# 大数据时代网上银行的安全保障义务研究

李 晗*

内容提要：大数据时代，数据被收集、分析，成为决策判断的基础，数据的价值不可估量，用户的信息和资金均以数据的形式存储在网上银行，一旦被非法窃取，将对用户信息和交易安全带来巨大的损失，因而，网上银行安全保障义务的核心内容主要是信息安全和交易安全；完善信息安全保障义务，设定最低信息安全技术标准是最基本的途径。规定网上银行对用户信息的使用规则，可以防止网上银行滥用用户信息。明确网上银行承担的责任能够防止网上银行将信息安全保障义务转移到用户身上；完善交易安全保障义务，保护交易安全，首先应保障电子合同的安全。采用有效的认证方式是保障交易安全的必要防线。区分经授权和未经授权电子资金划拨，能够减轻用户资金损失的风险。

关键词：大数据时代；网上银行；信息安全保障义务；交易安全保障义务

## 一、大数据时代网上银行安全保障义务转变的动因和核心内容

### （一）网上银行安全保障义务转变的动因

传统银行的安全保障义务内容主要是银行场所安全（包括柜台和 ATM）、用户的资金安全和一定的信息安全。网上银行的基本功能是为用户提供查询、转账、在线支付费用、理财等服务，用户的资金安全和交易安全仍然是网上银行非常重要的义务。但是在大数据时代，信息安全面临着前所未有的挑战，用户信息安全具有和用户资金安全同等重要的地位，这主要是由大数据的特点决定的。首先，大数据来源广泛。网络时代，大量数据存储于社交网络、电子邮件等媒介中，数据的集中存储增加了数据泄露的风险，而且目前法律并没有对数据的所有权进行明确的规定；其次，大数据带来更多的安全挑战。大量的数据集中存储，导致常规的安全防护措施无法跟上数据非线性增长的速度，无法满足日益增长的安全需求；最后，大数据技术易被滥用。由于数据挖掘技术和数据分析技术的发展和共享，网上银行在利用这些大数据技术提升自身保护能力的同时，黑客也可以利用这些大数据技术对网上银行进行攻击，且攻击将变得更加的精准。因而，在大数据时代，网上银行安全保障义务的核心内容从着重保障用户资金和交易安全，转变为用户信息安全和交易安全保障并重。

### （二）网上银行安全保障义务的核心内容

* 北京工商大学法学院副教授，法学博士。本文系 2015 年国家社科基金项目“大数据时代网上银行的安全保障义务研究”（15CFX049）的阶段性成果。

信息安全是指保障用户信息的保密性、完整性、可控性和不可否认性。在 PC 互联网时代,[1] 用户对自己的信息还有一定的控制权,但在大数据时代,散落在各个门户网站和社交网站上的个人信息都可能通过一定的相关物匹配和识别出来,个人的安全面临着空前的挑战。[2] 在数据关联紧密的大数据时代,网上银行也没有例外,网上银行在依赖互联网提供服务和产品的同时,大量的信息和资金均以数据的形式通过网络和设备进行存储和传输,网上银行的安全与否往往取决于这些数据在互联网传输的安全性。网上银行信息安全面临着更大的风险。因此,网上银行安全保障义务的实现首先就需要保证信息安全系统和数据信息不被侵害。

交易安全是指保障用户资金不被窃取、交易过程不受监控、交易信息不被泄露。网上银行电子交易具有数字化、虚拟化的特点,电子交易的安全依托于网上银行防火墙、身份认证系统和加密技术等电子技术的支撑,由于现有的科技技术的有限性和大数据时代风险的无限性,网上银行交易安全面临着重大风险。同时,作为追求利润的金融机构,网上银行也不会忽视大数据时代带来的巨大商业价值,目前国内各大银行已经开始建立数据库,利用数据挖掘技术分析用户的交易行为,以更有针对性地提供服务,但这很容易会侵害用户的资金和交易安全。因此,网上银行安全保障义务的另一个核心内容就是交易安全保障义务。

## 二、大数据时代网上银行安全保障义务面临的主要问题

### (一) 信息安全保障义务面临的主要问题

#### 1. 未设定网上银行信息安全存储和安全传输技术标准

网上银行与传统银行最大的不同就是,网上银行是依赖计算机网络生存,网上银行高度依赖包括互联网在内的信息技术,因此采用各种安全技术手段是实现网上银行安全保障义务最基本和最有效的途径。目前国内各大银行顺应信息化、数据化时代的潮流,纷纷提升自身的安全技术,比如工商银行网上银行采用中国金融认证中心(CFCA)提供的、目前最严密的 1024 位证书认证和 128 位 SSL 加密的公钥证书安全体系;北京银行网上银行将云计算技术与环境准入、桌面管理、数据加密等技术相结合,构建信息安全体系。虽然这些安全技术能在一定程度上实现信息安全保障义务,[3] 但仅仅由网上银行来决定应该采取什么样的安全防护措施,是远远不够的,还必须由法律为网上银行设置强制性的最低安全存储和安全传输技术标准,以强制网上银行采用足够的安全保障技术。各国及国际组织都纷纷制定相关的法律对网上银行应该采取的加密方法、电子签名技术等进行了规定,以形成信息系统安全的统一的最低技术标准。[4] 如 2008 年 1 月 1 日,德国相关法律规定国内所有的网上银行统一执行技术标准 EBICS,以保障所有网络传输交易信号的安全。[5] 而我国《电子银行业务管理办法》,对于网上银行的系统设施、加密技术等的标

