情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

FTA 체결에 따른 금융정보 국외이전에 대한 정책적 대응방향 연구*

이 정 훈,† 박 석 훈, 임 종 인‡
고려대학교 정보보호대학원

A Study on the policy counterplan of Cross Border Financial Information Transfer according to FTA*

Jung-hun Lee,† Seok-hoon Park, Jong-in Lim‡
Graduate School of Information Security, Korea University

요 약

전 세계적으로 국가 간 자유무역이 확대되고 있는 상황에서, 우리나라도 최근 미국, EU 등 금융선진국들과 FTA 협정을 체결하는 등 급속히 추진되고 있다. 이 협정문에 따르면, 우리나라의 외국계 금융회사가 보유하고 있는 이용자 정보가 국외로 이전이 가능하게 될 전망이다. 본 논문에서는 이러한 금융정보의 국외이전에 대비하여 정보이전의 개념과 범위를 정의하고, 국내·외 관련 법·제도 현황을 파악해 보고자 한다. 아울러 정보이전 시 예상되는 문제점을 제도적, 기술적 부문으로 나누어 검토하고 정보규제의 차별화, 개인정보보호법과 관련법규의 제·개정, 금융회사의 안전성 확보 및 정보이전 표준가이드라인 마련 등의 정책적 대응방안을 제시한다. 특히, 이용자의 프라이버시 보호를 위하여 개인정보의 이전 시 금융정보와 차별화하는 정책 수립의 필요성을 언급한다. 본 논문에서 제안된 방안은 향후 FTA 시행 후 금융정보의 국외이전에 대비하여 금융회사와 감독당국 등 관련기관이 준비해야 할 대책 마련에 도움이 될 것으로 기대한다.

ABSTRACT

In a situation where worldwide free trade between countries has expanded recently, our country is being rapidly pushed FTA agreements with the financial developed countries such as United States, EU. According to the agreement, the user information of foreign financial companies in Korea is expected to be transfered overseas. In this paper, we need to define the scope and the definition about the transfer of information and analyze the relating domestic and foreign laws preparing for Cross Border Financial Information Transfer. Also, we review the expected issues about the transfer of information divided into institutional and technical sectors and are presented the policy implication such as differentiation of regulatory information, enactment and amendment of Personal Information Protection Law(Draft) and related regulations, ensuring the safety of financial companies, raise the standard guidelines of the transfer of information. We refers to the needs for policy formulation to differentiate our privacy information from financial information to protect the privacy of users.

The proposed countermeasures in this paper is expected to be helpful the measures to prepare for other institutions such as banks and supervisory authorities prepare for the future Cross Border Financial Information Transfer according to FTA.

Keywords: FTA, Data Transfer, Personal Information, Financial Information, Information Security, Cross Border

접수일(2010년 7월 15일), 게재확정일(2010년 10월 13일)
* 이 연구에 참여한 연구자(의 일부)는 '2단계 bk21사업'의 지원비를 받았음.

† 주저자, onlyu2k@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

I. 서 론

전 세계적으로 국가 간 상품 및 서비스 교역에 대한 관세 및 무역장벽을 완전히 철폐하는 국제자유무역협정(FTA) 체결이 확대되고 있는 추세이다. 과거의 FTA는 관세철폐, 통관절차 등 규범이 주로 협상의 대상이었으나 최근에는 서비스, 투자, 지적재산권, 환경 등 사회전체 분야로 범위가 확대되는 경향이 있다. 외교통상부 자료에 따르면 우리나라는 2004년 칠레와의 FTA협정 발효를 시작으로 국제자유무역국가가 되었으며 최근에는 미국과 유럽연합(EU) 등 금융선진국들과도 협정을 체결하고 국회 비준 후 시행에 들어갈 것으로 기대된다. 또한, 세계 최대 무역국가인 중국과 우리나라와 오랜 무역 경쟁국인 일본과도 협상을 준비하는 등 현재 우리나라는 약 70여개의 많은 국가들과 협상을 발효, 체결 또는 준비 단계에 있다.

한-미 FTA협정문에서는 금융서비스 부문과 관련하여 국가 간 금융회사 정보를 국외로 이전하는 것에 대하여 허용토록 명시하고 있다. 이는 국내에서 영업중인 외국계 금융회사가 업무과정에서 생성된 우리나라 국민의 이용자 정보를 해당 금융회사의 글로벌한 정보 분석 및 평가 등의 업무를 위하여 본·지점 간에 공동으로 처리할 수 있도록 허용한다는 것을 의미한다. 지금까지 외국계 금융회사의 경우 주로 홍콩, 싱가포르, 인도 등 해외 거점국가에 자체 데이터센터를 두고 아시아 및 태평양 지역의 국가들을 대상으로 금융시스템을 운용하였으며, 우리나라의 경우 국내법(전자금융감독규정시행세칙 제7조)에 따라 금융회사 전산설비의 해외 이전이 사실상 어려웠기 때문에 국내에 데이터센터를 따로 두고 금융시스템을 운용해 왔다. 그러나 현재 FTA협정이 발효 중인 칠레, 싱가포르, 인도 및 동남아 국가들과 달리 미국, EU 등 금융선진국들과 FTA협정이 체결됨에 따라 은행, 증권, 보험 등 외국계 금융회사가 보유하고 있는 우리나라 이용자의 개인정보를 포함한 금융정보가 국외로 이전할 수 있게 될 전망이다. 금융회사가 보유하고 있는 금융정보는 개인의 신상정보인 개인정보 뿐만 아니라, 개인의 재산과 관련된 금융정보가 포함되어 있어 어떤 다른 산업의 정보보다도 그 가치와 중요도가 높은 이용자의 자산이라고 할 수 있을 것이다.

최근 국가 간 정보이전으로 인하여 정보유출 사고가 빈번히 발생하고 있으며 또한, 이러한 사고들은 단순한 개인범죄 차원을 넘어서 국가 간 분쟁으로까지 문제가 확대되고 있다. 이에 따라 FTA 발효 시에도 양국 간의 금융정보 유출로 인한 사고방지를 위하여 철저한 대책을 마련하고 정보유출사고 발생 시 양국 간 협력 방안과 해결을 위한 조치 방안에 대하여 사전에 상호 간 긴밀한 협의가 이루어져 할 것이다. 이는 향후 정보유출 및 금융사고의 발생으로 국제 분쟁 시 소송으로 진행될 경우 당사국 또는 제3국 등 어떠한 국가와 지역의 법원이 재판 관할권을 가지며 어떠한 법률이 적용될 것인가 하는 문제가 발생하기 때문이다. 이를 국제적 분쟁에서 재판 관할권과 준거법의 문제라 한다. 국가 간 정보의 이전은 다양한 행위주체와 관련되어 있기 때문에 재판관할권 문제가 매우 복잡해질 가능성이 있다. 피해자의 손해배상 소송이 외국에서 이루어지면 비용이 증가될 뿐만 아니라 언어장벽 등의 이유로 소송의 결과에도 상당한 영향을 미칠 수 있기 때문이다. 따라서 FTA 시행에 대비하여 국가 간 정보이전 시 사법 관할권 적용에 관한 문제점들을 명확히 인식하고 이에 관한 준비를 철저히 해야 할 것이다. 또한 금융정보의 국외이전은 정보이전과 관련된 산업분야에도 영향을 미칠 가능성이 있다. 금융정보를 저장, 처리, 분석하기 위한 하드웨어와 소프트웨어의 개발·유통 등 정보의 순환과 관련된 국내 정보기술(IT) 산업에 영향이 미칠 가능성도 있다. 반면 FTA는 상호 국가 간의 협약이므로 해외에서 영업하는 우리나라 금융회사에도 동일하게 적용됨에 따라, 국내 IT업체의 매출 증가 요인이 될 수도 있을 것이다. 특히 우라나라가 인터넷 및 IT산업의 강국임을 감안할 때 향후 우리나라 IT산업분야의 새로운 발전계기가 될 가능성도 있다.

금융감독원 자료에 따르면 금융서비스 이용의 편리성, 정보기술의 급속한 발달 등으로 인하여 2008년도 전체 금융거래 중 인터넷뱅킹, 폰뱅킹, 모바일뱅킹 및 자동화기기 등 은행의 전자금융거래가 차지하는 비중이 80%를 초과하는 것으로 나타났다. 아울러 최근에는 무선인터넷 접속이 가능한 스마트폰 보급의 확대로 이를 이용한 모바일뱅킹, 모바일증권거래, 모바일전자지급결제 등 모바일 전자금융거래가 급속히 증가할 것으로 기대된다. 이처럼 전자금융거래가 활발한 우리나라에서 금융거래의 안전성과 가용성이 확보되지 않는다면 이는 금융회사와 관련된 경제적 측면뿐만 아니라 큰 사회적 혼란을 일으킬 수 있는 문제가 발생할 수도 있을 것이다.

