

·域外掠影·

德国联邦数据保护法的发展趋势

马民虎 冯立杨 (西安交通大学法学院 陕西西安 710049)

摘要:德国数据保护法作为世界范围内产生较早、影响力最大的数据保护立法,对世界各国的数据保护立法具有重要影响。近几年来德国《联邦数据保护法》应技术和社会发展的要求进行了数次修改。文章通过对该法近年来修改内容的具体考察,总结归纳了其修改的原因,并对该法未来的发展趋势进行预测,以期为我国数据保护相关立法活动提供可资借鉴的模式。

关键词:数据保护 合法拦截 发展趋势

中图分类号:D923.4

文献标识码:A

文章编号:1003-6938(2009)01-0103-05

The Trends of the German Federal Data Protection Act

Ma Minhu Feng Liyang (School of Law, Xi'an Jiaotong University, Xi'an, Shanxi, 710049)

Abstract: As one of the worldwide earliest and the greatest data protection legislation, German data protection law has had a major impact on the world of data protection legislation. In recent years, Germany "Federal Data Protection Act" had been amended several times with the requirements of technology and social development. This article investigated the content of the amendment in recent years of this act, summed up the reasons of this change and forecasted the development trend of it. China's data protection legislation can learn many things from this model.

Key words: data protection; lawful interception; trends

CLC number: D923.4

Document code: A

Article ID: 1003-6938(2009)01-0103-05

信息经济的发展以及信息技术的普及,使数据成为最重要的生产要素之一。工业时代以资本、能源为核心的经济发展模式逐渐向信息化、虚拟化的信息经济转型。在这个过程中,各种各样的数据成为经济生活的重要组成部分,尤其是密切关系个人利益的个人信息也成为具有一定财产属性的“利益共同体”。

个人信息^①不仅仅是个人人格利益的重要组成部分,它还可以为政府、企业决策提供依据。通过对海量个人数据的统计与分析,可以获得关于一个社会群体或社会阶层的政治倾向、消费特点,以及其他对信息持有者有用的信息。个人信息兼具社会经济资源和个人人格利益两种价值。^[1]社会本质上是由个人

组成的集合体,当个人数据组合到一起,并运用统计学、概率论等数学方法进行分析、甄别之后就存在两种利用价值。一是公共管理方面的利用价值,一是商业利用价值。非公共机构尤其是营利性的非公共机构收集个人数据的目的在于个人数据的商业利用价值。个人信息不直接具有财产内容,但经过开发利用能够产生经济利益。企业通过收集个人信息,增加对顾客的了解,有利于做出更好的决策,同时增强了预测市场发展的能力,有利于对未来做出更好的决策。例如,有银行将客户的个人信息出售给保险公司,从而使保险公司得以向顾客推销业务。^[2]由于个人信息存在可观的价值,因而各种非公共机构都热衷于收集个人信息并加以开发利用,这就使得个人信息

①《联邦数据保护法》(第3节(1)条)中的个人信息是指“任何关于一个已识别的或可识别的个人(数据主体)的私人或者具体情况的信息”。

基金项目:本文系国务院信息化领导小组办公室“德国数据保护法与欧盟电子信息技术拦截法律标准发展趋势研究”(S2007W003)项目研究成果之一。

收稿日期:2008-07-06;责任编辑:刘全根

泄露和滥用的风险大大增加,导致本来稳定的管理关系、买卖关系充满了风险和不确定性,使社会经济关系日趋紧张。

因此,信息经济高度发达的西方国家率先制定了一系列针对个人数据问题的法律法规,其中又以德国的《联邦数据保护法》最为著名。这部法律体系完整、结构清晰、规范明确,对促进个人权利保护和个人数据合法开发利用起到了至关重要的作用,在维护社会生活稳定的同时也促进了信息经济的发展。基于信息技术的数据活动在大大促进经济增长的同时,也带来了许多挑战,尤其是给国家安全和公共利益造成了新的威胁。因此,德国联邦数据保护法数次修改,在保护个人数据权利的同时,对个人数据权利做出了诸多限制,为侦查机关拦截个人数据、维护国家安全提供了法律依据。这是一条值得关注的清新溪流,将融入“以人为本”的数据保护立法潮流中。

