私人密码在电子商务中的法律地位和作用

孟勤国　刘生国*

内容提要：私人密码在电子商务中是一个关键性的系统控制要素，其技术性和法律性应当受到同等的重视。私人密码具有私有性、唯一性和秘密性特点。应当设立私人密码一经使用即认为其进行了交易并应承担相应责任的原则，但应以软件密级程度过低、及时挂失或者系统遭黑客攻击为例外。在特定情形下，应适用公平责任。

关键词：电子商务　私人密码　法律责任

我们正在走进电子商务时代。事实上，我们早已习惯于信用卡存取款、证券自动委托交易以及其他种种利用计算机网络通讯技术而完成的自动交易。在现有的技术条件下，一方当事人通常通过其私人密码的设密和运用进入自动交易系统从而完成交易。由此经常引发关于私人密码的法律地位和作用的争议和纠纷。最简单的例子是，在人工自动取款机输入持卡人私人密码后取款，但持卡人既不承认取过款，也不承认泄露私人密码与他人，这样的纠纷应如何处理？现行法律对此没有规定，司法部门各有不同的理解。如广西仅存取款业务中就有此类纠纷上百起，涉及标的达数千万元。如何看待私人密码，几乎都是争议的焦点。因此，在理论及实践上研究私人密码在电子商务中的法律地位和作用，是当务之急。

一、私人密码的概念、特点及基本功能

（一）私人密码的概念

所谓私人密码，又称私人密钥，[1] 它是密码技术中与公共密钥相对应的一种密钥，它由本人生成并所有且只有本人知悉，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保密。

（二）私人密码的特点

私人密码有如下特点：

* 孟勤国，武汉大学法学院教授；刘生国，武汉大学法学院民商法博士研究生。

〔1〕 所谓钥，其实就是数字。例如当发送的信息为“1、2、3”时，在这些数字上加“3”，便变成“4、5、6”而发送出来。接收者对这“4、5、6”减以“3”便可得到原来的信息“1、2、3”。在这里，“3”便是钥。

1. 私有性。从理论上讲,私人密码属个人数据,[2] 而个人数据、个人私事和个人领域是构成隐私权的三种基本形式,[3] 故私人密码具有隐私权的属性。依此属性,公民对因其生成的包括私人密码在内的个人数据拥有无可争议的专有权,并享有拒绝、排斥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。

2. 唯一性。在自动交易系统中,私人密码结合其他要素如帐号,能够识别出交易者身份。以牡丹卡提款系统为例,本人在银行开立牡丹卡帐户后,其存款和取款都须输入本人在开立帐户时设定的密码才能进行;除非在自动交易系统中有修改密码的记录,根据存取款业务的事实可以肯定私人密码的使用,从而识别出存取款者即为本人或知晓本人密码的他人。

3. 秘密性。私人密码由本人生成且为其持有,除非本人泄密,他人不得知晓。实践中,一些法官和当事人常误以为私人密码能为交易对方如银行的操作人员所知晓,其实,在规范的自动交易系统中,私人密码不仅在操作员的电脑中看不出来,即使到中心机房,也无法查到。私人密码的技术价值就在于私人密码一旦设定和输入,非经复杂的破译程序不可再现。私人密码的数字在技术上破译不仅相当困难,而且往往因为破译时间可能需要几十年而不具有现实性。

(三)私人密码的功能

私人密码最初是为保密而设,但其在电子商务中的功能不限于此,正象有的学者所述:"加密技术为电于贸易提供了三个重要服务:鉴别(包括进行身份确认),不可否认行为确认以及秘密性。身份确认,是鉴别的一种,用来确认消息的发送者是否与他所声称的身份一致。鉴别,则更进了一层,它不仅仅确认消息发送人的身份,而且确认发送的消息是否被修改。不可否认行为确认在电子贸易中有很大需求,它能防止某些人否认他们曾经接收或发送过某些特殊性文件或数据。最后,秘密性是对未授权的访问进行拒绝。"[4] 具体说来,我们认为,私人密码在电子商务中有如下功能:

1. 私人密码的使用表明对交易者身份的鉴别及对交易内容的确认,从而起到数字签名(电子签名)[5] 的功能。

在传统的交易中,因其是直接或间接面对面的纸面上的交易,交易当事人就交易的内容商定后,可以书面签字或盖章。在通过计算机网络进行的电子交易中却很难做到,但"在现代技术下,要达到这一目的,并不是不可能。公钥加密技术和认证中心系统的产生已为我们妥善地

〔2〕 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,不少国家和地区将个人数据明确为隐私权的对象,并对个人数据作出了法律界定。如瑞典在 1973 年制定的《数据法》、美国在 1974 年颁布的《个人隐私法》、英国在 1984 年制定的《数据保护法》、1995 年通过的《欧洲联盟数据保护规章》对个人数据皆有明确的规定。以上资料参见汤啸天:《网络空间的个人数据与隐私权保护》,《政法论坛》2000 年第 1 期。

〔3〕 同上引,汤啸天文。

〔4〕 [美]Davi Ddosiur:《电子贸易》,陈曙浑等译,清华大学出版社 1998 年版,第 40 页。

〔5〕 据联合国国际贸易法委员会统一电子签名法规草案《UNCITRAL Draft Uniform Rules on Electronic Signatures》第一条(b)款规定,电子签名(Electronic Signature)是指一种电子形式的签署,这种签署或者是被包含在一个数据电文中,或者是附带于该数据电文,或者是同该数据电文有逻辑联系,而且该数据电文是被一个人或以该人的名义用来确定其身份,并且表明其对该数据电文所包含内容的认可。以上转引自陈凌:《电子商务若干法律问题研究》,载第二届中国信息化法制建设研讨会《电子商务立法论文集》,第 381 页。

解决当事人签名的独特性及当事人身份认证问题提供了技术上的可能。"[6] 这就是数字签名,其功能等同于书面签字,私人密码正是数字签名的基本方式,即通过加密技术而设定的包括私人密码在内的电子密码等数据电文,对交易者身份及对交易内容予以确认。首先,私人密码的使用证明了交易者身份。因为据密钥加密的原理可知"你是知道私人密钥的唯一人员,这样你在电子文件中使用私有密钥就如同你在纸上签名一样。"[7] 在应用私人密码的场合,因私人密码由本人生成并持有,只有本人知道,因此,能读出加密信息的只有他本人。由此起到了鉴别当事人身份的作用。例如在证券自动委托交易中,除非本人泄露私人密码与他人,他人不知交易密码。因此,凭私人密码打开交易帐号从事交易的,当然是本人从事了交易。其次,私人密码的使用表明对交易内容予以确认。在传统的纸面交易中,交易双方通过在书面上签名或盖章,确定交易内容,并预防抵赖行为的发生。电于商务同样要求交易的各个环节都是不可否认的,对交易的文件内容是不可被修改的。从这个意义上讲,私人密码的使用,即表明交易主体对交易内容的确认。

正因为私人密码在电子商务中起到以上所述鉴别交易主体身份及确认交易内容的作用,故在目前有关国家、地区及国际组织的立法中将包括私人密码在内的数据电文的使用视为一种数字签名。如联合国国际贸易法委员会于1996年6月通过的《电子商务示范法》第7条规定,如果数据电文的发端人使用了一种既可鉴定该人的身份,又表明该人认可了数据电文内容信息的方法,且从所有各种情况(包括任何相关协议)来看,他所用的方法是可靠的,对生成或传递电文的目的来说也是适当的,即满足了签字确认的要求。[8] 不过,"电子签名与传统的手书签名虽然都叫签名,但二者的差别非常大,甚至没有多少内在联系。此处只是借传统签名对签署人的辨认功能,来指称在电子商务中对交易人进行识别的电子鉴别手段。"[9]

2. 私人密码的使用表明本人进行了交易行为。

由电于商务的特点所决定,在交易中,信息发送和接收者都不能对此予以否认,即电子商务行为的"不可抵赖"性,这就要求系统具备审查能力,以使交易一方不能抵赖已发生的交易行为。从这个角度讲,私人密码的使用是审查当事人是否从事交易行为的有效手段,就是说,凡是使用私人密码从事的交易即为本人进行了交易行为,本人不得抵赖,不得否认曾经接收或发送某些特殊的文件或数据。

