【网络社会变革与管理】

我国个人电子密码的法律保护研究

张 琴

(南京邮电大学 人文与社会科学学院, 江苏 南京 210023)

摘 要:个人电子密码是信息安全的重要组成部分,涉及个人隐私保护,对保障交易安全具有重大意义。分析个人电子密码的法律性质和功能,结合我国对个人电子密码保护的现状,借鉴发达国家电子密码保护的相关经验,提出个人电子密码的保护建议:我国应加快个人电子密码保护立法;加快密码的标准化和专利化步伐,建立统一的个人数据保护机构,提供维权、申诉等一站式服务;加强行业自律;对窃取、泄漏、传播密码等行为加大打击力度,从而保护公民的个人信息安全。

关键词:个人电子密码;信息安全;隐私权;法律保护

中图分类号:G203 **文章编号**:1673-5420(2017)04-0030-10

随着互联网的日益普及,电子交易、身份认证等行为对密码的需求越来越多,信息安全的重要性也日渐突出。密码作为最底层的信息安全保障,对电子交易安全具有决定性的作用。实践中,违法犯罪分子窃取持卡人姓名、账号、身份证号、银行卡号、银行卡密码等信息,给当事人造成损失的案件时有发生。因密码泄露而产生的人身、财产损害的纠纷也越来越多。目前我国个人电子密码的泄漏风险有来自密码持有人(如政府机关、银行、保险公司、网络服务商、软硬件供应商等)的泄漏、传播,也有来自网络入侵者(如黑客)对密码的破译、盗取,对公民的人身权、财产权都构成极大的威胁。该问题已经引起许多国家的重视,我国也迫切需要采取措施应对。

一、个人电子密码的概念、特点及法律属性

(一)个人电子密码的概念

个人电子密码,即私人密码,是现代社会中商品交易、支付、使用电子产品的必备环节。所谓私人密码,又称私人密钥,是密码技术中与公共密钥相对应的一种密钥,由本人生成并所有且只

收稿日期:2017-08-10 **本刊网址**:http://nysk.njupt.edu.cn

作者简介:张 琴,副教授,研究方向:宪法与行政法学、信息法学。

基金项目:南京邮电大学社科研究项目"物联网时代个人电子密码法律保护研究"(NYS214011);南京邮电大学信息文科建设项目(XXWK02402)

有本人知悉,其作用在于辨识文件签署者身份及表示签署者同意电子文件内容并对数据电文进行加密[1]。个人电子密码一般由一系列不规则的数字、字母、符号、图形、声音等构成。随着科学的发展,特别是脸部辨别、指纹识别等技术的普及应用,密码越来越多地带有现代科技的特征。本文所指个人电子密码是个人密码技术和密码产品,不涉及国家秘密。

(二)个人电子密码的特点

1. 私有性或个人专属性。个人电子密码是由个人生成的、为达到交易安全或正常使用设备的目的而设的,具有个人私有且专属于个人的特点。在网络交易中,识别交易者身份主要靠密码。以网上银行为例,支付、交易的前提是成功登录,成功登录的前提是正确输入密码。如密码允许共享,势必影响账户安全。

2. 秘密性。私人密码属于个人的秘密。一般除非本人泄密,否则他人无法获知。秘密性是密码区别于其他信息的重要属性。所谓秘密性,是指有关信息不为其所属领域的相关人员普遍知悉或轻易获取,不为公众所知晓。秘密性意味着密码不得公开披露、不得被他人通过各种途径非法获得,否则将直接影响密码所有者的利益。

3. 复杂性。为了确保秘密性,个人电子密码在设定的时候就被要求以不规则的数据、字母、图形、符号设置,具有安全密级要求。复杂性越高,安全性也就越高。正因为如此,设定密码时一般不能用简单有规律的数字(如生日、电话号码、身份证号等)。只有对密码进行复杂设置,才能确保密码无法按一般常识、凭简单观察被直接破译。私人密码的技术价值在于一旦设定和输入,非经复杂的破译程序不可再现。

(三)电子密码的法律属性

我国目前尚未对电子密码的性质作明确法律规定,以致对密码纠纷的解决方法也不尽一致。关于密码的法律属性,主要有以下不同的观点:

1. 电子数据说

一般认为电子密码是通过计算机加密算法设置的密码,是以电子形式存在的数据,相当于纸面交易中的签名。《中华人民共和国电子签名法》指出,电子签名验证数据是指用于验证电子签名的数据,包括代码、口令、算法或者公钥等。可见,这部法律把密码视为电子签名验证数据。