이에 본 논문에서는 우리나라와 주요 국가가 시행중인 정보의 국외이전과 관련된 법·제도 현황을 살펴보고, 외국계 금융회사의 금융정보 국외이전에 대비하

여 향후 발생 가능한 제도적·기술적 부문의 문제점을 분석함에 따라, 우리가 사전에 준비해야 할 대응 방향을 정책적 관점에서 모색해 보고자 한다.

II. 정보이전의 개념 및 법·제도 현황

2.1 정보이전의 개념

2.1.1 "금융정보"의 정의

한-미 FTA 협정문에는 금융정보에 대한 명시적 정의 규정은 없다. 다만 협정문[1] 가운데 부속서에 규정된 정보의 이전 조항을 살펴보고 본 논문에서 사용하고자 하는 금융정보의 용어를 정의하고자 한다.

〔표 1〕 한-미 FTA 협정문 정보이전 관련조항

〈제13장〉 제2절 정보의 이전
각 당사국은 다른 쪽 당사국의 금융회사가 그 기관의 일상적인 영업과정에 데이터 처리가 요구되는 경우 그러한 처리를 위하여 자국 영역 안과 밖으로 정보를 전자적 또는 그 밖의 형태로 이전하는 것을 허용한다. 대한민국은 이 협정 발효일 후 2년 이내에 이 약속을 발효한다.

제3절 기능의 수행

1. 양 당사국은 당사국 영역 내의 금융회사가 그 당사국의 영역 안 또는 밖에 소재한 그 기관의 본점 또는 계열사에서 일정 기능을 수행하도록 허용하는 것이 유익함을 인정한다. 실행 가능한 한도에서, 각 당사국은 그러한 본점 또는 계열사가 이 기능을 수행하는 것을 허용하여야 할 것이다. 이 기능은 일반적으로 다음을 포함하나 이에 한정되지 아니한다.

나. 데이터 처리[16], 프로그래밍 및 시스템 개발과 같은 기술 관련 기능

16) 당사국이 부속서 13-나 제2절에 따라 자국 영역 밖으로 정보의 이전을 허용할 의무를 지는 한도에서, 그 당사국은 또한 이전 후 그 정보의 데이터처리를 허용한다.

"금융정보"란 우리나라에서 영업 중인 외국계 금융회사가 영업과정에 생성되어 보유하고 있는 우리나라 이용자 정보를 말한다. 이는 국내에서 수집되고 저장된 금융회사의 정보 중 해외의 글로벌한 영업실적 조사와 리스크 분석, 통계자료 작성 등 분석·평가 업무를 수행하는데 있어서 필요한 정보를 가리킨다. 구체적으로는 금융회사가 영업과정에 데이터 처리가 요구되는 경우로써 정보처리가 가능한 저장매체에 보관된 정보를 의미한다. 즉, 금융회사가 보관하고 있는 전자적으로 처리 가능한 정보로써 일반적으로 개인정보 및 금융정보를 모두 포함한다. 이러한 금융회사가 보관하고 있는 전자적으로 처리 가능한 정보를 세부적으로 살펴보면 금융회사 보유정보와 금융정보 처리업무로 구분할 수 있다.

〔표 2〕 금융회사의 보유정보 및 처리업무

구분	세부 내용		특성
금융회사 보유정보	개인(법인) 정보	이름(법인명), 주민번호(사업자등록번호), 주소, 전화번호, 아이디, 비밀번호, IP주소 등	정보 자체
	금융정보	계좌번호, 비밀번호, 거래일자, 거래금액, 잔고, 카드번호 등	
	기타 정보	신용등급, 대출한도, 대출금액, 직업, 재산, 소득금액, 재무제표(법인), 손익계산서(법인) 등	
금융정보 처리업무		정보(가공)처리, 프로그램 개발 및 유지보수, 콜센터 등	정보 처리

협정문의 금융서비스 부문 제13장 제2절에 명시된 정보의 이전은 "금융회사의 일상적인 영업과정에 필요한 정보의 이전"임을 명시하고 있다. 이는 정보의 개념이 금융거래 이용자의 이름, 주민번호, 계좌번호, 거래내역 등 명확하게 열거된 특정 항목이 아닌 영업 활동에 필요한 모든 정보를 포함하는 개념으로 해석될 수 있다. 즉 금융회사가 금융거래 과정에서 발생되는 본질적인 정보뿐만 아니라 일상적인 영업업무 거래과정에서 발생되는 부가적인 정보도 포함될 수 있는 것으로 해석된다. 이러한 개인정보를 포함한 금융정보는 각기 규제하는 핵심 논거가 다름에 따라, 이는 다음 절에서 구체적으로 살펴보기로 한다.

2.1.2 "이전"의 정의

금융정보의 "이전"이란 금융정보를 외국의 해당 금융회사 본·지점 등으로 전송하는 것을 말한다. 한-미 FTA 협정문의 경우 금융서비스 부문 제13장 제2절에 따르면 우리나라에서 영업 중인 외국계 금융회사가 보유하고 있는 우리나라 이용자 정보를 외국의 해당 금융회사 본·지점 등으로의 전송을 허용하고 있다. 즉 외국의 금융회사가 보유하고 있는 금융정보를 업무의 효율성과 서비스 향상을 위하여 옮기거나 접근할 수 있도록 허용한다는 의미이다.

경제협력개발기구(OECD)에서 설명하는 정보의 국외이전(Cross-Border)을 살펴보아도 "정보가 정보의 수집이 이루어졌던 곳과 다른 곳에 위치하는 경우, 정보 자체가 제3국으로 전송되었을 경우, 단순히

정보의 중요한 사안이 제3국가에 있을 경우를 의미"한다고 정의하고 있다[2]. 이는 정보의 수집 국가와 정보의 이용 국가가 상이한 경우를 모두 포함하므로 매우 광범위한 의미로써 정보의 국외이전을 상정하고 있는 것이다. 아울러 전 세계적으로 인터넷 보급 및 활용이 급격하게 성장함에 따라 정보의 이전이 갈수록 용이해지고 있는 현실을 감안하여 "이전"의 의미를 광의로 인정하는 것이 현실이다.

2.1.3 금융정보 이전의 범위

앞서 본 바와 같이 국외로 이전 가능한 금융정보는 개인정보를 포함한 금융회사의 일상적인 영업과정에 필요한 모든 정보로 해석된다. 아울러 한-미 FTA 협정문 제13장 제3절에서는 정보의 국외이전과 관련하여 "데이터처리, 프로그래밍 및 시스템 개발과 같은 기술 관련 기능"을 포함하여 단순히 정보 자체의 이전에만 국한하지 않고 전송된 정보를 가공 및 처리할 수 있도록 하는 데이터 처리도 가능하도록 명시하고 있다. 즉 국외로 이전된 정보를 가공·처리하기 위해 필요한 전산설비와 이와 관련된 서비스의 이전을 허용하는 것으로 해석될 수 있다. 다시 말해서 한-미 FTA에 명시된 정보 이전의 범위는 금융회사가 보유하고 있는 금융정보와 이전된 정보를 처리하는 데 필요한 업무도 함께 포함하는 것을 의미한다.

2.2 정보이전 관련 법·제도 현황 및 국가 간 정보 이전 사례

2.2.1 정보이전에 따른 위해요소 및 법·제도 규제의 핵심 논거

금융정보 국외이전과 관련하여 크게 두 가지의 위해요소가 발생할 수 있다. 첫째, 개인 프라이버시 침해 가능성이 존재한다. 개인의 프라이버시는 국민의 기본 권리로 인정되고 있는 현실에서 금융정보를 이전하게 되면 금융정보에 포함된 개인정보도 함께 이전될 수 있기 때문에 개인 프라이버시의 침해 가능성은 커질 수밖에 없다. 이러한 프라이버시의 침해 가능성을 줄이기 위해서 OECD는 "프라이버시 보호와 개인정보의 국제유통에 관한 가이드라인"을 제정하여 프라이버시를 보호하고 있으며 각 국은 이러한 유사 규제를 강화하고 있는 추세이다. 둘째, 금융거래의 안전성 확보가 소홀해질 우려가 있다. 국외로 이전되는 금융정보의 용량에 반비례하여 금융거래의 안전성은 반대급부적으로 줄어들게 된다. 금융정보의 이전으로 인하여 금융회사의 거래 활성화 및 편익 증대의 이익뿐만 아니라, 금융거래의 안정성 확보는 반드시 함께 고려되어야 할 필수 요소이다.

최근 많은 비중의 금융거래가 전자적으로 이루어짐에 따라 전자금융거래법 제21조 제2항에서는 "금융기관 등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자금융거래의 종류별로 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융업무에 관하여 금융위원회가 정하는 기준을 준수하여야 한다."라고 규정하여 금융거래의 안전성 확보를 위해 노력하고 있다. 이와 같이 정보이전에 대한 위해요소가 각각 다름에 따라, 개인정보와 개인정보를 제외한 금융정보를 각기 다른 관점에서 규제해야 할 필요성이 있다.