〔1〕互联网的发展有三个阶段:PC 互联网时代、移动互联网时代和万物互联网时代。PC 互联网时代是指互联网产生初期,电脑之间的连接,这一时期网上银行的安全可以通过防病毒、防火墙进行防御。移动互联网时代是指手机等移动设备之间的连接,这种连接打破了对网络边界的定义,手机和个人隐私信息联系在一起,网上银行安全的问题变得更加严重。万物互联网时代是云计算技术和大数据分析技术发展的产物,即将一切还未联接起来的人、数据、流程和万事万物都联接起来。这种连接方式使得人与人之间的边界更加模糊和融合,网上银行存储的数据安全面临着巨大的风险。

〔2〕大数据的核心就是预测,以一种前所未有的方式,通过对海量数据进行分析,获得有巨大价值的产品和服务。大数据时代,个人安全面临的危险不再是隐私的泄露,而是被预知的可能性。

〔3〕网上银行中的信息技术通常会产生或者增加操作风险。一,外部风险。电子银行的身份认证技术、访问限制系统、认证机构的可靠性等都很有可能会遭到外来攻击;二,网上银行本身系统设置、实施和维护风险。网上银行安全系统可能会技术缺陷或者没有及时更新无法提供的完善服务。

〔4〕李德 《经济全球化中的银行监管研究》,中国金融出版社 2002 年版,第 133 页。

〔5〕余素梅 《网上银行业务安全的法律保障机制研究》,武汉大学出版社 2006 年版,第 47 页。

准均只规定为“合适”，如第38条规定“金融机构应采用适当的加密技术和措施，保证电子交易数据传输的安全性与保密性”；第40条规定“金融机构应采取适当的措施和采用适当的技术，识别与验证使用电子银行服务客户的真实、有效身份”；《电子银行安全评估指引》规定了对电子银行进行安全评估的具体内容，但是没有规定评估依据的安全标准，仅规定“电子银行安全评估应真实、全面地评价电子银行系统的安全性”。由此可以看出，我国对于网上银行安全技术的规定过于笼统和原则，缺乏明确的最低安全技术标准。

2. 缺乏网上银行的信息使用规则

在大数据时代，采集的大部分数据都包含个人信息，而个人信息作为数据的价值不仅仅来源于提供基本信息，更是来源于二次利用，商业公司通过收集个人的各种信息，来还原一个人的相貌、喜好、情绪和购买意向等，实现更精准的营销。〔6〕银行作为商业金融的一部分，自然也追求个人数据的最大利用。网上银行由于天然的便利条件，存储有用户属性信息、用户行为信息、用户交易信息等隐藏着用户需求和潜在业务机会的数据。对于这些信息，目前国内的网上银行已经开始使用一些大数据应用工具进行数据挖掘，分析用户情绪、预测用户行为。在这种情况下，网上银行面对存储的海量用户数据，很有可能出于追求精准营销等营业目的，滥用用户信息，而这也将导致网上银行信息安全保障义务难以实现。因此，如何规定网上银行对用户信息的使用规则，限定网上银行对用户信息的使用范围和方式，明确信息泄露后应承担的后果，以保证用户享有知情权、选择权，平等交换和授权使用的权利，关系到信息安全保障义务的实现，但我国《电子银行业务管理办法》等相关法律法规，并没有对网上银行的信息使用规则进行规定。

3. 未规定网上银行的附随义务及责任承担

在大数据时代，数据的价值很大一部分体现在二级用途上，即利用数据进行再分析和再预测。〔7〕由于企业往往是在收集数据之后才意识到数据再分析和再利用的价值，那么规定限制企业对用户信息的滥用，并不能很好地保护用户的个人信息安全。因此，保护网上银行用户信息安全，重点不应只是设定“告知与许可”的信息使用规则，更应确定网上银行承担的责任，使得网上银行为了避免承担相应的责任，不得不对用户信息的收集和保护进行进一步的优化。因此，必须对网上银行在信息安全保障义务中应承担的义务和责任进行明确规定，以实现对用户信息安全的充分保障。我国《电子银行业务管理办法》规定了电子银行应采用适当加密技术、身份认证技术，并负有签订电子合同的义务，但没有规定网上银行审慎审查用户身份、限制储存个人信息时间和帮助追查、追偿等附随义务。〔8〕该法第89条规定“金融机构在提供电子银行服务时，因电子银行系统存在安全隐患、金融机构内部违规操作和其他非客户原因等造成损失的，金融机构应当承担相应责任。”也并没有对网上银行未合理履行信息安全保障义务应承担怎样的责任、如何承担责任进行细致规定。