2006年11月15日德国《联邦数据保护法》进行了21世纪之后的第三次修订。这部产生于1977年的法律在20世纪的最后20余年时间之中也不过进行了四次修改,2000年之后平均每两年一次的修改,其频率不可谓不高,而且其内容的大幅调整也是前所未有的。纵观2001年、2003年和2006年德国《联邦数据保护法》的三次重大修订,我们不难发现德国在个人数据保护立法和司法层面的新趋势。

1 对新技术的规范不断进入立法视野

信息技术的发展不断给传统法律带来新的挑战。^[3]从上世纪90年代进入信息社会以来,信息技术发展日新月异,各种各样的新技术层出不穷,尤其是网络的普及使得个人数据传播途径多样化、便捷化。数据一旦泄露,将会在短时间内迅速传播,且其传播范围之广不可估量,这给个人数据保护带来了严峻的挑战。一方面,数据保护立法必须关注信息技术的发展,不断吸纳技术发展带来的个人数据保护的各种新问题。因此,《联邦数据保护法》适应网络时代技术发展的特征,对一些收集、存储、处理、传播个人数据的新技术进行了相应的规范。另一方面,国家用以进行数据合法拦截的各项技术手段也需要通过法律予以明确界定,以限制国家权力的滥用,从而有效地保护个人数据的隐私性。

21世纪之后,德国《联邦数据保护法》的历次修改对各项新兴信息技术给予了极大的关注,将许多新技术列入法律规制的范畴,通过法律形式来应对新技术所带来的数据风险和社会问题。具体表现在:

(1)对“自动做出的个人决定”进行限制(第6a节)。这是基于数据自动处理技术的发展而做出的新的法律规定:“不能仅仅依据用于评价其个性的数据自动化处理程序作出将给数据主体带来一定法律后果,或者严重损害数据主体利益的决定。”

(2)规定了对公共领域进行电子监控的条件(第6b节)。随着图像技术和电子技术的发展,对公共领域进行电子监控变得十分容易实现。国家凭借其掌握的权力资源和技术优势,利用监控技术收集公共领域的个人数据无疑会侵害社会公众的人身权利。因此,有必要通过法律严格限制国家对公共领域的电子监控。“只有在履行公共任务、行使允许或拒绝他人进入的权利、为具体的确定的目的追求合法利益,并且没有证据表明数据主体的合法权益更为优先时,才允许对公共领域进行电子监控。”

(3)对“个人数据移动存储和处理介质”的使用做出规定(第6c节)。个人数据移动存储和处理介质的普及和大量使用带来了巨大的个人数据泄露风险,因此,必须强化这些介质的发放机构在这些介质上运行或修改个人数据的自动化处理程序,明确发放机构告知数据主体相关信息的义务。这些信息包括:上述机构的性质和地址、该介质的运作模式、要处理的数据类型、该介质丢失或损坏时应采取的措施。这样就保证了数据主体的知情权,以便于他们做出选择:是否应该使用此类介质?使用哪一机构提供的介质?

(4)对“电子目录或登记簿”中包含的个人数据问题做出规定(第29节(3)条)。随着“无纸化办公”的实现,大量的目录、表格、登记簿都采用了电子存储的形式,个人数据不再仅仅停留在纸面上,而是以新的形态出现。“如果电子或印刷目录或登记簿中包含的个人数据明显违背了数据主体的意志,则电子或印刷的地址、电话、分类或类似目录中不得含有个人数据。”

