韓國IT서비스學會誌
第19卷 第1號
2020年 2月, pp.37-53

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2020.19.1.037

개인정보 손해배상책임 보장제도의 쟁점과 과제

이수연* · 권헌영**

Issues and Tasks of Personal Information Protection Liability Insurance

Suyeon Lee* · Hun-Yeong Kwon**

■ Abstract ■

Today, our society is exposed to cyber threats, such as the leakage of personal information, as various systems are connected and operated organically with the development of information and communication technology. With the impact of these cyber risks, we are experiencing damage from the virtual world to the physical world. As the number of cases of damage caused by cyber attacks has continued to rise, social voices have risen that the government needs to manage cyber risks. Thus, information and telecommunication service providers are now mandatory to have insurance against personal information protection due to amendment of "the Act on Promotion of Information and Communication Network Utilization and Information Protection". However, the insurance management system has not been properly prepared, with information and communication service providers selecting the service operators based on sales volume rather than selecting them based on the type and amount of personal information they store and manage. In order for the personal information protection liability insurance system to be used more effectively in line with the legislative purpose, effective countermeasures such as cooperation with the government and related organizations and provision of benefits for insured companies should be prepared.

Thus, the author of this study discuss the current status of personal information protection liability insurance system and the issues raised in the operation of the system. Based on the results of this analysis, the authors propsoe tasks and plans to establish an effective personal information protection liability insurance system.

Keyword : Protection of Personal Information, Cyber Liability Insurance, Personal Information Protection Liability Insurance, Data Protection

Submitted : November 4, 2019 1st Revision : December 16, 2019 Accepted : December 18, 2019

* 고려대학교 정보보호대학원 정보보호학과 석사과정
** 고려대학교 정보보호대학원 교수, 교신저자

1. 서 론

자본주의 경제의 발달과 산업사회로 들어오면서 사물인터넷, 인공지능 등의 신기술로 인해 인류사회는 편리함을 추구할 수 있게 되었다. 그러나 그 부작용으로 사회구조적인 위험을 비롯하여 과거와는 비교할 수 없을 정도의 다양한 위험과 사고가 발생하고 있고, 이에 따른 피해자 구제의 필요성이 어느 때보다도 강조되고 있다. 피해자에 대한 가해자의 책임, 특히 기업의 책임은 엄청나게 강화되고 있으며, 이로 인해 자력만으로 손해를 배상하기 어려운 기업들이 존폐 위기에 처하는 사례 또한 발생되고 있다(금융보안원, 2017). 이러한 배경 하에 기업의 책임을 보험자에게 전가함으로써 손해배상책임 부담으로 인한 가해자의 경제적 어려움을 극복 또는 완화하고, 신속한 피해자 구제가 이루어질 수 있도록 하는 책임보험이 여러 분야에 걸쳐 발달하게 되었다(박세민, 2017).

오늘날, 정보통신기술의 비약적인 발전과 함께 새롭게 출현한 사이버 위험은 금융·국방·의료 등 분야를 뛰어넘는 신·변종 랜섬웨어 공격, 정치적 목적의 해킹, 기업정보 및 개인정보 유출 등 공격의 범위와 수단을 확산시켜나가고 있으며, 가상세계를 벗어나 실제 물리적인 세계에서까지 피해를 발생시키고 있다(Talesh, 2017). 또한, 일반대중 및 기업에 주는 거대 위험의 발생 빈도고 계속해서 높아지고 있으며, 막대한 사회적 비용을 발생시키고 있어 디지털 경제를 기반으로 하는 4차 산업혁명의 방해요소로도 작용되고 있다(최우석, 2017).

이에 정부는 2019년 6월 사이버 위험에 대한 현실적인 대응과 국민의 안전을 위하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 개정하였다. 또한, 기업들의 사이버 위험에 대한 인식과 개인정보의 중요성을 높여 안전한 개인정보보호 체계를 마련하고자 정보통신서비스 제공자 등을 대상으로 '개인정보 손해배상책임 보장제도'를 시행하게 되었다. 하지만 제도 시행에 앞서 사적 자치의 원칙을 제한하면서까지 보험 가입을 강제해야 할 필요성이 있는지에 대한 논란이 일부 불거져 왔으며, 보험 상품 개발 과정에서의 소통 부재, 사전 연구 부족 등으로 인한 상품 준비 및 관리체계 미흡 등 여러 문제가 지적되어 왔음에도 불구하고 이를 완벽히 해소하지 못한 채 법률에 의해 가입 의무화 제도가 시행되었다(임준 외, 2018). 개인정보 손해배상책임 보장제도가 입법취지에 맞춰 더욱 유용하게 활용되기 위해서는 정부와 유관단체의 협력, 보험가입 기업에 대한 혜택 마련 등 실효성 있는 대책방안이 마련되어야 한다. 이에 본 논문에서는 개인정보 손해배상책임 보장제도가 무용지물의 정책성 보험으로 운영되지 않도록 제도 운영 현황을 살펴보고, 실효성 있는 개선방안을 마련해보고자 한다.