（二）交易安全保障义务面临的主要问题

1. 电子合同规定不完善

真正意义上的电子合同是将合同信息或者数据记录储存在计算机内存或者硬盘等中介载体的

〔6〕精准营销分为两种，一种是基于社会属性的营销，社会属性即性别、年龄、收入状况等；第二种是基于兴趣、行为的营销。精准营销的前提是获得用户的信息，对于精准营销和用户隐私权保护之间的关系，维克托·迈尔·舍恩伯格认为精准营销获取的数据同时包括用户的社会属性信息和兴趣、行为信息，无法保证企业会严格区分这两种信息，不利用行为信息去匹配用户的社会属性信息，从而侵犯用户的隐私安全。因而精准营销必须满足用户的知情权和选择权：一，网站必须事先告知数据采集的范围、方式、用途；二，严格区分用户的社会属性信息和行为信息；三，网站需保证用户有拒绝网站继续收集、使用其信息的权利；四，网站在将用户信息提供给第三方时，必须经用户同意。

〔7〕车品觉 《决战大数据》，浙江人民出版社2014年版，第110页。

〔8〕王华庆 《网上银行风险监管原理与实务》，中国金融出版社2003年版，第203页。

合同形式，其虽然不是以书面形式订立，但仍然属于合同的范畴，具有确定双方权利义务的功能。从法律意义上说，交易的主要形式和载体就是合同，网上银行交易和传统交易活动一样，强调对交易安全的保护，实际上也是要求保护交易合同的安全。目前，我国网上银行制定的电子合同存在以下几种问题:

(1) 电子合同的格式合同属性容易侵害用户权益

如今电子合同主要有三种形式，EDI 合同、电子邮件合同和点击许可合同，[9] 网上银行通常采用的是点击许可合同，该合同实质上是格式合同，网上银行事先拟制好相关条款，放置在网上银行页面上。一方面，用户只能选择同意或者不同意，没有协商、更改的权利，甚至在一些情况下没有拒绝的权利; 另一方面，电子合同往往繁杂、冗长，缺乏明确的提示，大多数用户不仔细阅读就直接选择同意，使得一些不利于用户的条款被用户忽视，导致发生纠纷时，用户权益得不到保障。

(2) 电子合同在签订过程中容易发生错误

电子合同错误有两种原因: 其一，用户之外的第三人假借用户身份与网上银行签订电子合同。由于网上银行交易省略了交易双方当面交流环节，这种交易方式增加了交易的匿名性，导致交易双方的身份、资格都无法得到有效确定。尤其在大数据时代，个人数据存储在各种服务器上，留心收集、分析便可以获得一个人的各种信息，很容易出现用户被冒名现象，造成用户损失; 其二，电子传输系统迅速、即时导致用户无法更改信息。由于电子合同签订具有即时性，一经点击或者发出即成立，用户出现错误也无法得到更改，造成用户损失。[10] 对于这两种电子合同情形，我国《电子签名法》仅对电子合同的书面形式、原件、保存和证据要求等作了规定，并没有规定电子交易服务方的义务和双方的责任分担。[11] 而且我国的相关电子银行监管法律中，对于第一种电子合同错误情形，没有规定网上银行应采用的身份认证和电子签名技术的标准，也没有规定网上银行审慎审查、帮助追查义务和双方责任分配。对于第二种情形，虽然是用户自身错误导致，但是由于互联网交易的特殊性以及用户处于弱势地位，法律没有对用户应承担的责任进行明确限定，以防止出现网上银行误导用户，发生损害用户权益的现象。

2. 电子签名“技术中立”的立法模式存在缺陷

网上银行由于虚拟化、数字化、信息化等特点，省略了交易双方面对面交流的环节，传统的签名、盖章的认证形式无法再适用，网上银行的身份认证环节更有难度，也更有风险，采用有效的方式确认交易双方的身份、资格等成为网上银行交易安全保障义务的重要内容。目前，广泛适用的方式是电子签名，其可以在很大程度上鉴别交易双方的身份，确认双方认可合同的内容，保障网上银行交易的安全，因此各国非常重视创设电子签名法律制度。我国的《电子签名法》也对电子签名制度进行法律规制，包括数据电文的法律地位、证据效力和原件效力、电子签名的有效条件和电子签名人的义务等。但该法第 14 条的规定表明我国采用的是严格的“技术中立模式”，即认可电子签名存在多种技术手段，对于应该采用哪种技术手段，立法者不作出具体选择，交由市场去选择。“技术中立模式”虽然有利于鼓励电子签名技术的发展，也能够鼓励网上