다음은 법·제도 규제에 관한 핵심논거에 대해 살펴보기로 한다. 첫째, 개인정보는 자국민의 권리에 관한 부분이므로 매우 강하게 보호되어져야 한다. 개인정보는 누구도 침해할 수 없는 개인의 프라이버시와 관련된 국민의 권리에 관한 문제이므로 양보할 수 없는 보호법익이 된다. 그렇기 때문에 미국과 EU 등 세계 각국은 이러한 개인정보를 보호하기 위하여 최선의 노력을 경주하고 있으며 법률적 규제도 갖추고 있다. 거래의 편리성 보다는 자국민의 권리보호에 보다 더 비중을 두고 있는 추세이다. 둘째, 개인정보를 제외한 금융정보는 감독의 대상으로써 글로벌 환경 하에서는 활용을 극대화하여야 한다. 일반적인 창구금융거래가 전자금융거래로 발전되어 이용자와 거래량이 증가함에 따라 당사자인 금융회사뿐만 아니라 이용자인 거래고객과 이를 감독하는 기관도 매우 편리해진 것이 사실이다. 거래의 안정성만 확보된다면 이러한 편리성이 증가할수록 사회전체의 이익이 증가할 것이다. 따라서 글로벌 환경의 시대에서 개인정보를 제외한 금융정보의 활용은 금융 산업 발전과 이용자의 편리성 향상 측면에서 적극적으로 활용되어져야 할 필요성이 있다.

2.2.2 우리나라의 법·제도 현황

전 세계적으로 인터넷 및 정보기술 산업의 발달로 인하여 정보화 사회에 들어서면서 갈수록 정보보호의 중요성이 강조되고 있는 현실에서 우리나라도 공공 및 금융부문의 관련 법·제도를 마련하여 개인정보와 금융정보를 보호하고 있다. 향후 한-미 FTA 발효 등으

로 금융정보의 국외 이전에 대비하여 국내의 현행 정보이전 관련 법·제도 현황을 파악해 보고 개정 여부의 가능성을 검토할 필요성이 있을 것이다.

현재 우리나라 국내법 상 정보의 국외 이전과 관련하여 정보의 이전을 금지하는 제한을 두고 있는 법률은 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정통망법)이 있으며, 아울러 공공 및 금융 관련 법률 등에서 개인정보 등 정보보호를 위한 법적 안전장치를 마련해 놓고 있다. 정통망법에서는 원칙적으로 개인정보의 국외이전은 허용하지 않고 있다. 다만, 예외적으로 개인정보의 국외이전 시 국가 간 이전 및 개인정보의 보호에 관한 업무, 안전성을 침해하는 행위를 방지하기 위한 업무 등에 대해 상호 협력하고, 아울러 국외로 이전된 개인정보의 보호와 관련하여 이용자의 동의를 받고 이에 따른 동의 항목과 절차에 대해 명시함으로 엄격한 보호절차를 취하고 있다. 공공기관의 개인정보보호에 관한 법률은 개인정보의 국외이전에 대하여 구체적인 조항을 가지고 있지는 않지만 개인정보 파일의 보유·변경 시 사전협의를 거쳐야 하며 개인정보의 이용 및 제공의 제한을 두고 있는바, 원칙적으로 국외이전에 대하여는 허용을 고려하지 않고 있다.

금융정보 제공과 관련하여 금융실명거래 및 비밀보장에 관한 법률(이하 금융실명법)에서는 금융거래 정보의 제공과 관련하여 원칙적으로 이용자의 동의 없이 제공을 금지하고 있으며, 사용목적의 특수성을 감안하여 영장에 의한 청구 등 예외조항을 두고 일부에 한해 정보 제공을 허용하고 있다. 또한, 이용자의 금융거래 정보 제공 시 제공사실을 당사자에게 통보하도록 명시하고 있으며, 동 제공 정보에 대한 요구자, 제공자, 법적 근거 등 관련 자료에 대해 사후 관리를 위하여 일정기간 동안 기록·보관토록 하는 등 이용자보호 장치를 마련하고 있다. 신용정보의 이용 및 보호에 관한 법률(이하 신용정보법)에서는 개인의 신용정보를 타인에게 제공 시 사전에 이용자에게 동의를 받도록 하고 있으며 서면, 전자문서 등 동의방법에 대해 자세히 기술하고 있다. 또한 동 정보의 이용에 있어서도 업무상 설정 및 판단 여부만을 파악하기 위한 목적으로만 사용하도록 함으로써, 이용범위를 엄격히 제한하고 있다. 전자금융거래법에서도 역시 전자금융거래정보 제공에 관하여 제한을 가하고 있으므로 엄격한 규제를 가지고 있다. 그러나 금융정보의 국외이전에 관한 명시적인 규정은 없는 것이 현실이다.

위에서 살펴본 정보이전 관련 국내법 중에서 정통망법을 제외하고 정보의 국외이전에 관한 이용자 보호 및 국가 간 협력 등을 위한 법·제도적 장치가 명시적으로 마련되어 있지 않다. 더욱이 정통망법의 경우 개인의 식별정보인 개인정보에 대해서만 명시하고 있으며 사고발생 가능성이 높고 시장 가치와 거래 가치가 큰 금융정보에 대해서는 명시되어 있지 않다. 따라서 우리나라도 향후 미국, EU 등과의 FTA 시행에 대비하여 외국계 금융회사의 금융정보가 국외로 이전될 경우, 예측 가능한 문제점들을 사전에 검토하고 금융정보 국외이전에 따른 법·제도적 안전장치를 마련하기 위한 노력들이 필요할 것으로 예상된다.

2.2.3 외국의 법·제도 현황

최근 개인정보, 금융정보 등 정보의 중요성이 갈수록 부각되면서 금융 선진국인 미국, EU 및 OECD 등은 정보의 국외이전 시 자국의 국민에 대한 개인정보 및 금융정보를 보호하기 위한 명시적인 법·제도적 장치를 마련하여 시행하고 있다.

외국의 정보이전과 관련하여 대표적인 법·제도로써 1980년도에 OECD에서 발표한 "사생활 보호와 개인정보의 국제적 유통에 관한 지침"이 있다. 이는 갈수록 증가되는 개인의 사생활(프라이버시) 보호를 위하여 8가지 기본 원칙[①개인정보 수집제한(Collection Limitation), ②정보 정확성(Data Quality), ③목적 명확성(Purpose Specification), ④이용의 제한(Use Limitation), ⑤안전성 확보(Security Safeguard), ⑥공개성(Openness), ⑦정보주체의 통제권(Individual Participation), ⑧책임 확보(Account-ability)]을 제시하고 국제적으로 준수토록 권고하였다.

이에 우리나라도 2000년도에 OECD의 8대 원칙을 정통망법에 반영함으로써 국제적인 개인정보보호 강화 추세에 동참하였다. 아울러 향후 한-미, 한-EU 등 FTA 시행에 따라 정보의 국외 이전 시에도 마찬가지로 8대 원칙이 반영되도록 하여야 할 것이다. 특히 이 원칙 중 사용 목적의 명확성, 안전성 확보 및 책임의 원칙 등에 입각하여 개인정보의 이전은 보다 엄격해질 것으로 기대된다. 즉 FTA의 본질에 맞게 금융회사 영업행위 향상의 목적을 위한 금융거래 정보의 국외이전은 적극적으로 검토되고, 상대적으로 금융회사의 영업행위와 관련이 작은 고객의 개인정보는 소극적으로 논의되어 추진될 것으로 전망된다.

또한 정보의 국가 간 거래 시 상대국의 정보보호수

준을 평가토록 한 영국의 "정보보호법(DPA, Data Protection Act, 1998)"과 EU의 "정보통신망에서 개인정보 수집 및 처리에 관한 개인정보보호지침(1999)" 등이 있다. 이에 따라 EU 회원국 중 하나인 아일랜드는 정보의 국외이전 시 EU의 안전국가목록(White List)과 미국의 세이프하버(Safe Harbour)에 속한 국가로만 전송토록 한 "개인정보보호법(1988)"을 2003년 개정하여 시행하였다[3]. 위 사례와 같이 우리나라도 금융정보의 FTA 상대국 또는 제 3국으로의 이전에 대비하여 정보유출 사고방지대책 등 이전 정보의 안전성 확보가 가능한지 여부에 대해서도 객관적이고 합리적인 평가가 선행되어야 할 것이다.

2.2.4 국가 간 정보이전 대처사례

FTA 체결에 따른 금융정보의 국외이전 허용은 한-싱가폴, 한-미, 한-EU 등 우리나라뿐만 아니라, 이미 시행된 EU-멕시코(2000), 미국-싱가폴(2004) 등 여러 국가에서도 FTA 조항에 유사한 내용으로 반영되었다. 이처럼 국가 간 자유무역거래에 있어서 금융회사 정보의 국외이전 허용은 매우 보편화되어가는 것이 전 세계적인 추세이다. 이러한 상황에도 불구하고 당사국들은 자국민의 소중한 정보를 보호하기 위한 적극적인 대처방안을 마련하고 있다.