논문의 구성은 다음과 같다. 제 2장에서는 개인정보 손해배상책임 보장제도의 도입취지 및 주요내용 등 제도의 이론적 배경에 대하여 살펴볼 것이며, 제 3장에서는 본 제도의 운영 현황과 문제점을 살펴본다. 제 4장에서는 실효성 있는 개인정보 손해배상책임 보장제도 정립을 위한 개선방안에 대하여 고찰해보며, 제 5장에서 지금까지의 논의를 정리하고, 본 제도가 나아가야 할 방향에 대하여 논의해보면서 본 논문을 마무리한다.

2. 개인정보 손해배상책임 보장제도의 이론적 배경

2.1 개인정보 유출사고에 대비한 보험의 필요성 대두

제4차 산업혁명 시대로 접어들면서 우리는 사람과 사물, 공간과 데이터 등 모든 것이 서로 연결되어, 정보가 생성·수집·공유·활용되는 세계에 살고 있다. 여러 시스템이 서로 유기적으로 연결되어 동작하게 됨으로써 사이버 위험요인 또한 복잡하게 얽혀져 다양하고 고도화된 사이버 공격이 발생되고 있다(Camillo, 2017). 이에 피해자 구제와 개인정보보호의 중요성이 인식되기 시작하면서, 정부는 개인정보보호법, 정보보호 강화대책 등 여러 가지 정책과 법률

〈표 1〉 국내 개인정보 유출사고 현황

사고연도	기업	내용	손해배상액 및 행정제재
2012	KT	1,170만 건 개인정보 유출	- 과태료 1,500만 원 - 배상책임 없음
2014	홈플러스	700만 건 개인정보 유출	- 과징금 4억 3,500만 원 - 인당 10만 원 배상
2014	카드3사	1억400만 명 개인정보 유출	- 3개월 영업정지 - 과태료 600만 원 - KB국민카드 인당 10만원 배상
2016	인터파크	2,540만 건 개인정보 유출	- 과징금 44억 8,000만 원 - 과태료 2,500만 원
2017	여기어때	99만 명 개인정보 유출	- 과징금 3억 100만 원 - 과태료 2,500만원
2017	하나투어	42만 명 개인정보 유출	- 과징금 3억 2,725만 원 - 과태료 1,800만 원

개정을 통하여 개인정보 피해사고 대응방안을 강구하였다. 하지만, 날로 진화해가는 해킹기술과 사이버 위험으로 인해 개인정보 유출사고는 계속해서 발생되고 있으며, 그 피해액 또한 증가하고 있다(송은지 외, 2019).

<표 1>에서 확인할 수 있듯이, 금융회사・대기업 중심의 사이버 공격이 이루어져 왔던 과거와는 달리 최근에는 기업 규모와 무관하게 다양한 인터넷 서비스를 제공하는 기업들에 대한 공격이 이루어지고 있음을 확인할 수 있다(IBM Security, 2019). 특히, 전자상거래를 제공하는 기업에 대한 사이버 위협이 날로 증가하고 있으며, 신생 및 중소기업에 대한 사이버 공격이 60% 이상을 차지하는 것으로 확인되었다(Trang, 2017). 이처럼 개인정보 유출사고는 다른 유형의 피해사고와는 달리 한 번의 사고로 다수의 피해자가 발생할 수 있는 위험성을 내포하고 있다. 또한, 시・공간의 제약이 없는 인터넷의 특성 때문에 개인정보 피해는 국외에서도 발생될 수 있으며, 다양한 확대손해를 유발할 수 있다(진대화, 2014). 이처럼 전 세계적으로 사이버 위험사고와 개인정보 유출사고가 계속해서 발생함에 따라 미국, 유럽, 일본 등의 해외 기업 및 국가기관에서는 사이버 위험관리의 수단으로 사이버 보험을 장려하고 있으며, 해마다 사이버 보험 시장의 규모가 계속해서 커지고 있는 것을 확인할 수 있다(유진호, 2018).

