个人信息安全相关条款和违反规定的处罚。因有关个人信息保护不当所造成损失的处罚金额相当高。

一些承接外包项目的企业着手建立个人信息保护制度,但这种单个企业建立的个人信息保护制度,不能得到国外客户对个人信息保护整体状况的认可。

1.5 个人信息安全范畴

追踪个人信息安全的历史,最早可追溯到2400年前的古希腊。被西方尊为“医学之父”的古希腊著名医生、西方医学奠基人希波克拉底(Hippocrates),在著名的“希波克拉底誓言”中,要求医生必须遵守职业医德,不得泄漏个人信息:“……在治病过程中,凡我所见所闻,不论与行医业务有否直接关系,凡我认为要保密的事项坚决不予泄漏。”这可能是最早的保护个人信息安全的形式。

社会发展到21世纪,信息技术的迅速普及,使社会生活方式发生了根本变革。公共空间和个人空间的界限日益模糊,个人隐私的安全受到巨大冲击。

在现实生活中,经常会发生这样的事情:我们的手机会收到莫名的短信,电子邮箱会收到垃圾邮件……网络攫取了我们的个人信息,并被无限滥用。

电子政务是政府机构应用现代信息通信技术,以网络技术为基本手段,实现管理流程优化和服务扩展的综合性信息系统。通过电子政务,管理政府的公开事务、内部事务,为公众提供政府服务平台。

在电子政务环境中,政府借助信息通讯技术,提高行政效率和管理水平,维护公共利益。在为公众提供各种服务时,必然通过网络收集、储存、管理和利用个人信息,但个人信息处理的随意性,极易侵犯公民的个人利益。

电子商务是企业之间、企业和消费者之间利用计算机技术、网络技术和远程通信技术进行的各类商业活动,包括货物贸易、服务贸易和知识产权贸易等。

电子商务伴随着大量个人信息的流动,在电子商务活动中,为了解用户上网、消费习惯、提供个性化的服务,往往在用户注册时,根据不同的需要,要求用户提供简单的或详细的个人信息,如详细的姓名、通信地址、电话、电子邮件等,甚至个人兴趣、性别、职业、收入、家庭状况等,同时也可以利用技术方法获得更多他人的个人信息。

这些个人信息的再利用,是威胁个人信息安全的隐患。许多电子商务经营者未按承诺提供保密措施,甚至向其他网站出售个人信息,以谋取经济利益。

在软件外包业务中,大量软件及信息处理业务来自于国外。国外客户的信息、公司员工的个人信息、银行保险等商务信息的安全,直接影响外包业务的承接。

因此,个人信息安全的内涵丰富、外延广泛。采用自动或非自动处理方式收集、录入、加工、编辑、存储、管理、检索、咨询、交换、传输、输出、使用、提供、委托等或其他利用个人信息的行为,均在提供个人信息安全保护的范畴之内。

第2章 基本概念

本章探讨个人信息安全领域的一些基本的概念，这些基本概念是在个人信息安全实践中总结和提炼出来的，对理解、学习个人信息安全知识具有重要意义。

2.1 信息

2.1.1 信息的普遍性

信息是人类生产活动、社会活动中的基本载体，承载以文字、符号、声音、图形、图像等形式，通过各种渠道传播的信号、消息、情报、资料、文档等内容。信息普遍存在于自然界、人类社会和人的思维之中。

信息与我们人类的历史一样久远。人类自诞生以来就在利用信息，从结绳记事、文字发明到今天计算机的大规模应用，均包含着信息的产生、传递、识别、显示、提取、控制、存储、处理、利用。

早在殷商时期，根据殷墟出土的甲骨文记载，殷商盘庚年代（公元前1400年左右），国境四方戍卒向天子报告军情的记述，有“来鼓”二字。经考证，“来鼓”即以鼓报警，是我国古代与烽燧并行的传递报警信息机制。

2700年前的周幽王时代，已经有了利用烽火台通信的方法。有所谓“烽火戏诸侯”的故事：“褒姒不好笑，幽王欲其笑万方。不笑。幽王举烽火。诸侯悉至，至而无寇。褒姒乃大笑。幽王悦，为数举烽火。其后不信，诸侯益不至……待西夷犬戎攻幽王。幽王举烽火徵兵。兵莫至。遂杀幽王骊山下，虜褒姒。”可以窥见利用烽火台传递信息的概貌。

随着社会的发展和政治军事的需要，周代逐步形成了传送各类官府文书的更加严密的驿站制度，并与烽火台互为补充，配合使用。

社会发展到20世纪初，随着电报、电话、照片、电视、传真、通信卫星等先进技术的先后出现，信息传递更加方便、准确、迅速、快捷。特别是计算机的出现，随着计算机技术、数据库技术、通信技术、网络技术的迅速发展，信息处理技术进入一个全新的发展阶段。

因此，信息在我们的社会、生产等活动中无处不在，始终伴随着我们。信息贯穿人类社会的发展历史，是人类社会实践的深刻概括，并随着人类的发展进步而不断演变、发展。历史上发生过五次与信息相关的技术革命，推动了人类社会的进步和经济的发展：

1. 从猿进化到人的重要标志——信息交流的手段和工具——语言的创造和使用；
2. 信息产生、传播、存储跨越时间和地域限制——文字的出现；
3. 扩大信息交流和传播的范围和容量，提高信息的可靠性——造纸和印刷术