2. 条件说

有学者提出可以将密码作为附条件的民事法律行为中的“条件”看待[2]。例如,当金融机构要求存款人设置密码时,储户实际上对存款之提取附设条件,即存款人须在输入字符并经运算与金融机构计算机系统存储的密码吻合后方能取款,密码吻合就是取款条件成就。可见,密码吻合之条件实际上属于停止条件,即法律行为于条件成就时发生效力,于条件不成就时不发生效力。依其内容而言,密码吻合则属于随意条件,即当事人一方的意见是决定其成就与否的条件。也就是说密码吻合与否取决于存款人能否回忆起并且正确输入密码[3]420-424。笔者认为,可以把此处的“条件”理解为财产所有者拥有物权或财产权的内在附加前置条件。

3. 隐私权说

美国的沃伦和布兰代斯在1890年发表的《论隐私权》一文中最早提出隐私权概念。所谓隐

私权,是指每个人都有不让别人知道自己的秘密(如私生活、习惯、病史、财产信息等)的权利。随着计算机网络技术的发展和隐私权保护制度的完善,近年来,瑞典、美国、英国等许多国家和地区将个人数据明确为隐私权的对象,并对个人数据作了法律规定。隐私权一般包括个人私事、个人数据和个人领域三种基本形式。私人密码属于个人数据,具有隐私权的属性。公民对由其生成的包括私人密码在内的个人数据拥有专有权,并享有拒绝任何未经法律批准的监视、窥探及披露的权利。任何人非法利用计算机网络技术收集、存储、传播、使用包括私人密码在内的个人数据,均构成对他人隐私权的侵犯[1]。

4. 知识产权说

知识产权是指权利人对其所创造的智力劳动成果享有的财产权利。知识产权从本质上说是一种无形财产权,其客体是智力成果或知识产品,是智力劳动所创造的无形财产或者精神财富。密码作为一种数字、字母、图形的组合,是财产所有人不宜公开的智力成果,在某种程度上可视为一种特殊的知识产权。

5. 民事权利说

孙宪忠认为,将个人信息归到知识产权或隐私权都不合适。因为知识产权的一个显著特征是市场转让、市场开发,这与个人信息保护相悖;在传统观点看来,个人健康、疾病等信息属于隐私,可是在大数据时代,个人健康、疾病等信息在一定范围内共享,有利于患者得到更加及时、有效的治疗,由此看来,个人信息并不属于"隐私"。他还认为,应将个人信息保护独立出来,作为一项民事权利入法。这样做的目的在于一旦个人信息被滥用,受害者就可以从侵权法的角度维权[4]。

综合以上观点,笔者认为,电子密码是与财产权、人身权有关的电子数据,这种电子数据带有条件的特点,是公民享有财产权、人身权的重要组成部分。

二、电子密码的功能及其重要意义

(一)电子密码的功能

电子密码的主要功能是通过网络系统的辨认确认交易者身份及交易内容。具体体现在以下两方面:一是证明交易者身份。密码属于个人特有,因而能起到鉴别当事人的作用。例如在证券自动委托交易、银行卡交易中,除非本人泄露私人密码与他人,或者密码被破译窃取,一般情况下都有证明功能。二是对交易内容予以确认。在纸面交易中,双方通过书面签名或盖章的方式来确定交易内容。而在电子交易中,电子密码可代替传统的书面签名以保障交易各环节的稳定性、便捷性和高效性。

(二)电子密码的重要意义

首先,作为信息安全的核心,电子密码对维护网络信息安全具有重要作用。近年来,随着信息技术的蓬勃发展,人们对互联网的依赖程度越来越深。电子密码是用户进入网络社会、顺利完成交易及获取信息的必要前提。我们可以通过包括设置密码在内的技术手段提升个人信息安全

的保障能力,降低信息安全风险。

其次,电子密码有助于保护公民的隐私权。在信息时代,信任机制必不可少。只有建立信任机制,电子交易才能为人们提供隐私保障。作为信任机制中最为核心和根本的技术,密码能从根本上巩固网络信任机制,提升公民隐私保护的水平。