미국과 EU간의 국가 간 개인정보 이전에 대한 협약인 "미국 상무부의 Safe Harbor 원칙(2000)"은 국가 간 정보이전 대처 사례로써 중요한 의미를 가지고 있는데, 이에 대하여 구체적으로 살펴보도록 한다. 이는 미국과 EU간의 개인정보의 국제적 유통 논쟁의 해결책을 제시하였다. 이는 2000년 7월 EU의 승인으로 체결된 것으로써 금융선진국 간의 개인정보의 국외이전에 대한 국제적 합의를 이끌어 낸 원칙이다. 세이프하버[4] 원칙에 따르면 미국 기업들이 동 원칙의 7가지 정보보호 항목을 충족시키는 경우에 한하여 EU 내에서 자유로운 국제간 거래를 허용한다는 것이 골자이다.

이 세이프하버의 7가지 원칙은 첫째, 이용자에게 사전에 고지(Notice)하고 둘째, 이용자가 필요시 거부할 수 있는 선택권을 보장(Choice)하고 셋째, 국가간에 적절한 원칙을 따르는 제3자에게만 정보를 제공(Onward Transfer)하며 넷째, 정보보호를 위한 안전성(Security) 방안을 마련하고 다섯째, 데이터 무결성(Data Integrity) 방안을 마련하며 여섯째, 이용자의 접근(Access) 권한을 부여하고 일곱째, 실효성 담보를 위한 원칙의 강제할 수단 마련(Enforcement)하는 등의 요건을 충족시켜야만 국제간 거래가 허용됨을 구체적으로 규정하고 있다.

이와 더불어 EU의 개인정보보호지침에 의한 "적절한 수준"의 정보보호제도를 적용한 사례로써, 미국과 EU간에 체결된 "승객정보 이전에 관한 합의(2006)"가 있다. 2004년 미국은 9.11 테러를 계기로 자국 영토를 출입하는 항공기의 승객정보 제출을 의무화함에 따라 2004년 미국과 유럽 항공사간에 항공기에 탑승하는 승객정보 전체를 제공하는 협상이 체결되었다. 그러나 EU는 이 협상에 따른 자국민의 정보이전이 "적절한 수준"의 보호를 받지 못하고 있다고 판단함에 따라 EU의 프라이버시법에 저촉되므로 불법으로 판결하여 미국과 재협상 후 새로운 합의를 도출하였다. 이 합의안에서는 자동화된 시스템에 의해 제한된 승객정보(이름, 주소, 전화번호, e-메일, 항공승객정보(PNR), 예약날짜, 여권번호, 좌석번호 등 34가지)만을 제공하며 또한, 이 정보를 제공받는 미국기관도 국토안보부, 출입국 및 세관국 등으로 축소하였다[5]. 위 사례는 우리가 FTA 시행 후 금융정보 이전 시 정보이전에 있어서 그 목적의 명확성에 초점을 맞춰 본질에 충실해야 한다는 것을 보여준다. 즉 국가 간 이전되는 정보의 성격, 정보이전에 따른 역할 및 중요도, 이전된 정보의 적절한 안전성 등에 따라 국가 간 정보의 이전은 허용될 수도 있으며 이전이 제한될 수도 있다는 것이다.

이처럼 우리나라도 향후 국가 간 자유무역거래 확대에 따라 자칫 소홀해질 우려가 있는 국민의 정보보호에 대하여 충분한 법·제도적 안전성 확보 방안을 사전에 마련하고, 상대국의 적절한 보호조치 여부와 정보이전의 효과성 등에 입각하여 다각적인 대처방안이 검토되어져야 할 것이다.

III. 정보이전 시 예상되는 문제점

3.1 제도적 부문

3.1.1 개인정보보호의 취약성 증가

금융회사가 보유하고 있는 금융정보 중 개인정보는 금융거래에 있어서 거래 당사자의 신원확인을 위해 반드시 필요한 정보이다. 하지만 무분별한 정보의 수집·보관, 내부자의 정보관리 소홀 및 외부의 불법적

인 정보유출 등으로 인하여 이용자의 소중한 금융자산이 불법적으로 유출되는 사고가 많이 발생하고 있다. 이러한 금융사고의 유형은 사기에 의한 피싱(Phishing), 현금서비스 불법 인출, 신용카드 복제 사기 및 인터넷쇼핑몰의 안심클릭 결제사고 등 다양한 금융거래의 수단과 접근매체를 통하여 발생되고 있다[6]. 실제로 최근에 인터넷쇼핑몰 옥션의 1천만여명 개인정보유출 해킹사고와 GS칼텍스의 내부자에 의한 1천만여명 개인정보 유출사고, 모아저축은행의 7천여건 고객대출정보 해킹사고 등의 대규모 정보유출 사고가 발생하여 고객의 개인정보를 이용한 금융사고의 발생 가능성이 높아졌다.

외국의 주요 정보유출 사고사례를 보면 가장 큰 규모의 정보유출 사고로 2009년 1월에 발생한 미국 하트랜드사의 1억 3천만 건 개인정보 유출 사고가 발생하였다. 이 회사는 미국의 상위 신용카드 지급결제 처리회사로써 주요 고객인 중소 식당, 소매점 등에 대한 고객 정보가 유출된 것으로 나타났다. 또한 2007년 1월에는 미국의 의류 전문 업체인 TJX사가 보유하고 있던 9천4백만 건에 달하는 개인정보가 유출되었다. 금융회사 중에서는 2005년도에는 글로벌 신용카드 회사인 비자, 마스터카드, 아메리칸 익스프레스사의 고객정보 4천만 건이 유출되는 사고가 발생한 바 있으며, 과거 1980년대부터 2000년대인 현재까지 꾸준히 대규모 정보유출 사고가 발생하고 있는 것으로 나타났다[7].

다음은 국가 간 정보유출로 인한 사고 및 분쟁 사례에 대하여 살펴보자. 국가 간 정보유출 사고는 지속적으로 발생되고 있으며 대부분 금전적인 이득을 목표로 범죄가 이루어지고 있음을 알 수 있다. 2005년 6월 발생한 미국의 "CardSystems Solutions사의 정보유출 사건"은 일본의 4천여 고객정보가 유출되고 약 1백만 달러의 금전적 손실이 발생한 사건으로 미국과 일본 간의 국제적 분쟁을 야기 시킨 사건이다. 2006년도에는 캐나다의 한 회사가 130만 명의 미국 학생의 이름과 사회보장번호(SSN) 기록이 저장된 컴퓨터를 분실하여 대량의 개인정보를 유출시킨 사건이 발생하였다. 또한, 2006년 6월 인도로 아웃소싱한 영국은행에서 2천5백 명의 미국 노동자 개인 정보를 이용하여 20만 파운드를 절도하다 체포된 사건도 발생하는 등 많은 국가 간 정보유출 사고가 발생하였다[8]. 위 사례에서 보듯이 우리나라도 국가 간 정보유출 사고 방지를 위하여 국가적 차원에서 우리나라 국민에 대한 최소한의 프라이버시 보호를 위해 적극적인 자세로 최선의 노력을 다하여야 할 것이다. 이와 같이 개인정보 유출이 불법적인 금융사고로 연계될 가능성이 높아짐에 따라 금융정보의 국외이전 시 개인정보 유출방지를 위한 보다 강력한 대책을 마련해야 할 필요성이 있다. 즉 정보이전 시 금융회사가 보관하고 있는 금융정보 중 이름, 주민번호, 전화번호 등 개인정보는 보다 엄격한 보호기준을 마련하여야 할 것이다.

3.1.2 정보이전에 관한 전담주체의 불분명

최근 정보유출 사고가 급증하고 개인정보의 중요성이 부각되면서 소중한 개인정보를 보호하기 위하여 기존에 산재된 관련법들을 통합하고, 보다 체계적인 법·제도 마련을 위한 "개인정보보호법"이 현재 제정되어 2011.9.30일부터 시행될 예정이다. 동 법에 따르면 개인정보의 수집·이용 제한 및 제3자에 대한 제공·파기 절차, 주민번호 등 고유식별 개인정보 처리 제한, 개인정보의 안전한 관리 방법 및 법 위반 시 처벌 조항 등 보다 명확하고 강화된 세부 내용들을 포함하고 있다.

이 법에서는 제7조 내지 제8조에 "개인정보보호위원회"를 설치하여 전담 주체를 명시하고 있으나, 현재 시행 예정인 법률이므로 현행법상에서는 금융정보 이전에 관한 주체가 불분명한 상태이다. 따라서 향후 정보이전에 관한 법률적 해석이 필요할 경우 개별 법률들이 규제하는 정부, 사법부, 사업자 등 별개로 책임을 묻게 되어 책임소재가 불분명해짐에 따라 어느 누구도 명확한 책임을 질 수 없는 상황이 발생할 소지가 있으므로 더욱 주의를 기울여야 할 것이다.