(5)增加了数据控制人^①应当采取的技术和组织措施的种类(第七编附则第3、7、8条)。为了使数据控制人对其持有的个人数据尽到合理的注意义务,必须要求它们采取必要的技术手段保证这些个人数据的安全。例如“进入控制”措施:“确保获得授权进入数据处理系统者能够获取的数据仅限于其被授权获取的部分。在数据处理和使用过程中及数据被存储后,未经授权不得进行查阅、复制、修改或者删除。”此外,数据控制人还应当确保个人数据免于意外损坏或丢失,确保为不同目的而收集的数据进行分别处理。

① 数据控制人(Controller)指任何为自己收集、处理或使用个人数据的个人或机构,或者通过委托他人上述行为的个人或机构。

2 数据保护范围的持续扩大

20世纪90年代以来欧盟掀起了个人数据保护指令的变革,这次变革不仅仅是信息时代技术发展的要求,也是欧盟为主动适应信息时代的特点而建立统一的个人数据保护标准所做出的努力。欧盟1995年10月24日通过了《关于涉及个人数据处理的个人保护以及此类数据自由流动的指令(95/46/EC)》。这一指令要求欧盟各国采取欧盟统一标准对个人数据进行保护。为适应欧盟对其成员国个人数据保护的统一要求,欧盟各成员国相继制定了本国的数据保护法,或者对已有的数据保护法进行修改。^[4]欧盟在2006年3月15日公布了《关于储存因提供公用电子通讯服务或者公共通讯网络而产生或处理的数据及对2002/58/EC号指令的修正(2006/24/EU)》,其第15条规定:成员国最迟应当在2007年9月15日之前根据本指令修改其法律、条例和行政规定,并将此事项及时告知委员会。

德国作为欧盟的成员国,有义务将欧盟指令的要求内化到其国内立法之中,因此德国基于欧盟指令的要求对《联邦数据保护法》进行修改以适应整个欧洲对个人数据保护的新趋势。《联邦数据保护法》对个人数据的保护范围进行了扩大,这种扩大表现在两个方面。其一是将数据保护法的规制范围扩大到个人数据流动的整个过程,运用“过程控制”理论将包括个人数据的收集、处理、储存、传输、利用、删除以及贴标隔离在内的个人数据流动周期纳入法律规制范围。其二,法律所保护的个人的种类越来越多,增加了对“特殊种类的个人数据”的保护。

2001年的修改中,数据存档的定义扩大了,实际上扩张了《联邦数据保护法》的适用范围,将“许可”的范围扩大到“数据收集”阶段,规定数据的收集需要法律许可或数据主体同意。法律保护的个人的种类越来越多,特殊种类的个人数据也被纳入了数据保护法的调整范围。具体表现在:

(1)扩大了“数据控制人”的范围,不再局限于“数据存储”活动而是包括了“收集、处理、使用”在内的整个数据流程(第3节(7)条)。

(2)对接受数据的“第三方”的定义加以明确。指出“第三方”不包括数据主体及那些受委托在德国、欧盟其他成员国或者欧洲经济区域协议缔约国内收集、处理或使用个人数据的个人或机构(第3节(8)条)。

(3)增加了“接收者”、“特殊种类的个人数据”、“个人移动存储和处理介质”的定义(第3节(8)、(9)、(10)条)。其中“特殊种类的个人数据”是指关于种族血统、政治观点、宗教信仰、党派、健康状况或性生活的信息。这些个人数据又被称为“敏感数据”,密切关系数据主体的人身利益,因此需要法律给予特别保护。修改后的《联邦数据保护法》明确了收集特殊种类的个人数据的条件(第13节(2)条),规定了“为其他目的而存储、修改或使用特殊种类的个人数据”的条件(第14节(5)条)。

(4)将“获得数据主体许可”的范围扩大到“数据收集”阶段,规定数据的收集需要法律许可或数据主体同意(第4节(1)条)。不仅个人数据的处理、使用需要获得数据主体的许可,个人数据的收集也必须取得数据主体的同意。