最后,电子密码的应用能促进电子交易的发展。电子交易改变了传统交易面对面的交流方式,而是采用网络联系的方式。由于互联网的开放性,电子交易各方都面临未知的安全风险,易让交易的参与各方对交易的安全性产生疑问,较难建立起相互信任的关系。因此,要维系电子交易的发展就必须确保电子交易中信息的真实有效性、完整性、可靠性、不可抵赖性和可鉴别性。密码的应用无疑是实现上述要求的最佳途径[5]。

三、我国对个人电子密码的法律保护

(一)目前我国个人电子密码保护的相关法律规定

对个人电子密码的法律保护,实质上就是对个人信息加以保护。保护个人信息可以通过制定相关法律条款来实现,具体分为直接保护和间接保护。所谓直接保护,即通过专门的个人信息立法进行规范。所谓间接保护,即通过宪法明确规定,刑法、民法、行政法等有关法律加以配合保护。除此以外,行业规范、信息持有人或控制人的承诺也具有一定的约束力。例如银行通过承诺,明确规定禁止随意泄露其掌握的个人信息。由于目前掌握个人信息的行业如金融、电信、房地产等行业还没有统一高效的个人信息管理规范,彼此缺乏协调,因此,我国个人信息保护的完善格局和模式尚未形成。

目前,我国法律法规、部门规章及其他规范性文件中涉及个人信息保护主要包括以下内容:

1. 宪法相关规定

我国宪法规定国家尊重和保护人权,保护人格尊严,从而间接地保护了公民对其私人空间的控制权[6]。因为个人电子密码具有隐私性,属于人格尊严的范畴,当然也是我国宪法的保护内容。

2. 法律相关规定

除宪法保护以外,我国已在不少法律中规定对密码所属的个人信息进行保护。非法泄漏、获取、传播个人电子密码并以此牟利,造成严重后果的,都应纳入刑法制裁的范围。追究针对公民个人信息的犯罪行为的刑事责任依据主要有:“非法侵入计算机信息系统罪”(刑法第 208 条)、“破坏计算机信息系统罪”(刑法第 286 条)、“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”(《刑法第七修正案》)等。

2017 年我国《民法总则》把隐私权作为一项独立的人格权加以保护,并专门规定对个人信息进行保护。《侵权责任法》也明确将隐私权作为一项公民权利进行立法保护。对个人隐私的保护,其中就应包含对个人电子密码的保护。

此外,《网络安全法》规定,网络运营者应当对其收集的用户信息严格保密,并建立健全用户

信息保护制度。《电子签名法》中也有对密码保护的相关规定:网络运营者应当按照网络安全等级保护制度的要求,履行安全保护义务,防止网络受到干扰、破坏或者未经授权的访问,防止网络数据泄露或者被窃取、篡改。该法还规定,提供电子认证服务,应当具备符合国家安全标准的技术和设备,具有国家密码管理机构同意使用密码的证明文件等,可见,使用密码是有严格控制条件的。

3. 行政法规、规章及其他规范性文件

涉及个人信息保护的法律规范性文件也有不少。如《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国电信条例》《互联网电子公告服务管理规定》等。有的地方也及时推进相关立法,如《深圳市互联网安全条例》。

在司法实践中,有关密码的纠纷呈上升趋势,法院在判决中越来越重视保护公民的密码及相关利益。据澎湃新闻网载,在对"北京市民付先生信用卡未离身却被境外盗刷1 400欧元"一案的审理中,法院认为,银行应保障储户的存款安全,包括储户的信息安全,防止储户密码等信息数据被轻易盗用。银行对储户资金支付安全的保障义务应扩展到对储户密码的保障。因此,由于银行卡系统存在安全隐患而导致的损失应由银行承担[7]。

(二)目前我国对个人电子密码保护之不足

从立法来看,我国目前的电子密码保护缺乏系统性、综合性立法,可操作性不强,规定极为分散、不成体系。法律法规之间缺少纵向的统筹和横向的协调。侵犯密码的行为一旦发生,常常有无人去管,或者争着去管的现象。从实践来看,参与密码管理的行政部门比较分散。公安部门、工商部门、工业与信息化部门、银行、证券公司、保险公司都有权管,但职责不清。而且,管理多以事后管理为主,缺少防范措施。由于现行法律中没有明确规定对密码犯罪的惩罚手段,那些病毒制造者、侵犯密码的违法犯罪分子往往逍遥法外。同时,由于缺少必要的问责机制,制裁主要针对个人而非企业、组织,起不到理想的警示作用。从司法实践来看,我国法院目前受理的侵犯个人电子密码类的侵权案件比较有限,对公民电子密码保护的实效有待提高。另外,从观念上看,传统观念往往更注重保护国家的信息和秘密,不太重视保护个人信息。