3. 私人密码的使用表明交易是在保密状态下进行的,任何第三者都不知交易内容。

电子商务是在一个较为开放的网络环境中进行,因此如何保障信息的保密性、安全性是电子商务中的一个重要课题。就安全手段来说,私人密码可以说是目前较为重要的安全手段之一。因私人密码由私人生成并由私人专用,除非本人泄密,他人不得知晓,故私人密码的使用表明本人是在保密状态下使用。

〔6〕 黎希宁、梅绍祖:《电子商务网上合同的合同形式问题》,载第二届中国信息化法制建设研讨会《电子商务立法论文集》,第58页。

〔7〕 前引〔4〕,[美]DAVID DOSIUR 书,第43页。

〔8〕 参见姚立新:《新世纪商务》,中国发展出版社1999年9月版,第269页。

〔9〕 张楚:《美国电子商务法评析》,《法律科学》2000年第2期。

二、私人密码的使用效力规则

(一)私人密码使用即为本人行为的原则(以下简称本人行为原则)

所谓本人行为原则,是指只要客观上在交易中使用了私人密码,如无免责事由,则视为交易者本人使用私人密码从事了交易行为,本人对此交易应承担相应的责任。

确立以上原则的理由在于:

1.这是由私人密码的性质和特点所决定。

私人密码的使用,只能是本人或者知晓私人密码的人。实践中,在本人不承认使用私人密码同时声称不曾泄露过私人密码而私人密码已被使用时,经常有法官要求交易对方如银行举证证明本人使用了私人密码,或者以开户申请书不是本人填写为由,撇开本人是否使用或泄露私人密码。这是对私人密码缺乏了解的缘故。私人密码由本人生成而且在保密状态下由本人持有和使用,如果不是本人的原因,他人从何处得知?这是一个不容忽略而且必须由本人予以合理说明的关键问题。本人或许有意无意地将私人密码告知了他人,或许在操作时不注意防范为他人窥视了私人密码,甚至可能就是自己使用了私人密码,不论是哪一种情况,是本人的行为所致,与交易对方无关,因而应由本人承担私人密码使用的责任。

2.现代社会的经济生活和社会生活需要这一原则。

当前,以计算机网络为核心的信息技术的迅猛发展和因特网的迅速普及,极大地改变了人类数千年的传统生活方式。电子商务作为全球经济一体化背景下的一种全新的商业机制,以高效率、无疆界、无时限和低成本等特点获得迅速发展,将成为21世纪初全球经济最大增长点之一。电子商务是通过数据电文而进行的无纸化交易,在这种交易下,如何鉴别交易者身份,如何确认交易内容以及如何对交易的内容进行保密等是电子商务发展中的重要问题。而包括私人密码在内的电子密码在电子商务中的应用,可以说是目前解决以上问题的有效办法。事实上,在有电子商务的领域,必有包括私人密码在内的电子密码的应用。就目前的技术条件而言,没有包括私人密码在内的电子密码的应用,电子商务无从谈起。然而,使用私人密码必须有一定的规则,否则电于商务的"游戏"就无法进行,这个规则首先是使用私人密码即为本人行为。不然,谁都可以凭私人密码在自动取款机取款或凭私人密码从事证券委托交易后矢口抵赖,电子商务根本不可能开展。

3.现有技术完全可以做到其安全性超过传统交易方式。

在传统的纸面交易中,双方当事人的认证是通过书面签字来完成的。当事人对签字而生的后果承担法律责任。当事人签字后即应对所签内容负责的理由在于签字意味着当事人对交易主体及交易内容的确认,那么通过私人密码等数据电文的形式而完成的数字签字,同样达到书面签字的认证功能。通过私人密码完成的数字签名只要能做到:(1)除收发双方外别人无法知道信息内容(隐私性);(2)信息在传输过程中不被篡改(真实性);(3)发送方能确信接收方不是假冒的(非伪装性);(4)发送方无法否认自己的发送行为(不可否认性)等安全要求,当事人当然应对其通过私人密码认证后的交易承担责任。从目前的情况看,为保证以上安全要求,在技术上主要采用两类技术手段,"一种是为防止数据(信息)被盗窃篡改而使用的加密技术。另