(5)增加了对“个人数据向国外以及跨国或者国际机构传输”的规定(第4b节)。如果数据主体享有排除数据传输的权益,或者数据接收方不能保证合理的数据保护水平时,不得进行数据传输。对数据合理保护水平的判断要综合考虑数据的种类、数据处理目的和持续时间、数据来源国和接收国,以及适用于接收者的法律形式、专业规则和安全措施。传输机构还负有告知数据主体数据传输事实及其目的的义务,并承担许可传输的责任。

(6)增加“数据传输的接收者和接收者种类”为数据控制人向数据主体提供的信息之一(第19节(1)条第2款),增加了在相关个别情况中,为保护数据主体的合法利益而对数据进行贴标隔离的规定(第20节(6)条)。“有关机构如果不对数据进行贴标隔离,数据主体的合法利益将会受到损害,并且此数据对相关机构履行其职责不再需要,则既不在自动程序中处理的也不在非自动存档系统中保存的个人数据应当被贴标隔离。”

3 数据保护官和监管机构权力的持续扩张

为更好的保护个人数据,德国《联邦数据保护法》赋予数据保护官和数据监管机构^①的权力不断扩张。同时,数据保护官和数据监管机构权力的扩张也为个人数据的合理利用,例如为国家利益和社会公共利益等而进行的合法数据拦截,提供了权力基础和法律依据。

在《联邦数据保护法》2001年的修改中,明确规定“公共机关和私人机构应当为数据保护官行使职责提供支持”,增加了关于监管机构职权的规定。监管机构应当监督数据保护法的

^①数据保护官受自动收集、处理或使用个人数据的公共机关和私人机构的书面委托,直接服从于公共机关或者私人机构的领导,使用专业知识进行数据保护。联邦数据保护与信息自由专员是根据联邦政府的提名,由议会选举,总统任命,隶属于联邦内务部,进行数据保护与监督活动的政府官员。

执行,可以为监管目的进行数据传输,登记自动化处理交易。

2006年的修改则赋予数据保护官更多权利,以保证数据保护官更好地行使职权,保护个人数据。具体内容如下:

(1)规定了公共机关和私人机构协助数据保护官保护个人数据的义务。“公共机关和私人机构应当为数据保护官行使职权提供支持,特别是助手、场所、设备、以及其他资源。”(第4f节(5)条)数据控制人还应当向数据保护官提供必要的信息目录、人员名单等(第4g节(2)条)。

(2)数据保护官监测内容的范围扩大,延伸到专业上以及职务上的秘密,特别是财务会计法第30节规定的税务秘密(第4f节(2)条)。

(3)赋予数据保护官拒绝作证的权利(第4f节(4a)条),数据保护官的助手也拥有此项权利。在数据保护官拒绝作证的权利适用范围内,数据保护官的档案和其他文件不得被扣押。

(4)增加了数据保护官的职责,数据保护官可以依据《联邦数据保护法》的有关规定提供咨询服务(第4g节(1)条第2款)。

(5)由于某些小型私人机构受到治理结构、资金实力的制约,可能不具备指派数据保护官的客观条件,但出于保护个人数据的目的,又必须有相关人员负责执行《联邦数据保护法》的相关规定,因此该法第4g节(2a)条规定,由私人机构的首脑履行数据保护官的职责,监视用于个人数据处理的程序是否被合法使用、及时通告自动化处理个人数据的计划、采取适当措施增进个人数据处理人员对相关法律的了解。这样,就避免了小型私人机构无人负责个人数据保护工作的局面,使个人数据保护渗透到社会生活中的各个组织机构。

(6)增加了关于个人数据保护监管机构职权的规定,扩大了监管机构的权力范围。监管机构应当监督数据保护法的执行和适用。“监管机构可以为监管目的处理、使用、存储个人数据”,“监管机构可以为了监管目的给另一个监管机关传输数据”(第38节(1)条),这实际上成为个人数据保护的一种例外,为监管机构利用个人数据提供了法律基础。监管机构还应当编制强制注册的个人信息自动处理部门名单供社会公众查阅(第38节(2)条)。此外,监管机构还可以要求数据控制人提供必要的信息而且不得迟延,监管机构可以对机构团体的所有物和经营场所进行检查,内容包括商业文件、储存个人数据和数据处理程序的设备(第38节(3)、(4)条)。监管机构还可以要求数据控制人采取措施纠正技术或组织上的违法行为,如果在合理期限内没有纠正,监管机构可以禁止特定数据处理程序继续使用,监管机构如果认为数据保护官不具有专业知识或不具备履行职责的可靠性,可以将数据保护官免职