국내의 경우에도 다양한 형태로 빈번하게 발생되고 있는 개인정보 유출사고로 인해 개인정보보호의 중요성이 높아지면서 정보유출 피해자 구제를 위하여 「신용정보의 이용 및 보호에 관한 법률」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「개인정보보호법」상 법정・징벌적 손해배상제도를 도입하여 시행하고 있다. 본 제도를 통해 개인정보 유출로 인해 피해를 입은 정보주체는 개인정보 수집・처리・제공하는 자에게 손해배상을 청구할 수 있게 되었다. 하지만, 전반적으로 원인된 사실과 발생한 손해 사이에 인과관계에 대한 입증을 정보주체인 피해자에게 부담하고 있어 손해배상을 받을 수 있는 경우가 매우 제한적인 것이 현재의 상황이다. 또한, 실제로 법정손해배상제도를 활용하여 기업을 상대로 손해를 청구하였으나, 인과관계에 대한 입증의 어려움으로 결과적으로 패소한 경우가 많으며, 승소한 경우에도 소액의 손해배상액만 산정된 경우가 대다수이다(홍준호 외, 2019). 이렇듯, 현재 우리나라의 경우에는 법정・징벌적 손해배상제도를 통하여 정보유출 기업에 대한 책임을 강하게 지우지 못하고 있으며, 피해를 입은 정보주체를 전혀 구제하지 못하고 있어 실질적인 보호방안이 수립되어야 할 필요성이 있다.

이처럼 오늘날 법정 · 징벌적 손해배상책임, 무과실책임주의 등의 개념이 등장하면서 기업의 민사책임이 강화되었고, 이에 따라 배상의무자인 기업의 경제적 부담과 손실이 증대되었다. 이에, 피해자의 구제에 만전을 기할 수 있는 책임보험제도가 각광을 받아 위험의 종류에 따라 다양한 책임보험이 개발 · 운영되고 있다. 법률로 가입이 강제되는 자동차손해배상책임보험, 원자력손해배상책임보험, 근로자재해보상보험, 재난배상책임보험 등이 대표적인 예이다(김영국, 2015). 또한, 정보통신기술의발전과 함께 사이버 공격 · 사고가 계속해서 발생되면서 사이버 위험관리방안으로서 보험제도를 활용하기 위한 움직임이 확산되었다. 타 산업에 비해 사이버 사고로 인한 손실이 더 크게 발생될 수 있는 금융 산업을 시작으로 「전자금융거래법」, 「신용정보의 이용 및 보호에 관한 법률」에 따른 의무보험제도가 시행되었다. 아울러, 최근에는 정보통신서비스 제공자 등으로부터 유출된 개인정보 또한 폭발적으로 증가함에 따라 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」개정을 통해 '개인정보 손해배상책임 보장제도'가 도입되면서 개인정보 유출사고에 대비하기 위한 필수제로서 인식되기 시작하였다(이혜은, 2017).

2.2 개인정보 손해배상책임 보장제도의 도입배경 및 주요내용

2.2.1 개인정보 손해배상책임 보장제도의 도입배경

4차 산업혁명의 확산에 따라 인터넷 기반의 연결성 확대로 인해 기업의 주요 자산 및 정보 유출 등 사이버 사고가 지속적으로 발생하고 있다. 지난 2017년 암호화폐거래소 빗썸 직원의 개인용 PC가 악성프로그램에 노출되면서 해당 PC에 저장되어 있던 고객 개인정보 약 3만 1,000건이 유출되었으며, 유출된 정보를 통해 약 200회에 걸쳐 고객이 보유한 암호화폐 70억여 원이 탈취되는 사건이 발생되었다. 같은 해, 숙박중개업체 여기어때 또한 대규모 고객정보 유출사고가 발생하면서 이용자의 숙박예약 정보 32만 9,210건과 회원정보 17만 8,625건이 유출되었다(방송통신위원회, 2017). 아울러, 개인정보침해 신고센터에 2018년 한 해 동안 접수된 개인정보침해 신고 · 상담 건수는 총 164,497건으로 2017년도 총 접수건수 105,122건에 비하여 56.4%가 증가한 것으로 확인되었다(개인정보보호위원회, 2019). 이처럼 정보통신서비스를 제공하면서 방대한 고객 개인정보를 다루고 있는 기업들이 많아지면서 대량 개인정보 유출 사태가 계속해서 발생되고 있다. 과거에는 대기업 중심의 공격이 이루어졌으나, 최근에는 기업 규모와 무관하게 사이버 사고가 발생됨에 따라 사이버 위험에 대한 기업과 국민들의 불안감이 계속해서 높아져가고 있다.