四、发达国家电子密码保护的比较法考察及相关经验

在当今信息社会中,包括电子密码在内的个人信息安全非常重要,各国对于公民个人信息安全的保护已经比较广泛,纷纷出台法律打击侵犯包括电子密码在内的个人信息的行为。由于各国历史、文化的差异,不同国家、地区对侵犯个人信息的具体规定存在一定的差异,不同国家、地区的个人信息保护法律也有不同的特点。有关个人信息保护的条文有的国家相对集中,另一些国家则比较分散;一些国家采取由刑法直接规定的方法,另一些国家则采用单独立法来保护个人信息安全。大陆法系国家一般倾向于设置非常细致的刑法条文。以德国为例,德国在法律中设置了非常集中的个人信息保护条款。《德国刑法典》对侵犯个人信息的行为确定了侵害信件秘密罪、探知安全数据罪、侵害私人秘密罪、使用他人秘密罪四个罪名:第202条a款规定了探知安

全数据罪,即行为人取得了确定不是行为人自己的数据和特别保存的数据时,就触犯了探知数据罪;第 203 条规定了侵害私人秘密罪,涉及特定主体侵犯公民个人信息的行为;第 204 条规定了使用他人秘密罪,即行为人使用应由特定人特别保护的秘密,如企业秘密或者商业秘密时,按本罪处罚。可见,个人数据、个人资料、秘密在德国都受刑法保护。英美法系国家一般通过制定单行法保护个人信息。以美国为例,《隐私权法》是保护个人隐私权的基本法。该法把政府机构工作人员作为侵犯隐私权的重要主体,凡是通过虚构身份骗取、非法披露个人信息,以及在保护公民个人信息方面渎职等都要接受制裁,旨在限制政府权力,以保护公民权利。除此之外,美国对隐私权保护的法律数量众多,如《公平信用报告法》《计算机欺诈和滥用法》《儿童在线隐私权保护法》等单行法律都涉及个人信息的保护。但美中不足的是法律规范之间缺乏有效协调,甚至常常发生冲突。

综观各国电子密码保护立法,一些发达国家和地区在个人电子密码的保护方面先行一步,其经验值得我国借鉴。

(一)制定密码标准

为推动商用密码产业形成,一些国家、国际组织纷纷开展或积极参与密码标准的制定工作,以此掌握密码技术的制高点和密码发展的话语权。美国于 1977 年公布了数据加密标准(DES),这被看作美国政府致力于密码技术标准化的开始。随后,美国国家标准技术研究院制定了密码技术的联邦信息处理标准(FIPS),要求在技术规范的前提下对密码产品进行严格的检验。美国在密码标准及其应用规范开发方面的探索对推动其国家信息安全建设及占领密码技术的国际市场起着不可估量的作用[8]。

(二)完善密码保护的法律法规

制定密码保护的法律法规是各国立法的大势所趋。全球密码保护的法律法规立法目前存在三种模式:

一是以欧盟为代表的统一立法模式。1995 年欧盟通过了有关数据保护的指令,旨在用指令中规定的最低标准来保证信息安全。2012 年欧盟对该指令作了修改。首先,把立法形式由指令提高为效力更高的条例,同时引入数据清除权和数据可携权,促进数据保护机构的改革和数据的跨境流通。20 世纪 90 年代,欧盟致力于建立欧洲范围内的可信第三方服务网络,其主要目的是建立公钥基础设施,同时解决密码恢复等合法访问加密信息的问题。1997 年“欧洲数字签名和加密框架意向”及“共同体市场准入的法律保护指令建议”出台,关注数字签名等加密认证功能的实现,认为数据加密是实现公众有效保护数据和通讯不受非法入侵的唯一有效便捷的方法。欧盟一直致力于在可信第三方密码托管、用户数据保护、密码恢复和隐私、高强度密码开发之间寻求平衡[9]。

二是以美国为代表的在移动互联网、云计算等新领域建立相关法规的模式。在美国,随着信息技术的普及,信息安全事件屡有发生。一个黑客截取并出版了 CD Universe 的客户资料(几千个信用卡号码)的事件就突显了网络安全的脆弱性[10]。基于公众对网络易受攻击的认识,强加密技术具有很大的市场。1996 年 5 月出台的《密钥管理基础设施》对政府和商业机构在密码恢