一是用以确认正在打交道者确实是本人的认证技术。"[10] 这些技术从理论上说均有严密的体系,具有较强的保密及认证功能,从实践应用来看,已起到保护交易安全的功能。故通过私人密码而完成的数字签名意味着同书面签字一样,完成了认证功能,因而通过私人密码的数字签字,本人亦应对此承担责任。

(二)私人密码使用即为本人行为原则的例外

私人密码的使用,原则上视为本人行为,本人应对此行为负责,但在下列情形下,该原则不予适用。

1.私人密码使用涉及的软件密级程度过低。

适用私人密码使用即为本人行为原则的基础之一,是私人密码使用所涉及的软件秘级达到足够安全的程度。如软件的密级程度过低,他人可轻易破译私人密码,则无私人密码的私有性、唯一性、秘密性可言。在此情形下,如仍适用私人密码使用即为本人行为原则,对本人极为不利不公。

2.失窃、失密后及时向交易对方挂失。

本人当对自己的私人密码妥加保管,如发生私人密码失窃、失密,应从速向交易对方挂失。在本人办理了挂失手续之后,有人仍凭此私人密码从事交易,此种情形,不适用为本人行为原则。因本人已履行了自己应尽的挂失义务,他人所以能凭此密码从事交易,是由于交易对方的过失所致。

3.操作系统受到黑客攻击。

操作系统受到黑客攻击作为本人行为原则例外的情况是指,操作系统的软件密级程度达到相关标准,且本人无过错的情况下,操作系统受到黑客攻击,致使黑客获取私人密码并从事交易的情形。在此情形下,不适用本人行为原则。因交易双方均无过错,故对本人所造成的损失应按公平责任原则由交易双方分担。

三、私人密码使用的风险防范与法律责任

(一)风险防范

在现有条件下使用私人密码从事交易,原则上说是可以保证交易安全的。但因私人密码毕竟是在开放性的网络中使用,这样,在使用中仍有一些风险隐患,这就须有更强的防范意识、得力的防范措施,防止和减少不必要的使用私人密码的风险损失。

1.本人管好自己的私人密码。

依私人密码使用的效力规则,只要客观上在交易中使用了私人密码,如无免责事由,则视为本人使用私人密码从事了交易行为,本人对此交易应承担相应的法律责任。依此效力规则,如本人对私人密码保管不善,造成私人密码失窃或失密,并且有人在本人挂失之前已从事了交易,对交易的相对方而言,这也是本人的行为,本人应承担相应的法律责任。故本人应对其私人密码严加保管,以防失窃失密。

2.操作系统的设计和使用应严格分开。

私人密码不仅对任何第三人是保密的,而且对经营使用和设计该操作系统的有关方也应

〔10〕 参见陈幼松:《数字化浪潮》,中国青年出版社1999年版,第199页以下。

是保密的。现实中经常有经营使用者与设计者关系密切的情形。因设计者对操作系统十分熟悉,有可能破译私人密码,对私人密码的保密大为不利,因为这里不能排除操作人员和设计人员相互串通的可能。故在实践中,操作系统的设计和使用应当严格分开,做到使用者不知是谁设计,设计者不知是谁使用,如银行系统,应由总行甚至由人民银行总行在严格保密的状态下委托设计操作系统软件,下发各行和分支机构使用,以确保私人密码的保密性、安全性。

3.在有条件的地方设立认证中心。

认证中心是指在电子交易中作为中介人,保管公共密钥,证实某一公共密钥确实是某一当事人的,从而保证交易的对象是真实的。私人密码要结合公共密钥才能进入交易,管好公共密钥对私人密码的安全使用有积极的作用。在颁布了有关数字签名法律的国家中,通常对认证中心也进行相应的规范。如德国、日本、美国各州、加拿大等许多国家颁布了各自的有关数字签名的法律,也同时对认证中心的作用及公共密钥的管理作出了相应的规定。我国目前存在的问题是对认证中心的设立和密钥管理没有统一的政策进行指导,导致各个机构、各个行业建立自己的认证中心,重复建设,管理混乱,从而不利于长远发展,也不利于安全保密。[11] 因此,我们建议,我国也应着手制定这方面的法律、法规,在有条件的地方,设立统一的认证中心,对公共密钥进行统一管理。