3.1.3 정보이전의 범위와 내용의 불명확성

협정문에 나타난 문구를 살펴보면 금융회사의 국외로 이전된 정보에 대한 가공처리 업무를 위한 설비 이전으로 해석하는 것이 합리적이나, 양국 간의 협정문 해석 차이로 인하여 여·수신 업무, 대출 심사·승인 등 금융회사 본질적 업무를 처리하는 핵심 전산설비도 이전이 가능하다고 해석할 수도 있다. 이는 양국 간 매우 큰 해석의 차이를 가져올 수 있으므로 국외로 이전 가능한 정보처리 업무를 구체적으로 적시하여 명확하게 해석되어야 할 것이다. 과거에 국민은행(현 KB국민은행)이 중국으로 고객센터 이전을 추진하였고, 외국계 메트라이프 생명보험사가 국내 전산센터의 해외이전을 추진함에 따라 국내 이용자 정보의 해외 유

출이 우려된 사례들이 있었다[9].

향후 FTA 시행에 따라 정보처리, 아웃소싱 등 금융정보 처리업무가 국외로 이전이 허용되더라도, 금융회사가 보관하는 금융정보의 저장 등 핵심전산설비는 국내에 유지하고, 원시데이터의 2차 가공 업무만을 국외로 위탁할 가능성이 크기 때문에 급격한 산업계 전반에 영향을 미치지 않을 수도 있다. 하지만 금융회사 감독정책의 변화와 안정적인 금융시장 확보를 위하여 국외로의 제3자 업무위탁에 따른 철저한 법·제도적 장치를 마련할 필요성이 있다. 따라서 금융정보의 국외이전에 따른 이전 대상의 범위와 내용의 불명확성에 대하여는 확실히 문제점으로 인식하고 접근해야 할 것이다.

3.2 기술적 부문

3.2.1 정보이전 금융회사의 리스크 증가

향후 한-미, 한-EU 등 FTA 발효 후 금융정보와 정보처리 전산설비를 국외로 이전하는 외국계 금융회사의 경우, 국내에서 과거 수년간 업무 수행을 통하여 이루어진 안정적이고 검증된 정보시스템에 큰 변화를 가져올 가능성 있다. 정보처리를 위한 서버, 데이터베이스, 네트워크 등 물리적인 환경과 금융서비스 제공을 위한 어플리케이션, 프로세스 등 논리적인 환경의 변화가 한 국가 영토 내에서 이루어지는 것이 아니라, 여러 국가에 걸쳐 이루어짐에 따라 원거리로 인한 통신지연, 예상치 못한 천재지변 등으로 서비스 중단, 정보 유출 등과 같은 사고로 이어질 가능성이 있다.

실제로 금융회사가 금융서비스의 성능 향상 및 노후화된 전산설비의 개선 등을 위하여 이른바 차세대시스템 또는 전산통합시스템으로 변경하는 과정에서 많은 비용과 오랜 준비기간에도 불구하고 시스템 변경 후 서비스 지연, 오류 및 중단 등 많은 시행착오를 겪은 사례들이 있다. 2004년 서비스를 개시한 외환은행의 차세대 시스템의 경우 결제청구 프로그램 오류로 인하여 신용카드 결제대금이 이중으로 인출된 사고가 발생하였으며, 2010년 KB국민은행의 경우 전산 프로그램 오류로 인하여 약 6시간 동안 인터넷뱅킹 이체 수수료 부과에 오류가 발생하는 장애가 발생한바 있다. 더욱이 이와 같은 국내 대형 금융회사 보다 상대적으로 기술적, 인적 자원이 열약한 외국계 금융회사의 경우, 정보이전 시 금융거래의 안전성 확보를 위하여 감독당국, 금융회사 및 IT보안업체 등 유관기관의 보다 많은 관심이 필요할 것이다.

3.2.2 정보이전에 따른 사고발생 증가

금융회사 정보의 국외이전으로 인하여 발생 가능한 사고는 크게 2가지로 정보유출사고와 이 유출된 정보를 이용한 금융사고로 구분할 수 있다.

정보의 국외이전 시 또는 이전된 정보의 처리 과정에서 관리소홀, 외부공격 등의 이유로 정보유출 사고가 발생할 가능성이 있다. 정보화 사회로 발전하면서부터 전 세계적으로 국가와 기업이 보유하고 있는 국민과 고객의 소중한 정보가 유출되는 사례가 꾸준히 발생하고 있다. 특히 최근에는 정보기술 산업 및 인터넷 등 정보기술의 발달로 정보처리가 용이해 지고 정보의 활용가치가 확대됨에 따라 정보를 불법적인 금전적 이익수단으로 악용하기 위한 정보유출 사고가 빈번하게 발생하고 있다.

정보유출은 유출경로에 따라 내부자 또는 외부자 유출로 나눌 수 있다. 전자는 담당자나 내부직원의 부주의 또는 고의적인 유출 방법이고, 후자는 외부의 불법적인 해킹, 피싱 등에 의한 유출 방법이다. 특히 금융정보의 국외 이전 시 국내 금융거래 이용자들의 금융정보가 무분별하게 유출되거나, 위탁기관의 목적 외로 활용될 가능성을 배제할 수 없다. 금융회사가 보유하고 있는 이름, 주민번호, 전화번호 등의 개인정보와 계좌번호, 비밀번호 등의 금융정보는 금융거래에 있어서 매우 중요한 정보로써 유출 시 심각한 금융사고로 이어질 개연성이 크다.

이러한 정보에 대해서는 국외이전 시 유출되더라도 사고로 이어지지 않도록 하기 위하여 주민번호, 신용카드번호 등 개인 식별정보는 정보의 일부분을 삭제 또는 마스킹(Masking)하거나, 의미 없는 데이터로 변경하는 등의 보안대책을 마련하여 사고를 미연에 방지토록 하여야 할 것이다. 실제로 금융부문에 있어서 개인정보 유출사고는 정보의 수집단계에서 부터 정보의 이용 및 보유단계, 그리고 마지막으로 정보의 제공 및 공개 단계에 이르기 까지 모든 경로의 정보 처리 단계에서 발생하고 있다[10].

더욱이 금융회사가 보유하고 있는 법인정보의 국외이전에 따른 정보유출 시 해당 기업에 큰 피해를 입힐 가능성이 있다. 공개되지 않은 기업의 재무제표, 손익계산서, 신용등급 등 재무정보는 유출된 정보 자체만으로도 기업 평가 및 주식 시장 등에서 금전적 가치를 가진 정보이므로 유출 시 기업에 매우 큰 악영향을 미

칠 수 있다. 국가정보원 자료에 따르면 2004년부터 2009년까지 발생한 국가 및 기업 간 기술정보유출 사고는 전직직원에 의한 정보유출이 56.2%, 현직직원이 24.6%로 전·현직 직원인 내부자 유출사고가 80% 이상인 것으로 나타났다. 이는 정보유출 보안사고 방지를 위해서 정보를 관리하는 내부 담당자에 대한 접근 통제와 외부로 정보유출 방지를 위한 담당자의 조치가 매우 중요함을 보여준다.

또한 경찰청 자료에 따르면 2006년 6월부터 발생하기 시작한 전화금융사기(보이스피싱)는 2010년 1월까지 총 20,873건이 발생하였으며, 그 피해액은 무려 2,066억 원에 달하는 것으로 나타났다. 더욱 주목해야 할 부분은 사고의 범죄자 분석 결과, 중국의 콜센터를 통하여 우체국 등 국가기관을 사칭하여 범죄를 발생하는 등 국제 조직에 의한 사고 발생률이 약 11.8%에 달하는 것으로 나타났다. 이와 같은 사실은 향후 금융정보 국외이전 시 불법유출로 인하여 전화금융사기 등 금융사고가 더욱 증가할 가능성도 배제할 수 없음을 나타낸다.