---

〔9〕EDI 即电子数据交换，最早应用于美国运输业，EDI 合同订立和履行的整个过程都是通过计算机自动处理，无需书面单证的人工传递。其优点是降低交易成本，提高效率。缺点是传递和存储的数据容易被剽窃与破坏; 电子邮件合同是当事人通过电子邮件进行要约和承诺，其优点是快速、经济，缺点是电子邮件在传送过程中容易被截获、修改，安全性不高; 点击许可合同主要应用于企业对消费者的交易模式中，企业在网络公共交易平台上放置交易条件，用户若同意交易条件，点击“确认”后合同就成立。优点是标准化、迅捷化。缺点是这种合同形式其实是格式合同，企业通常会加大用户责任，减少自身义务，而且由于点击许可合同往往冗长、繁琐，用户多不会仔细阅读，用户权益很容易受到侵害。网上银行通常采用的就是点击许可合同。

〔10〕吴宏、丁广:《合同法视野下的金融机构安全保障义务》，《人民司法》2009 年第 3 期，第 67 页。

〔11〕高晋康、唐清利《商业银行运行中的法律漏洞及其弥补》，法律出版社 2010 年版，第 125 页。

银行发挥自主性，选择更适合自身的电子签名技术，但如果将电子签名技术的选择权完全交由网上银行，那么很可能出现网上银行为了降低成本，延缓更新电子签名技术，造成用户交易安全受损。从国际社会的立法趋势来看，“技术中立”与“技术特定”相结合的立法模式更有优势。[12]

3. 未区分电子支付情形

电子支付是网上银行的重要业务之一，其各种支付方式均是通过数字化方式，具有快捷、高效和经济的优势，但是电子支付也面临着用户之外的第三人未经用户授权而从用户账户中划拨资金，造成用户损失的风险。在现实生活中，未经授权划拨原因包括网上银行安全技术落后、职员玩忽职守、用户自身过失泄露账户密码、第三方盗用账户密码。未经授权的划拨将影响到用户的资金安全和网上银行、用户的责任承担问题。但是我国现有的网上电子支付法律，如《电子支付指引（第一号）》中，并没有区分经授权和未经授权的电子资金划拨。

美国《电子资金划拨法》规定了未经授权电子资金划拨情形中消费者承担责任的条件以及责任承担的三个等级，同时规定了金融机构的责任承担情形，避免金融机构利用优势地位逃避责任承担。[13] 我国的《中国银行股份有限公司信用卡领用合约》中的密码条款规定“凡使用密码进行的交易均视为持卡人本人所为并由持卡人承担交易后果。银行卡遗失、被窃，或被他人占有时持卡人应当及时办理挂失手续，挂失自正式挂失手续办理完毕时生效，持卡人对挂失生效前发生的交易承担责任，对挂失生效后发生的交易不承担责任。”《电子银行业务管理办法》第89条规定“金融机构在提供电子银行服务时，因电子银行系统存在安全隐患、金融机构内部违规操作和其他非客户原因等造成损失的，金融机构应当承担相应责任。因客户有意泄漏交易密码，或者未按照服务协议尽到应尽的安全防范与保密义务造成损失的，金融机构可以根据服务协议的约定免于承担相应责任。”虽然该法完善了上述密码条款，但由于《电子银行业务管理办法》属于部门规章，在司法实践中，法院不能直接援引《管理办法》。[14] 因此由于缺乏明确的法律规定，我国的网上银行往往在格式合同中将未经授权电子资金划拨的风险损失分配给用户，排除自身责任。

## 三、网上银行信息安全保障义务完善途径

### （一）规定信息安全存储和安全传输的最低技术标准

2012年中国人民银行发布了《网上银行系统信息安全通用规范》，从技术、管理和业务方面提出了有针对性的安全要求，但该规范并没有涉及到数据存储安全性和完整性的技术要求，因此在完善法律时可以参照公安部颁布的《信息安全技术 信息系统通用安全技术要求》（GB/T20271－2006）、《信息安全技术 网络基础安全技术要求》（GB/T20270－2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272－2006）等技术标准，从数据完整性和数据保密性方面确定网上银行信息安全存储和传输最低技术标准：第一，信息完整性保护技术标准。信息存储中，安全技术须在读取数据时进行完整性监测，及时监测到泄露可能性，进行及时的恢复。信息传输中，

〔12〕“技术中立”模式：立法者确立电子签名技术的中立地位，对技术手段只提出原则性要求，具体的选择和使用交由市场和消费者自己去判断。采取这一种立法模式的国家有美国、澳大利亚、新西兰等 “技术特定”模式：立法者确定以非对称加密技术为基础的数字签名为合法的电子签名技术，规定认证机构的技术和财务等条件要求。采取这一立法模式的国家有德国、丹麦、韩国等 “技术折中”模式：即“技术中立”与“技术特定”相结合，立法者一方面设定电子签名技术的最低限度要求，另一方面对一些电子签名技术赋予更大的法律效力，对电子签名技术的选择作出法律指引。采用这一立法模式的有联合国《电子签名示范法》、我国台湾地区等。