4.操作系统达到一定的密级程度。

电子商务是通过数据电文的传输来完成的无纸化交易,为保障交易的安全,加密技术得以应用。从某种意义上,电子商务之所以得以发展,实赖于加密技术的应用。但在交易中如操作系统没有达到一定的秘级程度,纵使交易者自己设密,也可能因操作系统的密级过低,致使私人密码被他人破译。因此,为防范私人密码的使用风险,操作系统须达到一定的密级程度。具体需达到何种密级程度,应借鉴电于商务发达国家的有关规定及考虑我国电子商务发展的实际情况,由国家作出统一规定。

(二)举证责任

此处所说的举证责任是指私人密码的使用者及其相对方对私人密码的使用主张不承担责任或主张应由相对方承担责任,需举证证明。

1.交易一方如要本人对私人密码的使用承担责任,需证明:

(1)操作系统是符合保密安全等级的。操作系统密级程度过低,私人密码容易被破译,此情形不适用本人行为原则的效力规则。故交易一方如银行需证明其操作系统是符合保密秘级程度要求的,从而排除本人主张适用效力规则例外的可能。

(2)交易一方如银行只须证明交易是凭私人密码完成的,至于私人密码是否为本人使用,不负举证责任。因据本人行为原则,只要客观上使用私人密码即可,私人密码是本人委托,出借、转让他人使用,抑或是在失窃、失密挂失前被他人使用,对交易一方如银行而言,在所不问。

2.本人主张其对私人密码的使用不承担责任,需证明:

(1)证明泄露密码后已向交易对方挂失,如私人密码失窃、失秘挂失后,有人仍凭私人密码从事交易,则交易对方具有过错,故交易对方应对此承担相应的责任。当然,如有人在本人挂失前已从事交易,则当然适用本人行为原则。

(2)证明操作系统被他人破译。因为若操作系统的密级过低,致私人密码被破译并从事交

〔11〕 参见唐应茂:《认证中心的作用和公共密钥的管理》,《金融法苑》1998 年第 10 期。

易,本人可主张不适用本人行为原则。若操作系统是在符合有关保密秘级程度的情况下被破译,处理上虽不适用本人行为原则,但据公平责任原则,本人亦应承担一定的损失。

(三)法律责任

私人密码作为一种交易控制的关键要素,通过其应用,可达到对交易者身份鉴别及对交易内容予以确认等目的,最终促成交易的完成。交易完成必生一定法律后果。现就私人密码使用的法律责任承担分以下情形说明。

1.使用私人密码由本人承担责任的原则。这一原则其实是本人行为原则的必然结果,因按本人行为原则,凡使用私人密码从事交易,即视为本人从事交易,那么本人对本人行为承担责任则理所当然。

2.私人密码是由操作系统秘级过低而被破译,并依其从事交易,或私人密码失窃、失密挂失后从事的交易,则不适用本人行为原则。对此所生之后果,应由交易相对方如银行承担相应的法律责任。

3.操作系统的秘级程度虽达到要求的标准,但私人密码仍被破译,并依此从事交易。对此情形,因交易双方对损失的造成均无过错,应适用公平责任原则,在考虑双方当事人的财产状况及其他情况的基础上,由双方共同分担损失,经济实力强的当事人应当适当多承担一些损失。道理很简单,电子商务是现代社会带来的文明成果,我们每个人既然都在享受现代文明的利益,理所当然应承担一定的风险责任。如果有谁不愿为此承担丝毫的风险,只能选择不涉足电子商务。

Abstract: PIN is a key element for systematic control in electronic commerce. Its technical aspect, as well as legal aspect, shall be emphasized equally. PIN is characterized with privacy, uniqueness and confidence. A rule that assumption responsibility as long as a PIN is used should be established, with exceptions of too low degree safeguard of the software, prompt report of loss and heckler's attack. In certain conditions, the principle of equality shall be applied.