复上采用不同标准,以确保信息化进程中个人隐私、公众及国家安全。1996年10月,政府公布的BEP政策涉及密码使用和密码出口控制。该政策规定了政府和监管机构的责任。政府应扩大购买密码托管产品并促进服务创新。监管机构也应寻求促进民用密码托管的立法措施,包括释放密钥(泄密)的责任承担问题。1996年的《电子隐私法案》提出禁止强制性的密码恢复或密码托管。1997年,参议院曾举行听证会讨论加密、密码恢复和隐私权保护与进出口的相互制约关系,探询密码对确保出口贸易进行,加强隐私权保护,以及提高贸易自身的安全性的作用[11]。

三是以新加坡为代表的通过补充完善现有的法律法规来实现对信息的保护的模式。2013年1月,新加坡成立了个人资料保护委员会以贯彻实施2012年通过的《个人资料保护法令》,其目的是增加企业使用客户个人资料的透明度。

五、个人电子密码的保护建议

(一)加快个人电子密码立法保护,尽快形成统一的法律体系

个人信息保护既是互联网发展的基石,又是确保个人权利免受骚扰、实现社会安定的基础。党的十八届四中全会明确提出要加强互联网领域立法,加强网络安全保护,依法规范网络行为。我国的个人信息保护立法正在加快进行中。2016年出台的网络安全法就规范网络信息传播活动、完善公民个人信息保护制度作了明确规定,是我国个人信息立法的重大进展。2017年5月,最高人民法院、最高人民检察院发布了《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释》,明确把账号密码纳入个人信息的范畴。这些都表明了我国加强个人信息保护立法的决心。

但目前在个人信息保护立法的模式问题上尚有分歧。首先在名称上,有观点提出立的是“个人数据保护法”,也有观点提出立的是“个人信息保护法”;在体例上,有观点将个人信息保护与网络安全分立,也有观点将个人信息安全保护问题列入网络安全法范围。笔者认为,建立专门的个人信息保护法律制度是目前较为可行的立法路径。一方面,因为“个人信息安全”的范围有限;另一方面,个人信息还涉及其他权利,因此单独对个人信息进行立法能既保护公民个人的隐私权和与个人信息相关的财产权,又保护人身权。由于个人电子密码是信息安全的重要内容,在个人信息保护法中应设专章规定电子密码的保护。

在未来的个人信息保护法律体系中,宪法居于最高地位,其总体指导思想是对公民权利的保障,个人信息保护法是一部重要单行法。在这部法律中,应明确个人信息的概念、个人信息保护的立法宗旨、保护方法、侵害个人信息的类型和应承担的法律责任等。特别需要注意的是,作为个人信息保护重要内容的电子密码保护,应设专章规定。在立法时还需注意,个人电子密码本身就是科技发展的产物,对其保护立法必须关注信息技术的最新发展,不断研究技术发展带来的各种新问题,对收集、存储、处理、传播个人数据的新技术进行规范。同时,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。除了个人信息保护法这一单行法之外,其他相关立法(如对民法、刑法适当地修改,及时出台

司法解释)及行政立法都应及时跟进,打造一张严密的个人电子密码保护之网。

(二)加快密码的标准化和专利化

鉴于密码的技术性,管理部门、相关行业、专业机构应协调设计密码管理的技术标准规范。

首先要实现电子身份(EID)的标准化。电子身份是指在居民身份管理体系的基础上,经公安部门审核,由公安网络身份管理中心统一签发的网络电子身份证件,用于公民网络活动和真实身份管理。政府应制定相应的安全政策、密码标准,以严格规范数据信息交流,确保身份验证和识别的安全性。为了广泛应用在线服务,EID 管理系统必须具备可互操作性。为了实现互操作,就需要制定相应的技术标准以适应不同领域的身份证书[12]。

另外,在不侵犯国家秘密的前提下,可适当加快推动密码专利化步伐。我国《商用密码管理条例》规定:"商用密码技术属于国家秘密"。这意味着密码从研发到生产、销售、使用都实行专控管理,密码技术无法通过专利的方式进行保护。从事商用密码产品开发的科研人员所承担的保密义务与专利保护对技术公开的要求相冲突,实质上阻碍了商用人员积极性的发挥和技术的发展。将密码技术一概而论作为"国家秘密"加以保护实际上不符合密码标准化和专利化的趋势[8]。因此,对不涉及国家秘密的商用密码,应有条件地赋予密码技术研究人员申请和获得专利的权利,从而调动研究人员的积极性,促进密码技术的进步。