〔13〕李适时《各国电子商务法》，中国法制出版社2003年版，第162页。

〔14〕刘颖《电子资金划拨法律问题研究》，法律出版社2001年版，第25页。

安全技术须进行完整性监测，及时发现被篡改、删除的可能性，及时采取恢复性措施；第二，信息保密性保护技术标准。信息存储中，安全保护技术须做到保证除有访问权限的合法用户之外，其他人都无法进入数据系统，同时保证寄存器、磁盘等记录的剩余信息不会泄露原有信息。信息传输中，安全保护技术须做到保证在数据传输过程中，信息不被泄露和窃取。另一方面在完善法律规定的同时，也可以鼓励网上银行利用大数据特点和优势，建立自己的数据库，对用户信息做相应的数据挖掘，探索建立动态数据风险监控机制，及时发现用户行为数据中的异常变动，提升风险防范能力。

（二）制定网上银行信息使用规则

对于网上银行用户信息保护，我国尚未出台专门的法律规定。[15] 2013 年工信部发布《电信和互联网用户个人信息保护规定》，这被认为是我国在网络个人信息保护立法上的巨大飞跃，该法第 8 条规定"电信业务经营者、互联网信息服务提供者应当制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布"。第 9 条分四个层次对信息收集、使用规则进行细化，分别是事先经用户同意并且事先告知用户收集使用信息的目的、方式和范围；不得收集提供服务必需以外的用户个人信息或者将信息用于提供服务之外的目的；不得欺骗、误导或强迫收集、使用用户信息；在用户终止使用服务后，应当停止对用户个人信息的收集和使用。[16] 除此之外，欧盟有一套完整的个人信息使用体系，其中《欧盟隐私政策通知》最具有代表性。该政策规定，网络用户应该收到"清楚并且易于理解的"告知与解释，能够从中得知其信息将被收集、储存并且处理，同时该告知与解释应通过小图标或者小标题的超链接，链接到网站隐私政策的专门页面。[17]

我国在制定网上银行信息使用规则时，可以结合《欧盟隐私政策通知》和《电信和互联网用户个人信息保护规定》，规定：一、网上银行应该制定清楚并易于理解的信息使用规则，置于网上银行网站的显著位置，能够被直接看到；二、信息使用规则必须写明收集、使用用户信息的范围、用途和方式，以及信息收集、使用的后果，保障用户的信息自决权；[18] 三、信息使用规则不得有引诱、威胁用户提供信息的文字；四、信息使用规则必须写明网上银行不得泄露、篡改或者毁损，不得出售或者非法向他人提供用户信息的义务；五、信息使用规则必须写明网上银行违反相关义务时应承担的法律后果、赔偿范围和用户申请赔偿的途径。

（三）规定网上银行附随义务和责任承担

1. 规定网上银行附随义务

和大部分隐私保护法的要求不同，法律并没有规定数据使用者在实现最初使用目的后必须删除存储的个人信息，相反，其被允许在很长的时间内存储信息数据，但是永久存储的数据给个人的信息安全带来极大的风险。[19] 因此，立法者在平衡二次运用数据的优势和过度披露数据之间矛盾时，可以依据存储数据的性质和内在风险，决定不同种类的个人数据必须删除的时间，以督促网上银行更好地保护用户的信息。

《合同法》中规定的附随义务包括通知、协助、保密等义务，对于协助义务，《合同法》第

---

〔15〕王远均《网络银行监管法律制度研究》，法律出版社 2010 年版，第 42 页。

〔16〕周汉华主编《个人信息保护前沿问题研究》，法律出版社 2006 年版，第 121 页。

〔17〕Teresa M payton，"Privacy in the Age of Big Data：Recognizing Threats，Defending Your Rights，and Protecting Your family"，Rowman and Little Field，2014，pp. 111.

〔18〕"信息自决权"的概念最早见于 1983 年德国联邦宪法法院对《人口普查法》案件所作的判决内容，信息自决权肯定每个数据主体对涉及自己数据提供、利用等的决定过程，都有积极参与及形成自我决定的可能。

〔19〕Viktor Mayer－Schonberger、Kenneth Cukier，A revolution，"That will transform how we live，work，and think"，Law Press，2013，pp. 222.

240 条规定“出租人、出卖人、承租人可以约定，出卖人不履行买卖合同义务的，由承租人行使索赔的权利。承租人行使索赔权利的，出租人应当协助。”[20] 当发生第三人侵犯网上银行用户信息的情形时，用户由于自身能力的限制和信息的不对称，通常无法找到侵害人，无法诉诸法律，对于这种情形，可以比照《合同法》规定的协助义务，规定网上银行负有帮助追偿、追查的义务，尽量帮助用户寻找侵权人，帮助用户索赔，并在用户提起诉讼时提供相关证据和证词证言。并规定如果网上银行在接到用户通知后没有尽到帮助追查、追偿义务的，则应当承担相应的责任。