(第38节(5)条)。

4 立法增加数据保护的例外情形

个人数据保护例外情形的增多,一方面是信息经济发展对信息自由流动的要求,另一方面则是基于国家安全与公共安全的需要。

信息自由流动与信息安全保护的博弈,要求法律必须在二者之间保持平衡。信息天然具有流动性,而且信息的流动性是不可逆的,这是信息经济赖以存在和发展的基础。信息就是财富,如果信息不能流动,那么就不能参与到生产过程中,无法成为市场要素,更不能促进经济的增长。所以,在信息时代要保证经济的增长,促进经济转型,就必须保证信息的自由流动。但是,信息安全问题也是由信息的流动性造成的。由于信息的流动性,个人数据像具有实体的财产那样为数据主体所掌控。个人数据会被收集、使用、处理、传输,而且可以在数据主体不知情的情况下流动。这使个人数据完全不能由数据主体掌握其流动的方向和方式,在客观上,数据主体也无法掌握。所以,就产生了个人数据泄露与滥用的危险。

数据保护法必须兼顾信息流动与信息安全两个方面。既要追求信息自由,促进经济增长,同时,也要保护信息安全,保护数据主体的利益,维护信息社会关系的稳定。原有的数据保护法对个人数据安全保护的追求胜过促进信息自由,过于严格的个人数据保护法不利于信息经济的发展。《联邦数据保护法》的修改适应了信息经济发展的要求,对个人数据保护的例外情形越来越多。

数据保护例外情形的增多也是国家安全与公共安全的需要。现代社会网络犯罪日益增多,基于网络的恐怖活动和其他危害国家安全、公共安全的活动也屡见不鲜。因此,国家为打击网络恐怖活动、侦查网络犯罪有必要对个人数据进行合法拦截和存留。个人数据保护在这些方面必须让位于国家利益、社会利益。如果片面强调个人数据保护,将其视为绝对的权利,无疑将会为网络恐怖活动和网络犯罪提供极大的便利。如果诸如黑客攻击所遗留的个人数据、网络犯罪分子所利用的个人数据无法被国家安全、公共安全机关所获得的话,那么犯罪证据的取得、对犯罪案件的侦破、对犯罪分子的惩罚都将成为空谈。这将大大增加网络社会的风险和社会运行的成本,因此,必须赋予国家依照法定程序合法拦截个人数据的权力。《联邦数据保护法》的修订则为个人数据的合法拦截、存留提供了法律依据。具体表现在:

(1)2001年《联邦数据保护法》的修改中,规定了没有数据

主体参与的情况下进行数据收集的条件:法律规定或强制预先许可此种收集,要履行的行政职责的性质或者事务目的,有必要从其他个人或者机构处收集数据,或者从数据主体处收集数据需要付出的努力极不合理,并且没有迹象表明数据主体需要保护的重要利益受到了侵害(第4节(2)条)。这实际上为合法拦截提供了法律依据。

(2)规定了数据控制人进行数据传输的例外,具体包括:数据主体的同意,履行数据主体和数据控制人之间的合同,或者应数据主体要求履行的合同义务,有必要进行数据传输,数据控制人为了数据主体的利益已经或者应当与第三方缔结的合同的签订或者履行,有必要进行数据传输,维护重大公共利益,或者确定、实施一项诉讼请求或者对其进行抗辩,有必要进行数据传输,数据传输对数据主体至关重要利益的保护是必要的,数据传输旨在向公众提供信息(第4c节),并且满足具体情况下的法律条件。