3.2.3 금융전산환경 변화의 가능성

금융회사의 주요 업무 중의 하나인 정보처리 업무가 국외로 이전될 경우, 금융회사의 업무 편의, 비용절감, 자국의 이익 등을 위하여 이와 관련된 정보처리 서비스도 함께 이전될 가능성이 높다. 더욱 우려가 되는 것은 외국계 금융회사가 전자금융거래법에서 명시하고 있는 법적 준수사항인 금융회사의 전산센터(소규모인 경우 전산실)와 재해복구센터를 제외하고 모든 업무설비와 이에 따른 인력을 국외로 이전시킬 가능성도 있다는 것이다. 이는 궁극적으로 자국으로 정보를 이전한 외국계 금융회사의 영업형태가 미국, 싱가포르, 홍콩 등 금융선진국에서는 이미 제도화되어 영업중인 무점포·비대면 거래의 다이렉트뱅크(Direct Bank) 또는 인터넷전문은행(Internet Bank)과 유사한 형태의 금융회사로 변형될 가능성을 내포하고 있다[11]. 아울러 금융선진국의 대규모 글로벌한 인터넷전문은행들이 무점포, 고금리 등의 장점을 내세워 우리나라 금융시장에 신규로 진출할 가능성도 있다. 하지만 우리나라의 경우 현재까지 설립·인가된 인터넷전문은행은 없으며, HSBC은행 서울지점이 2007년 2월부터 이용자의 금융회사 직원의 직접 방문을 통한 대면확인 방법을 이용하여 다이렉트뱅킹 서비스를 제공하고 있는 수준이다. 따라서 외국계 인터넷전문은행이 다이렉트뱅킹 등 새로운 형태의 서비스로 우리나라 금융시장에 진출할 가능성에 대비하여야 할 것이다. 아울러 이러한 상황에서 정보의 국외이전이 가져올 수 있는 금융시장과 전자금융거래 환경의 변화를 미리 예측하여 신속하게 대처하기 위한 사전 준비가 필요할 것으로 보인다.

IV. 정책적 대응 방향

4.1 제도적 부문

4.1.1 국외이전 정보의 규제 차별화 정책 수립

앞서 살펴본 바와 같이 FTA 시행에 따라 국외이전 대상이 되는 정보는 개인정보와 개인정보를 제외한 금융정보로 구별된다. 이러한 정보는 법 제도 규제의 핵심논거가 다르기 때문에 이전되는 정보의 금융업무와 관련되어 가치와 필요성에 따라 개인정보의 보호기준 마련에 보다 엄격한 정책을 마련할 필요가 있다. 금융정보의 국외이전은 금융회사 업무의 가치와 필요성을 높이기 위함이므로 이에 상대적으로 차별화되며 프라이버시 성격이 강한 개인정보는 보다 엄격한 보호정책을 마련하여야 하겠다. 즉 개인정보를 제외한 금융정보의 거래는 글로벌 환경에서 금융업무의 효율성을 높이고 이용자의 편익을 증진시키기 위하여 적극 활용하도록 상대적으로 규제를 완화할 필요성이 있다. 이에 반해 개인정보에 대하여는 자국민의 권리 보호를 위하여 상호주의 및 미국이 진행하고 있는 세이프하버 원칙 등을 참고하여 보다 강화된 기준을 정책에 반영하여야 할 필요성이 있다고 판단된다.

4.1.2 개인정보 전담주체를 지정한 개인정보보호법 시행

금융정보의 국외이전에 있어서 개인정보보호기구의 역할은 매우 크다. 그 임무로는 외국으로 이전된 자국민의 개인정보와 관련하여 침해가 발생한 경우에 외국의 보호기구에 조사 및 침해 중단을 요청할 수 있기 때문이다. 또한 외국으로부터 자국에 이전되어 온 개인정보 침해사례에 대해서도 침해여부의 조사 및 법률 이행상황에 대한 감독과 피해구제 등의 역할을 하여야 하기 때문이다. 개인정보보호법에는 개인정보보호위원회를 두고 있는데, 이 위원회를 개인정보 관리의 주체로 지정하여 개인정보 침해조사 전담기구로 활용하여야 할 것이다. 제3국에서 개인정보의 오·남용 사고

발생 시 우리나라의 관련기관이 당사국의 침해 여부를 확인하는 것은 현실적으로 매우 어렵다. 이는 개인정보가 외국으로 전송되는 경우 정보주체가 당면하는 어려움에 대해 그들이 겪고 있는 문제의 원인을 파악하기 힘들고 따라서 정보보호가 제대로 이루어지고 있는지, 혹은 법적 구제수단을 취할 수 있는지에 대해서도 판단하기 어렵기 때문이다. 이러한 불만을 처리하기 위하여 독립적인 기관의 존재는 필수적이며 아울러 국제적으로 적절한 수준의 정보보호기반 구축에 있어서도 필수적인 이유이기도 하다.

4.1.3 법적장치 마련선행 및 국제협력체계 구축

금융정보 처리의 해외위탁은 정보기술 발전 및 대규모 금융업무 처리의 경제성·효율성 등의 측면에서 국제적으로 허용되고 있는 추세이다. 이와 더불어 금융회사가 운영하고 있는 금융정보 처리를 이용한 부가적인 산업에 변화가 있을 수 있다. 이에 앞서 FTA 협정문의 양국 간 모호한 해석은 금융정보를 이용한 부가산업 전반에 영향을 미칠 수 있으므로, FTA에서 명시한 정보처리 이전에 대한 명확한 범위가 정해져야 할 것이다. 향후 정보이전과 관련된 시행세칙 등 세부조항의 제·개정을 통하여 정보이전에 대한 명확한 방법과 절차를 마련하여야 하겠다. 온라인(On-line), 오프라인(Off-line) 등 정보이전이 가능한 방법들을 나열하고, 이에 따른 양국 간 합의된 세부절차를 마련하여 금융정보의 안전성을 확보하고 일관성 있는 방안 마련을 추진해 나가야 할 것이다. 우리나라 금융정보의 국외이전과 관련된 법·제도의 제·개정의 경우, 앞서 살펴본 외국의 정보이전 관련 법·제도 사례와 국가 간 정보보호협정 체결 원칙 등을 감안하고 우리나라의 현실성을 고려하여, 국제적 수준에 적합하도록 정비해야 할 것이다.

우리나라의 법률에 있어서 정보의 국외 이전과 관련하여 개정의 검토성이 필요한 법률은 정통망법이 있을 수 있다. 동 법률의 개정 작업은 미국, EU 등 금융선진국들과의 FTA 시행으로 향후 발생 가능한 금융정보의 국외 이전에 따른 문제점에 대해 보다 명확하게 대처하기 위한 방안을 마련하기 위한 것이다. 아울러 금융실명법, 신용정보법, 전자금융거래법, 개인정보보호법 등 관련법들은 금융정보의 국외 이전에 대한 근거가 미비함에 따라 발생할 수 있는 문제점을 보완하기 위하여 명확한 제도적 장치를 마련함으로써 안정적인 법·제도 시행에 기여할 것으로 기대된다.

정보이전과 관련된 세부 시행세칙 제·개정은 아래의 7가지 방안을 포함하여 검토되어야 하겠다. 첫째, 정보의 책임소재를 명확히 해야 한다. 국외로 이전된 정보의 보안성, 무결성 및 가용성에 대한 문제 발생 시의 책임 소재 및 처벌 조항을 명확하게 하기 위한 방안을 마련하여야 하겠다. 둘째, 정보이전의 기준을 정확히 명시해야 한다. 정보의 이전방법 등에 따라 정보이전이 성립되는 시점 및 조건에 대해 국가 간 공통적인 기준을 명확하게 마련하여야 할 것이다. 셋째, 정보이전의 절차를 명확하게 해야 한다. 온라인 전송, 오프라인 전송 등 이전 방법에 따른 정보 이전 절차를 명확하게 하기 위한 방안을 마련할 필요가 있다. 넷째, 상호 감독권 보장을 제도화하여야 한다. 아울러 정보이전에 따른 금융회사 및 아웃소싱 업체 등에 대한 감독·검사 필요시 상대국의 감독권 및 검사권 보장을 위한 권한, 절차 등 대응 방안을 마련하여야 할 것이다. 다섯째, 합의사항 이행을 위한 방안을 마련하여야 한다. 금융회사, 아웃소싱 및 국가 간에 합의된 사항을 미 이행 시 양국 간 해결을 위한 대응방안을 마련하여야 한다. 여섯째, 상대국의 정보보호수준에 대한 객관적인 평가기준을 마련하여야 한다. 안전한 정보이전을 위하여 상대국의 정보보호수준을 국제적이고 합리적인 기준에 따라 평가하고 적용할 수 있는 객관적인 방안이 마련되어야 할 것이다. 마지막으로, 예외 조항에 대한 방안을 마련하여야 한다. 정보이전에 있어서 양국 간에 자국 내의 법·제도 및 사회적 환경 등 국가적 특성을 고려하여, 예외상황 발생 시 합리적인 수준 내에서 허용 가능한 수준의 조치 방안에 대해서도 논의하여야 할 것이다.

개인정보보호법 제14조 2항(국제협력)에는 "정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다."라고 규정하고 있다. 국가 간 정보유출 사고 발생 등으로 당사국 간 분쟁 사례가 늘면서 자국의 국민에 대한 개인정보 보호 및 원활한 국가 간 정보 이전을 위한 국제공동협력 사례가 늘어나고 있다. 1980년 시행된 OECD의 "프라이버시(Privacy) 보호 및 개인정보의 국가 간 유통에 관한 지침(1980)"에 이어, EU의 "개인정보의 자동처리와 관련된 EU 국가 간의 국제적 협약(1981)", UN의 "컴퓨터화된 개인정보파일의 규율에 관한 지침" 및 EU의 "개인정보의 처리와 개인정보의 자유로운 유통에 관한 개인의 보호지침(1995)" 등이 대표적인 국가 간 정보보호를 위한 국제협약 사례로써 참고할 필요성이 있다[12].