(三)建立统一的个人数据保护机构,提供维权、申诉等一站式服务

建立统一的个人数据保护机构,是保护个人信息(包括密码)的有效尝试。例如, 2015 年 12 月欧盟通过了数据保护新规定(GDPR),设立数据保护投诉的一站式监管机构,旨在简化流程,提高数据保护实效。

我国目前尚未建立专门的个人数据保护机构。全国人大代表、南京邮电大学校长杨震教授多次在全国两会上提案建议加快我国的信息安全立法,并呼吁成立负责个人数据保护的专门机构。从长远来看,建立专门机构有利于监督个人信息保护法的落地,提升个人数据保护水平,更有利于为消费者建立维权申诉的一站式服务[13]。各部门、机构、企业要为个人密码保护提供有力的技术支撑。网站的开发者有义务提供通俗易懂的隐私政策,在此政策指引下,在取得用户知情和明确授权后方可收集、处理和披露数据。网站运营者应告知用户拥有同意或拒绝修改、删除数据等权利。要明确加强移动 APP 技术保障,在 APP 设计和实施阶段进行隐私设计以确保安全。

同时,应当建立数据泄露通知制度,在一定时限内向受损主体发出公告。我国网络安全法规定,在发生或者可能发生个人信息泄露、毁损、丢失的情况时,应当立即采取补救措施,按照规定及时告知用户并向有关主管部门报告。这实际上也是一种有力的惩罚措施。发生数据泄露问题会对企业声誉产生不利影响,因通知而产生的高成本会倒逼企业提高信息保护的意识和能力。

(四)加强行业自律、加强网络空间治理

国外通过行业自律加强网络空间治理的经验值得我国学习和借鉴。例如,在美国,行业自律组织对个人隐私权保护起到重要作用。这类自律组织规定组织的成员必须承诺在网络隐私权保护方面发挥作用,遵守有关行为准则。在英国,行业组织和政府有关部门合作,共建有效的网络空间治理模式。其中,互联网观察基金会(IWF)被称为法律监管和行业自律相结合的典范。我

国在这一领域具有较大影响力的行业组织有中国通信企业协会、中国互联网协会、中国银行业协会、中国电子商务诚信联盟等。这些组织应学习国外经验,出台专门的密码保护措施,引导本行业提高密码保护意识。同时应加强宣传,向相关企业宣传密码保护的重要性,转变行业观念,更好地服务用户。

(五)对窃取、泄漏、传播密码的行为严格追究责任

对窃取、泄漏、传播密码等违法、犯罪行为如果缺乏严厉的追责机制,保护密码就会沦为空谈。发达国家对密码违法、犯罪行为的法律责任进行了明确规定。例如,新加坡《个人资料保护法令》授予委员会各种权力以执行法令,包括进入公司以获取与调查相关的信息、文件和设备;要求违反法令的企业遵守以下所有指示:停止收集、使用或披露已违反《个人资料保护法令》的个人资料;销毁已违反《个人资料保护法令》的个人资料;根据《个人资料保护法令》第28条第2款遵守委员会的任何指示,并且支付委员会认为合适的罚金[14]。

借鉴相关国家的立法经验,我国应在立法中加大对个人电子密码违法、犯罪行为的惩治力度。法律责任主要分以下几类:第一类是民事责任。2017通过的《中华人民共和国民法总则》明确规定了自然人的个人信息受法律保护,这是立法的重要进步。个人信息(包括密码)一旦被侵害,受害者可以要求追究侵权人的民事责任,如赔礼道歉、赔偿损失等。第二类是行政责任。我们应适时修改《治安管理处罚法》《行政处罚法》等法律的有关条款,增设对侵犯密码行为的行政处罚。其适用对象为违反相关行政法律法规、尚未触犯刑法的行为。行政处罚可采取行政拘留、罚款、没收非法所得等形式。要设定合理的罚款规则,保证合理的处罚力度,以威慑违法分子。第三类是刑事责任。这是相对而言最严厉的一类责任,我国目前的刑罚主要有罚金、管制、拘役、有期徒刑、无期徒刑、死刑等。而针对侵犯个人信息行为的刑罚主要是有期徒刑和罚金。例如,2017年5月,最高人民法院、最高人民检察院发布的《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释》规定,违法所得5 000元以上的,应当认定为刑法第253条之一规定的"情节严重",最高可判三年有期徒刑;情节特别严重的,如造成被害人死亡、重伤的最高可判七年有期徒刑,并处罚金。笔者认为,从立法来看,这些规定和以往这方面的立法空白相比已属进步,但力度有待加强。建议对情节特别严重的信息密码犯罪,如造成被害人死亡、重伤的则由现在的最高七年有期徒刑,并处罚金提高到无期徒刑、死刑等,这样才能更好地威慑犯罪分子、告慰受害者家属。