(3)规定了对公共领域进行电子监控的条件:履行公共任务、行使允许或者拒绝他人访问的权利、为了具体的、确定的目的追求合法利益的必要,而且没有证据表明数据主体的合法权益更为优先(第6b节)。

(4)增加了两种免除数据控制人告知义务的情形:法律明确规定或者为科学研究目的之必要并且告知需付出极不合理的代价(第33节(2)条第4、5款)。

(5)增加了两种拒绝受害人“因德国之声的报道侵犯其隐私”而要求获取作为侵权报道基础的已储存个人数据信息的情形:根据数据可以推断确认出具有筹划、制作或者传播广播节目专业能力者的身份;公开以研究或者其他方式获取的数据会泄漏德国之声的信息资源,导致其新闻功能被淡化(第41节(3)条第1、3款)。

(6)在与数据合法拦截密切相关的公共机关的数据处理方面,对收集特殊种类的个人数据的条件做出了更加详细的规定。这些条件包括:

- ①法律明确规定或为保护重大公共利益所必需;
- ②数据主体依本法规定表示同意;
- ③为保护数据主体或第三方的重大利益所必需,而数据主体出于身体或法律上的原因无法表示同意;
- ④所收集的数据是数据主体明显已经公开的;
- ⑤为排除公共安全的重大危险所必需;
- ⑥为排除公共健康面临的重大损害或者保护公共健康的重大利益所急需;
- ⑦为医疗或科学研究所必需;

⑧这种收集对联邦公共机关履行保卫职责,或履行国家间或国际处理危机或防止冲突的义务,或者人道主义措施来说是必要的(第13节(2)条)。

(7)增加了公共机关数据控制人向数据主体提供数据传输的接收者与接收者种类信息的要求。如果所提供的信息涉及传输到有关联邦安全的宪法保护机构、联邦情报部门、联邦武装部队反情报部门或者联邦国防部的其他机构,则信息的提供必须得到上述机构许可(第19节(3)条)。

(8)增加了对数据主体告知内容和条件的规定,不能向数据主体提供信息的条件有:

- ①不利于数据控制人正常履行其职责;
- ②会破坏公共安全或公共秩序,或者对联邦、联邦州不利;
- ③根据法律规定或其性质,尤其是基于对第三方重要合法利益的考虑,应当对数据和数据被存储的事实保密(第19节(4)条)。

5 结语

德国联邦数据保护法的改革与发展是各方面因素综合作用的结果。从外部环境来看,它深受欧盟个人数据保护指令变革的影响;从技术对法律的影响来看,这种发展是对信息技术发展带来的新的法律课题的应对;从社会经济发展的要求来看,它是数据保护法基于信息经济对信息自由流动的需求而做出的主动调整;从国家安全的角度出发,数据保护法的改革为个人数据合法拦截提供法律依据,以更好地维护国家安全和公共利益。德国联邦数据保护法的制订和修改促进了对个人数据合法权利的保护,又为信息化时代信息自由流动和合法开发提供了法律规范,促进了信息经济的发展。这部法律体系完整、结构清晰、规范明确,且根据信息技术和经济发展新情况不断作出修改,可供我国制定相关法律参考借鉴。

参考文献:

- [1]齐爱民.个人信息开发利用与人格权保护之平衡——论我国个人信息保护法的宗旨[J].社会科学家,2007(2):7.
- [2]郭永刚.银行将客户信息卖给保险公司不合适[N].中国青年报,2007-03-19(7).
- [3]马民虎.网络安全:困惑与法律对策[J].中国人民公安大学学报(社科版),2007(1):57.
- [4]国家保密局法规处.德国荷兰保密法律制度[M].北京:金城出版社,2001:31.

作者简介:马民虎(1959-),男,西安交通大学法学院教授,硕士生导师;冯立杨(1984-),男,西安交通大学法学院硕士研究生,研究方向:民商法学、信息法学。