2. 规定网上银行的责任承担

(1) 规定网上银行履行信息安全保障义务的标准

安全保障义务设立是为了防范风险，对风险处于支配、控制地位的人，必须以一个一般理性人应有的注意去控制风险，避免给他人、给社会带来损害。注意义务包括危害结果预见义务和危害结果控制义务。[21] 对于具体的安全保障义务标准的确定，需要综合考虑风险的大小、风险控制的可能性、风险控制人的能力、受害人自我保护的能力和危害结果的严重性等因素，对具体的个案得出合理的安全保障义务标准。[22] 网上银行具有风险大、技术依赖强和专业性强的特点，用户的信息保障很大程度上都依赖于网上银行自身的安全保障技术和格式合同约定等，网上银行由于本身的专业性和在信息收集、保护中占有的优势地位，承担的安全保障义务应当超过“一般理性人”应该具有的审慎义务，即网上银行的注意义务不是在危害结果预见和危害结果控制这两种义务中平衡分配，而是应该更新自身的安全技术，随时监控、排查，做到更优先地预见到风险的存在，主动排查危险。[23] 当网上银行尽到了这种注意义务时，即为履行了信息安全保障义务。

(2) 区分信息安全侵害的不同情形，确定不同的责任

网上银行信息安全侵害来源包括：网上银行自身安全技术漏洞和职员操作不当，用户故意、重大过失或者过失，第三人侵害。对于第一种情形，网上银行当然负起全部责任，不能通过格式合同将责任转嫁给用户；第二种情形，用户故意或者重大过失造成信息泄露的，应该由用户承担责任。对于用户一般过失造成自身信息泄露，为避免处于弱势地位的用户承担过重的责任，应当规定网上银行分担相应的责任；第三种情形，可依据《侵权责任法》的规定，存在第三人侵害行为的，网上银行承担补充责任。[24] 对于举证责任分配问题，理论和实践中安全保障义务的违法性多采用过错推定原则。只要负有安全保障义务人违法性确定，就推定其有过错，受害者无需举证证明。[25] 网上银行安全保障义务也当然适用过错推定原则，当发生用户信息泄露时，直接推定网上银行有过错，用户无需举证证明。网上银行信息泄露案件的证据多为电子证据，具有网络化、数字化的特点，又储存在网上银行服务器上，用户并不能真正掌握，在诉讼中要求用户提供并不在其掌握中的电子证据不公平且艰难，为保护用户的合法权益，应当根据网上银行和用户对电子证据的实际掌控能力等因素，合理分配举证责任。[26]《劳动争议调解仲裁法》第 39 条规定“劳动者无法提供由用人单位掌握管理的与仲裁请求有关的证据的，仲裁庭可以要求用人单位在指定期限内提供。用人单位在指定期限内不提供的，应当承担不利后果。”立法者可以比照该法规定，规定当电子证据是由网上银行掌握管理时，由网上银行承担举证责任。

---

〔20〕韩世远《合同法总论》，法律出版社 2011 年版，第 247 页。

〔21〕王利明、周友军、高圣平《中国侵权责任法教程》，人民法院出版社 2010 年版，第 430 页。

〔22〕Davi Otterheimer, “The Realities of Securing Big Data”, John Wiley and Sons, 2014, pp. 122.

〔23〕谢永志《个人数据保护法立法研究》，人民法院出版社 2013 年版，第 37 页。

〔24〕[德] 马克西米利安·福克斯《侵权行为法》，齐晓琨译，法律出版社 2006 年版，第 101 页。

〔25〕王泽鉴《债法原理》，北京大学出版社 2009 年版，第 120 页。

〔26〕张新宝《互联网上的侵权问题研究》，中国人民大学出版社 2003 年版，第 119 页。

## 四、网上银行交易安全保障义务完善途径

### (一) 完善电子合同规定

1. 优化电子合同格式条款

在互联网金融中，相比用户，网上银行处于主导的地位，为了平衡双方利益，立法机关在制定相关法律法规时，应该要求银行在风险提示以及信息披露义务方面承担起更多的义务，以保护用户知情权和选择权。因此，可以在借鉴《合同法》格式合同规定的基础上，作如下规定：其一，格式合同需简洁明了，写明双方的权利、义务、风险和责任；其二，格式合同内记载的信息必须真实、准确和完整，保护用户的知情权；其三，格式合同内的风险提示必须清晰、明确，做到足以引起用户注意；其四，格式合同必须做到对用户的保护，提示用户注意与自身有重大利害关系的条款;其五,格式合同必须保护用户的隐私权,防止用户交易数据泄露、丢失或不当使用。

2. 减少电子合同错误的发生

首先，网上银行必须保证电子合同的完整性和不可篡改性、用户签名行为的不可否认性和用户签名的不可仿冒性;[27] 其次，加强网上银行审查用户身份的能力。由于网上银行对于用户身份的审查的内容多是用户线上提交的身份资料，审查效果远远不如柜台当面的审核，因此应该要求网上银行审慎审查用户的身份。