국제협력체계 구축과 관련하여서는 우리가 선택할 수 있는 것은 2가지이다. 첫째, 미국의 정보보호 기준이나 EU의 "적절한 수준"의 정보보호 지침을 우리가 수용하는 것이다. 다시 말해 미국이나 EU 등의 정보보호 지침을 수동적으로 받아들이는 방법이다. 둘째, 미국이 EU에 세이프하버 원칙을 적용했던 것처럼, 우리의 정보보호 수준을 강화시켜 우리나라 업체가 강화된 정보보호 항목을 충족시키는 경우에 한하여 미국과 EU 등 상대국 내에서 자유로운 국제간 거래가 허용될 수 있도록 하는 것이다. 즉 우리가 강력한 정보보호 기준을 마련하고 이에 맞추도록 능동적으로 상대국에게 요구하는 방법이다. 이러한 국제협력체계 구축과 관련하여서 정보이전에 따른 금융회사 및 아웃소싱 업체 등에 대한 감독·검사 필요시 감독대상의 기관, 권한, 범위, 절차 및 처벌 조치 등 양국 간 상호 감독권 보장 방안을 구체적으로 마련할 필요성도 있다. 참고로 개인정보보호법에서는 개인정보분쟁조정위원회(제6장: 제40조 내지 제50조)를 설치하고 손해배상 책임을 명시함으로서 피해자에 대한 실질적 보호가 될 수 있도록 규정하고 있다.

이와 같이 금융회사가 보유하고 있는 정보의 주체이지만 정보의 국외 이전에 대한 권한이 미비한 개인 등 금융거래 이용자에 대한 보호 장치가 국제협약사례 등을 감안하여 합리적인 수준에서 마련되어야 할 것인바, 아래의 6가지 방안을 포함하여 마련되어야 하겠다. 첫째, 개인 및 법인 등 금융거래 이용자 정보의 국외 이전 시 이용자에 대한 사전 고지, 이전 여부의 선택권 보장 등 이용자의 사전 동의를 위한 명확한 방법 및 절차 등 작성 방안이 마련되어야 할 것이다. 둘째, 이용자가 국외로 이전된 본인 정보에 대하여 적절한 절차에 따라 정보의 내용, 목록, 일자, 유출여부 등 이전 정보의 조회, 수정 및 철회의 권한을 부여할 수 있는 방안이 마련되어야 할 것이다. 셋째, 국외로 이전된 이용자 정보의 금융회사에 정해진 용도 외에 정해진 다른 용도로 고객정보 활용을 금지하기 위한 양국간의 이전 정보의 이용 제한을 위한 합의 안이 마련되어야 할 것이다. 넷째, 금융실명법, 신용정보법 등 이용자 정보보호 관련 국내 법·제도를 준수하거나 또는 이를 신뢰할 만한 적절한 대응책 마련을 위한 노력이 필요할 것이다. 다섯째, 금융정보의 위·수탁자에 대하여 고의·중과실 등에 따른 이용자 정보 유출 시 위탁자의 민사상 책임 등 이용자 피해 보상을 위한 구제 방안이 마련되어야 할 것이다. 마지막으로, 국외로 이전된 정보의 유출사고 등으로 인한 국가 간 분쟁을 사전에 예방하기 위한 양국 간 공동협력기구 구성을 검토해 볼 필요성이 있다. 이 기구는 사고 발생 시 신속하고 합리적인 조치를 위한 협조와 공동 대응, 국가 간 금융정보 이전 및 정보보호에 관한 법·제도 개정 논의, 이전 정보 관련 최근 동향 파악 및 정보공유 등을 위하여 양국 간의 금융회사, 감독당국, 소비자보호단체 등 민관이 합동으로 참여하는 국제공동협력기구를 구성하는 방안 마련을 검토해 볼 필요성이 있을 것이다.

4.2 기술적 부문

4.2.1 정보이전 금융회사의 안전성 확보를 위한 기술 전담조직 구성

금융정보 국외이전에 대비하여 금융거래의 안전성을 확보하고 이용자가 안심하고 서비스를 이용할 수 있도록 발생 가능한 기술적인 문제점을 파악하고, 이에 따른 보호대책 마련을 위한 감독당국, 금융회사, IT보안업체 등 다자가 공동으로 참여하는 테스크포스(T/F, Task Force)를 구성하여 외국계 금융회사에 대한 안전성 확보를 위한 종합적인 대책을 마련할 필요성이 있다. 과거에도 금융회사와 감독당국은 금융거래의 안전성 확보와 이용자 보호를 위하여 2005년 7월 "전자금융거래 안전성 강화 종합대책 T/F", 2006년 9월 "IC카드용 단말기 전환촉진 방안 마련을 위한 T/F", 2009년 7월과 12월에는 "사이버테러(디도스 공격) 대응을 위한 T/F", "스마트폰 전자금융서비스 안전대책 마련 T/F"를 각각 운영한 바 있다. 이러한 테스크포스의 목적은 첫째, 정보이전의 기술적 안전성 및 보안성을 검토하고 둘째, 정보이전 이행상황에 대해 점검 및 대응 조치하며 셋째, 체계적인 정보이전을 위한 기술 표준을 마련하고 마지막으로, 분야별 담당자의 의견 조정 등이 주요골자가 될 것이다. 또한, 성공적인 T/F 운영을 위해서 구성원의 담당 업무, 운영기간 및 방식, 일정 작성 등 철저한 세부계획을 수립하여 운영하여야 할 것이다. 아울러 정보 이전 시 자료 생성, 전송 처리, 자료 파기 및 사후 관리 등 모든 단계에 있어서 기술적 문제점과 사고 위험성을 철저히 분석하고 명확한 해결방안을 강구하여야 할 것이다.

4.2.2 금융정보 국외이전의 표준 가이드라인 마련

금융정보의 국외 이전 시 체계적인 관리와 합리적인 운영을 위하여 정보유출 및 금융사고 방지를 위한

정보보호 표준 가이드라인을 마련해야 할 필요성이 있다. 이 가이드라인은 크게 2가지 대응방안으로 구분되며 첫째, 접근통제 강화와 둘째, 정보유출 방지를 위한 목적으로 나눌 수 있다.

먼저 접근통제 강화를 위한 대응방안으로는 첫째, 안전한 정보보호를 위해서는 1차적으로 이전된 정보를 입력, 변경 및 삭제 등 처리업무를 담당하는 내·외부 직원의 명확한 접근통제 절차와 체계적인 권한관리를 갖추어야 한다. 둘째, 정보유출 사고는 내부자에 의해 발생되는 경우가 많으므로 내부직원에 대한 정보유출 및 불법 사용 방지를 위한 상시 모니터링과 주기적인 감사 실시 등으로 엄격한 내부통제시스템을 갖춰야 할 것이다. 셋째, 국외 정보이전 사항에 대한 내용을 철저히 기록하고 접근기록, 이전내용, 처리결과 등 주요 처리내역을 감독당국에 사전·사후 보고가 이루어져야 할 것이다. 이는 국외로 이전된 자국민의 정보에 대하여 국가적 차원에서 통제가 이루어지지 않는다면, 국외이전 정보의 유출 등 국가 간 사고 발생 시 신속하고 명확하게 대처하기 어려울 것으로 판단되기 때문이다.

정보유출 방지를 위한 대응방안으로는 첫째, 정보이전 과정에서 유출 방지를 위하여 온라인 전송 시 전용선 사용 등 보안기준을 마련하고 오프라인 전송 시 이송용 전용케이스를 사용하는 등 정보이전 보안대책을 마련하여야 할 것이다. 둘째, 개인의 인적사항을 포함하는 개인정보의 경우 마스킹하거나 변경 또는 암호화 하는 등 정보유출 시 불법적인 금융사고 방지를 위하여 국제적 수준에 맞는 보호기준을 마련해야 할 것이다. 아울러 부득이하게 마스킹이나 변경하지 않고 원시데이타를 전송하는 예외상황에 대비하여서도 대응책도 마련하여야 할 것이다. 셋째, 이전된 정보를 저장·처리하는 서버 등은 물리적으로 네트워크를 분리하여 안전한 내부망에 보관토록 하고, 국제인증등급의 방화벽, VPN(가상사설망, Virtual Private Network) 등 안전한 보안장비를 설치·운영토록 하며, 노트북, USB 등과 같은 저장매체와 e-메일, 휴대전화 등을 통한 외부유출 방지를 위한 물리적인 시스템 및 네트워크 보호대책도 마련되어야 할 것이다.