笔者同时建议,除个人以外,密码持有人(如政府机关、银行、保险公司、网络服务商等)泄漏、传播个人电子密码,造成对方人身财产损失,情节严重的,应追究密码持有人的刑事责任,视情节轻重对相关责任人处以适当的刑罚;另外,如网络入侵者(如黑客)破译、盗取密码,造成对方人身财产损失、甚至危及生命的,应追究网络入侵者的法律责任。除给予民事赔偿、行政处罚外,对窃取、泄漏、传播密码造成严重后果者应纳入刑法范畴。只有通过严厉的法律制裁,才能从根本上打击违法犯罪活动,保护人民群众的根本利益。

未来的社会是数据的社会,电子密码是数据社会的核心。只有重视并采取切实措施保护电子密码,才能顺应时代要求,体现依法治国的基本方略,促进社会安全、稳定、科学地发展。

参考文献:

[1] 孟勤国,刘生国. 私人密码在电子商务中的法律地位和作用[J]. 法学研究,2001(2):104 - 110.
[2] 王向阳. 试论存款合同中密码的法律性质[J]. 经济与社会发展,2003(12):117 - 118.
[3] 王泽鉴. 民法总则[M]. 北京:中国政法大学出版社,2001.
[4] 个人信息保护拟纳入民事权利[N]. 新京报,2016 - 11 - 01(A 08).
[5] 江智茹,冯立杨. 电子商务领域的密码法律理念与价值思考[J]. 政法学刊,2011(2):33 - 38.
[6] 胡雁云. 我国个人信息法律保护的模式选择与制度建构[J]. 中州学刊,2011(4):105 - 107.
[7] 赵崇强. 信用卡未离身被境外盗刷 1400 欧元,银行被判全责[EB/OL]. [2017 - 06 - 20]. http://www.thepaper.cn/newsDetail_forward_1399099.
[8] 冯立杨. 电子商务环境下的密码法律困境[J]. 信息网络安全,2009(4):14 - 16.
[9] 马民虎,原浩. 密钥托管与公民隐私权的国外立法[J]. 网络信息安全,2005(8):62 - 63.
[10] 陈欣新. 美俄商用密码法律监管制度比较[J]. 北方法学,2011(1):44 - 51.
[11] 金波. EID 网络身份管理[EB/OL]. [2017 - 07 - 11]. http://www.cio360.net/h/1784/366189 - 16071.html.
[12] 赵丽莉,江智茹,马民虎. 比利时电子身份管理制度评鉴[J]. 图书情报工作,2011(10):52 - 55,133.
[13] 王赟. 建议信息保护立法 设专门数据保护机构[N]. 扬子晚报,2014 - 03 - 12(A04).
[14] 新加坡的个人资料保护法令[EB/OL]. [2017 - 07 - 12]. http://opinion.caixin.com/2015 - 07 - 02/100824560.html.

(责任编辑:楼启炜)

On the legal protection of personal electronic code in China

ZHANG Qin

(School of Humanities and Social Sciences, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Personal electronic code is an important part of information security which involves personal privacy protection and is of great significance to transaction security. The author discusses the legal nature and functions of personal electronic code, analyzes the status quo in China and puts forward suggestions for the protection with consideration of relevant experience of developed countries. To protect citizens' personal information, China should speed up relevant personal electronic code protection legislation; speed up the pace of code standardization and patenting; establish unified personal data protection agencies to provide one-stop service of right protection and appeal filing; reinforce the self-discipline of businesses; and improve efforts to combat code stealing, leaking or dissemination.

Key words: personal electronic code; information safety; privacy; legal protection