由于互联网的特性和用户的弱势地位，在完善立法时可以规定当用户采取了必要的行为时，则用户不承担责任，必要的行为包括：用户在得知发生电子合同错误时及时通知网上银行，并且提供了所有信息，没有造成重大损失；用户没有使用该信息或者服务，也没有从中获得任何利益。当用户采取了这些行为时，则用户不承担责任。为督促网上银行认真履行安全保障义务,可以要求网上银行发现有可能的合同错误时,应该及时通知用户,获得用户的回复,才能履行合同。

### (二) 完善电子签名的立法模式

1. 电子签名立法适用“技术中立”与“技术特定”相结合的立法模式

“技术特定”立法模式认为在现有的电子签名技术里，对称密钥加密管理密钥困难，虹膜识别技术应用成本太高，只有公开密钥加密方法成本较低，同时又能满足安全保障的需求，应当确定为法定的电子签名技术，赋予其同书面签名一样的法律效力。[28] 但“技术特定”模式有以下缺陷：其一，技术特定限制了电子签名技术的发展。其二，公开密钥加密技术将密钥被冒用的风险推到了消费者身上，不利于保护消费者。“技术中立”立法模式认为电子签名技术不断发展，不同的电子签名技术的成本、保障功能等都参差不齐，应该由市场和消费者根据自身需求作出判断，立法者只需规定电子签名技术的最低标准。[29] “技术中立”立法模式的缺陷是,将电子签名技术的风险全部交由市场,而电子服务者往往将这种风险转移到消费者身上,不利于消费者权利的保护。

各国电子签名立法以美国和欧盟为典型代表。美国《联邦电子签名法》是完全自由放任的立法主义，对电子签名技术不作任何限定，将所有技术水平的电子签名都包含在内，目的是赋予电子签名使用者充分的自由选择权。但另一方面，不对电子签名技术进行强制性规定，也就不会

---

〔27〕王利明 《电子商务法律制度：冲击与因应》，人民法院出版社 2005 年版，第 151 页。

〔28〕对称密钥加密是指发送和接收数据的双方均使用相同的密钥对明文进行加密和解密；虹膜识别技术是指对人体眼部虹膜进行识别的生物识别技术，比指纹识别技术更具有安全性，成本也更高；公开密钥加密是指每个通信方均需要两个密钥，即公钥和私钥，这两把密钥可以互为加解密。公钥是公开的，不需要保密，而私钥是由个人自己持有，并且必须妥善保管和注意保密。目前公开密钥加密技术最为成熟，安全性也最高。

〔29〕欧阳武 《电子签名法原理与条文解析》，人民法院出版社 2005 年版，第 291 页。

规定电子签名使用过程中的法律责任的问题，不利于消费者权益的保护。欧盟电子签名指令同样对电子签名作了一个广泛的定义，即使是技术水平低的电子签名也具有法律效力，但该指令又根据电子签名安全性的高低将电子签名分为三种：简单的电子签名、一般的先进电子签名和严格的先进电子签名，〔30〕并赋予不同的法律地位，安全性更高的电子签名具有更高的真实性和更高的证据力，表明了对市场选择严格的先进电子签名的指引，以保障电子签名的一定程度的真实性。

我国的电子签名法采用的是完全的技术中立，对电子签名作了非常广泛的定义，避免了未来新增电子签名无法律效力的尴尬，也保证了电子签名使用者的自由选择权，但该立法模式也会带来电子签名技术的混乱，不利于消费者的权益保护。因而我国可以借鉴欧盟电子签名指令的做法，在认可任何技术水平的电子签名的同时，根据技术性和安全性的高低划分不同等级的电子签名，并赋予不同的法律效力和证据力，作出一定倾向性的指引，实现“技术中立”与“技术特定”相结合的立法模式，以更好地规范电子签名技术，保护电子签名使用者的合法权益。

2. 规定网上银行的附随义务

(1) 网上银行对用户负有保证认证证书所载信息真实性的义务

网上银行要求认证机构签发认证证书的目的，就是为了以此来证明自身身份和存储信息的真实性，以吸引更多的用户与之交易，因此网上银行对用户应负有注意、保护的附随义务。如果认证机构签发的认证证书存在错误，网上银行则应该因为违反了保证证书所载信息真实性的义务，向信赖认证证书的用户承担缔约过失责任或者违约责任。

(2) 网上银行对用户负有帮助追查、追偿的义务

我国《电子签名法》第28条规定，“电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任”。但是因为在网上银行交易中，网上银行往往提供了电子签名技术的选择，而用户是因为信赖网上银行才选择了电子认证服务提供者，而且由于用户的相对弱势，向电子认证服务提供者申请索赔，往往很难得到有效赔偿，因此在出现电子认证服务提供者造成用户损失情形时，网上银行应该负有帮助用户追查、追偿的义务，提供电子认证服务者的相关信息，帮助用户向电子认证服务者索赔，提供相关的证据。