4.2.3 새로운 금융전산환경 변화에 대비한 보안대책 마련

금융회사 정보의 국외이전이 가져올 새로운 금융환경의 변화에 대비하기 위하여 한발 앞선 준비와 대책 마련을 서두를 필요성이 있다. 스마트폰을 이용한 모바일뱅킹 증가, 인터넷전문은행 또는 다이렉트뱅크 형태의 전자금융거래 업무 확대 및 클라우드컴퓨팅과 같은 신규 정보기술 도입 등 새로운 형태의 정보기술 및 전자금융 환경의 변화에 대비하기 위한 준비를 해야 할 것이다. 금융위원회 자료에 따르면 2008년도부터 최근까지 정부기관, 금융회사, 투자기업 등에서 자본금, 업무방식, 본인인증 확인방법 등 여러 문제점에 대한 인터넷전문은행 제도 도입에 관하여 검토해 온 바 있다. 그러나 최근 개정된 은행법에서 그 동안 논의되어 왔던 제도적·기술적 문제점들을 해결하지 못하고 국제정세 등 여러 복합적인 상황을 반영하여 인터넷전문은행 설립이 무산되었다. 하지만 금융선진국에서는 이미 보편화 된 인터넷전문은행 형태의 신규 업무진출 가능성 대비하여 금융회사와 감독당국은 보안대책 마련 등을 검토할 필요성이 있다. 특히 인터넷전문은행을 설립하는 모회사의 경우 미국 등 금융선진국 뿐만 아니라, 국내에서 추진되었던 경우도 마찬가지로 은행, 증권사 등 금융회사에 비해 규모가 작고 비금융회사인 일반 기업체인 경우가 많다. 이 경우 상대적으로 규모가 크고 안정적인 전산설비와 금융시스템을 보유하고 있는 금융회사에 비하여 시스템의 안정성과 보안성이 낮을 가능성이 있으므로 보다 강화된 보안대책을 강구하여야 할 것이다.

또한, 2009년도말 국내에 도입된 애플사의 아이폰을 계기로 급증한 우리나라 스마트폰의 활성화에 따라 향후 정보이전 외국계 금융회사의 모바일뱅킹 등 온라인 거래가 증가할 가능성이 있다. 특히 정보를 국외로 이전한 외국계 금융회사의 경우, 국내 인력을 축소하고 창구업무를 줄이는 반면, 인터넷뱅킹, 모바일뱅킹, 자동화기기 등 온라인거래를 중심으로 하는 전략적 방안을 구사할 가능성도 있다. 또한 새로운 IT기술인 클라우드컴퓨팅 시장의 확대로 인하여 데이터의 이동 및 관리가 용이해짐에 따라 외국계 금융회사가 보관하고 있는 정보의 국외 이전을 가속화 시킬 가능성도 배제할 수 없을 것이다. 이처럼 정보의 국외이전으로 인하여 유발될 가능성이 있는 금융시장의 새로운 영업형태 출현과 정보기술의 발전으로 인한 다각적인 금융전산환경 변화에 대비하기 위하여 전자금융거래의 안전성을 확보하고 이용자를 보호하기 위한 철저한 보안대책이 마련되어져야 할 것이다.

V. 결론 및 향후 추진과제

전 세계적으로 국가 간 자유무역협정이 늘어남에 따라 금융정보의 국외이전도 증가할 것으로 기대된다. 이러한 상황에서 무엇보다 중요한 것은 FTA 당사국 간의 이해와 신뢰뿐만 아니라, 안전하고 합리적인 제도적·기술적 보호 장치의 마련이 선행되어져야 한다. 금융정보의 정의, 정보이전의 개념과 범위에 대한 당사국 간의 명확한 해석이 필요할 것이며, 정보이전에 따라 나타날 수 있는 위해요소에 대해서도 앞서 살펴보았다. 또한, 주요국가의 정보이전 관련 법·제도를 참고하여 우리나라 국민의 프라이버시 보호를 위한 법률의 제·개정 시 반영하여야 할 것이다.

아울러 금융정보의 국외이전 시 예상되는 문제점에 대해 파악하였고, 이에 따른 제도적·기술적 대응방안을 부문별로 제시하였다. 제도적 방안으로 금융정보 중 개인정보에 대한 보다 강력한 보호정책의 필요성에 따른 이전 정보의 규제 차별화 정책 수립과 개인정보보호법의 조속한 시행, 세부 시행세칙 제·개정 및 국제협력체계 구축 등을 제안하였다. 기술적 방안으로는 테스크포스를 통한 정보이전 금융회사의 안전성 확보, 정보이전 시 표준가이드라인 개발, 새로운 금융전산환경에 대비하기 위한 대책 마련 등을 제시하였다.

본 연구에서는 향후 금융정보의 국외이전으로 인하여 발생 가능한 이슈와 문제점에 대하여 고찰하였고 이에 따른 제도적·기술적 대응방향을 제시함으로써, 향후 한-미 FTA 발효 후 2년의 유예기간 동안 감독당국과 금융회사의 세부방안 마련을 위한 단초가 될 수 있을 것으로 판단한다. 이에 따라 향후에는 국가 간 정보이전이 합리적인 제도적 절차와 안전한 기술적 방법에 따라 처리되도록 세부적인 법·제도를 정비하고 정보보호 및 보안장치를 갖추어야 할 것이다. 이러한 체계적인 정보이전을 통해 자국의 이익을 극대화하고 이용자 편익을 증진하며, 나아가서는 국가 간 협력과 공조를 통하여 세계의 금융정보 공유가 신 성장 동력으로써 발휘되고 정보화 시대의 투명성과 금융거래의 활성화에 기여할 수 있는 발판이 되도록 모두 노력하여야 할 것이다.

참 고 문 헌

[1] 외교통상부 FTA, "한-미 FTA 협정문", 외교통상부, p.23-24, 2007년 5월.

[2] 이윤희, "OECD의 국가간 프라이버시법 시행에 대한 논의 및 제안", 한국정보보호진흥원, p.4, 2006년 11월.

[3] 박창곤, "2003 개인정보보호백서", 한국정보보호진흥원, pp.244-247, 2004년 1월.

[4] U.S. Department of Commerce's Commercial Service.http://www.export.gov/safeharbor/eu/eg_main_018476.asp

[5] 이용규, "개인정보 국외이전 관련 국가 간 협력방안 연구", 한국정보보호진흥원, pp.81-83, 2006년 12월.

[6] 김인석, 김태호, 강형우, 이정호, 홍기석, 전자금융 이러면 안전할까?, 디비바다미디어, pp. 52-60, 2010년 4월.

[7] Open Security Foundation. http://www.opensecurityfoundation.org

[8] 이윤희, "OECD의 국가간 프라이버시법 시행에 대한 논의 및 제안", 한국정보보호진흥원, p.6, 2006년 11월.

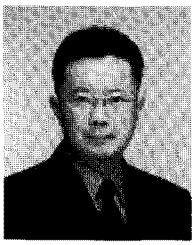
[9] 조화순, "초국가네트워크의 개인정보: 국가 간 갈등의 사례와 현황분석", 한국전산원, pp. 29-33, 2004년 6월.

[10] 이창범, 윤주연, "해외 개인정보 판례 및 사례 조사·분석", 개인정보분쟁조정위원회, 한국정보보호진흥원, pp. 114-231. 2004년 12월.

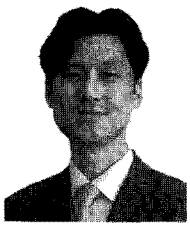
[11] 김태호, "국내 인터넷전문은행 설립시 예상되는 전자금융리스크에 대한 대응방안 연구", 석사학위논문, 고려대학교, pp. 17-22, 2008년 12월.

[12] 조화순, "초국가네트워크의 개인정보: 국가 간 갈등의 사례와 현황분석", 한국전산원, pp. 37-47, 2004년 6월.

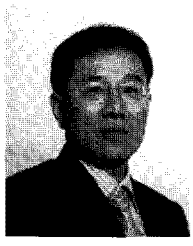
〈著者紹介〉



이 정 훈 (Jung-hun Lee) 정회원
1996년 2월: 숭실대학교 전자계산학과 졸업
2011년 2월: 고려대학교 정보보호대학원 석사
2000년 5월~현재: 금융감독원 선임조사역
〈관심분야〉 정보보호정책, 금융보안, IT보안정책



박 석 훈 (Seok-hoon Park) 정회원
2009년 9월~현재: 고려대학교 정보보호대학원 박사과정
2003년 8월~현재: (주)신세계 I&C Risk Manager
〈관심분야〉 정보보호정책, 디지털프라이버시, 기업보안



임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 원장 및 정보보호기술연구원 원장,
금융보안연구원 보안전문기술위원회 위원장,
검찰청 디지털수사자문위원회 위원장,
행정안전부 정책자문위원회 위원,
경찰청 정보통신위원회 자문위원 등
〈관심분야〉 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등