(三) 完善未经授权电子支付法律制度

1. 区分授权和未经授权电子资金划拨

现实生活中未经授权的电子资金划拨现象千差万别，采用列举式或者概括式规定都无法涵盖所有情形，也会造成网上银行借此推卸责任，因此，我国可以借鉴美国《电子资金划拨法》的规定，对不适用的情形进行规定：其一，用户提供账号、密码或其他访问工具给第三人，除非用户通知网上银行不再授权该第三人划拨电子资金，第三人划拨电子资金的；其二，用户和第三人共同欺诈划拨电子资金的；其三，网上银行实施的错误电子资金划拨的。

2. 确定未经授权电子资金划拨中网上银行和用户的风险分担

网上银行由于预防、控制和转移风险的能力，应当承担更多的冒用风险责任。〔31〕在设定未

〔30〕简单的电子签名只需要具备电子签名的最低基本形式即可。一般的先进电子签名要求能够确认双方的身份。严格的先进电子签名要求具有合格的认证证书、由安全的签名生成设备生成。

〔31〕在分配未经授权划拨电子资金的责任时，应当主要从风险预防、风险控制和风险转移三个方面来确定网上银行和用户的责任。风险预防中，由于电子支付的虚拟性和电子签名等认证技术的有限性，用户在风险防范中能够起到的作用很小，风险的预防主要是由网上银行去承担；风险控制中，用户对于风险的控制的手段主要是妥善保管自己的账户、密码和工具以及在发生未经授权划拨时及时告知网上银行，而网上银行对于风险的控制则可以通过增强自身的安全保障技术、审慎审查用户身份等方式实现。风险转移中，网上银行可以通过如保险等方式转移风险，而用户没有其他方式可以转移风险。网上银行更有能力预防、控制和转移风险，而且网上银行从电子交易中获得的利益更大，应该从承担更多的责任。

经授权划拨电子资金的责任分担规则时，可以规定：其一，用户与第三人共同故意欺诈或用户有重大过失时，用户承担全部责任；其二，用户怠于通知或者有其他违反诚实信用原则情形时可借鉴美国《电子资金划拨法》做法；其三，除上述两种情况外，责任由网上银行承担。

美国的《电子资金划拨法》规定消费者只对三种未经授权划拨情形承担责任：划拨使用的卡或访问工具已经经过用户同意并接受；金融机构已经提供如签字、指纹等手段确认持有访问工具的用户身份；金融机构已向用户披露了未经授权划拨的责任。我国也可以借鉴该做法，明确限定网上银行用户在以下情形对未经授权电子资金划拨承担责任：该电子资金划拨是用户已经接受、使用的账户、电子签名或者其他访问工具；网上银行已经采用了国内通用的、有效的身份认证方式，能够在电子资金划拨时有效认证用户的身份；[32] 网上银行已经在有关合同中约定了发生未经授权电子资金划拨时的责任，以及受理办公室的电话号码、地址和受理流程。在符合上述条件时，用户才有可能承担相应的责任。

美国的《电子资金划拨法》对消费者承担的责任规定了三个等级：50 美元、500 美元和无限责任，同时设定了严格的适用条件。责任等级的具体适用取决于未经授权电子资金划拨发生的时间和用户通知金融机构的时间，即在知晓发生未经授权电子资金划拨时及时告知。[33] 该规定一方面可以限定消费者承担的责任，保护消费者的利益；另一方面也鼓励消费者在发现访问工具遗失或被窃时及时通知金融机构，以免损失发生或进一步扩大。[34] 我国也可以分级网上银行用户的责任，并设定用户通知网上银行的时间，以督促用户及时行使权利，保护用户的合法权益。除了用户故意、重大过失造成电子资金未经授权划拨外，网上银行都应该承担相应的责任，以实现交易安全保障义务。

## 结　语

大数据时代，网上银行存储的用户数据、交易数据等都在大幅度增长，与传统网络时代相比，大规模的数据聚集和不断更新发展的数据分析工具，使得网上银行用户的信息安全和交易安全面临着前所未有的挑战。对此，仅仅依靠《电子银行业务管理办法》等网上银行监管法律法规和《合同法》、《侵权责任法》、《消费者权益保护法》等传统法律，已经不足以应对不断发展的危机。对于网上银行安全保障义务的法律完善问题，必须细化至信息安全技术标准、信息使用规则、电子合同、电子签名等层面，深入探讨完善路径。与此同时，网上银行完全可以利用大数据的优势，建设自己的“数据仓库”，完善数据挖掘技术，分析存储的用户静态数据和动态数据，建立事中交易的监控机制，以更好地实现安全保障义务。

责任编辑：李　剑

〔32〕樊林波　《电子商务中的跨国电子认证问题初探》，法律出版社 2002 年版，第 271 页。

〔33〕由于发生未经授权电子资金划拨时，用户并不能随时知晓，因此规定了金融机构寄送定期报表的义务，所以消费者通知金融机构的时间包括发生划拨时及时告知或者定期报表寄送后 60 日内。

〔34〕孙晔　《美国电子商务法》，北京邮电大学出版社 2001 年版，第 87 页。