〈표 2〉 연도별 개인정보침해 신고 및 상담 접수 현황

구분	신고	상담	계
2012	2,058	164,743	166,801
2013	2,347	175,389	177,736
2014	2,992	155,908	158,900
2015	2,316	149,835	152,151
2016	1,559	96,651	98,210
2017	1,249	103,873	105,122
2018	1,325	163,172	164,497

이에 정부는 개인정보 보호방안으로 정보유출기업에 대한 과징금, 과태료 등의 행정처분을 부과하여 기업이 엄격하고 세밀하게 고객 개인정보를 관리하도록 하고 있다. 실례로, 2016년 5월 발생한 인터파크 개인정보 유출사고를 대표적인 예로 들 수 있다. 당시, 고객 개인정보 2,540만여 건이 APT 공격으로 인해 유출되면서 과징금 44억 8,000만 원, 과태료 2,500만 원과 시정명령이 내려지면서, 개인정보 유출사고 중 최대 금액의 과징금이 부과되었다(방송통신위원회, 2016). 이에 인터파크는 방송통신위원회의 행정처분이 지나치게 과도하다며 불복 소송을 제기하였으나, 법원은 "개인정보보호법과 정보통신망법 등이 개정되면서 과징금 부과 기준이 크게 강화되었고, 기업의 기술적 · 관리적 책임 소홀이 인정된다."며 인터파크에 대해 1심 패소 판결(서울행정법원 2018.7.5. 선고 2017구합53156 판결)을 내렸다.

아울러, 2.1절에서 살펴보았듯이 현재 「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」에서 법정 및 징벌적 손해배상책임제도를 규정하여 정보유출 피해자가 개인정보보호 의무를 다하지 못한 기업에 대하여 손해배상을 청구할 수 있도록 하고 있다. 하지만 전반적으로 원인된 사실과 발생한 손해 사이의 인과관계에 대한 입증을 피해자인 정보주체가 부담하고 있음에 따라 실제로 손해배상을 받을 수 있는 경우가 극히 제한적이다(전승재, 2018).

나날이 신·변종 악성 프로그램 등이 대거 등장하고, 개인정보 유출 경로가 다양화됨에 따라 정보유출 사고가 대규모인 경우가 많아 유출사고 건 별로 정보통신서비스 제공자 등이 부담해야 하는 배상액이 클 수밖에 없는 실정이다. 1인 당 피해배상액이 적은 액수라 할지라도 다수의 피해자가 정보유출사고로 인해 발생하기 때문에 총 배상액은 기업이 감당하기 어려운 수준이다. 이 때문에 상대적으로 자금 여력이 충분한 대기업에 비해 신생 및 중소기업의 경우에는 독자적으로 사고 대응 비용을 모두 부담하기 힘들다는 점에서 보험제도를 활용하는 방안이 논의되기 시작하였다(임준, 2019). 정보통신망을 이용하여 통신·쇼핑 등 생활밀접 분야의 비즈니스를 수행하는 사업자들이 많아지고, 고객 개인정보를 다루는 온라인 기업의 수가 증가함에 따라 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 일부 개정하면서 '개인정보 손해배상책임 보장제도'를 시행하게 되었다.

〈표 3〉 유출 사고 신고 현황

(2017년 12월 말 기준)

구분	유출 기관(업체) 수	유출 건수
공공기관	14	1,990,000
민간 기업	67	130,547,000
총계	81	132,537,000

2.2.2 개인정보 손해배상책임 보장제도의 주요 내용

개인정보 손해배상책임 보장제도는 2018. 6. 12. 법률 제15628호로 신설된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제32조의3에 의해 도입되었다. 본 규정에 따라 개인정보보호 배상책임보험에 가입해야 하는 대상자는 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 1,000여 명 이상이며, 매출액이 5,000만 원 이상인 정보통신서비스 제공자 및 그로부터 개인정보를 제공받는 자로 한정된다. 반면, 보유하고 있는 이용자 개인정보의 양이 적은 사업자의 경우에는 개인정보 유출 등 사이버 사고 발생 시 피해 및 배상액의 규모가 상대적으로 크지 않다는 점을 고려하여, 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 1천여 명 미만인 사업자에 대해서는 보험 가입을 의무화하지 않고 있다. 또한, 신생기업 등과 같이 매출액이 거의 없거나 미미한 경우에는 사실상 규제 준수가 어려운 점을 고려하여 매출액이 5천만 원 미만인 정보통신서비스 제공자 등에 대해서는 '개인정보 손해배상책임 보장제도'의 적용대상에서 제외하였다.

개인정보보호 배상책임보험 또는 공제에 가입하거나 준비금을 적립할 경우 최저가입금액은 사업자별 이용자 수와 매출액에 따라 최저 5,000만 원에서 최고 10억 원으로 차등 설정된다. 다만, 다른 법률에 따라 가입된 보험이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 손해배상책임의 이행을 보장하는 경우에는 손해배상 보장조치를 이행한 것으로 인정하여 중복 가입 부담을 완화하고 있다.

〈표 4〉 개인정보 손해배상책임 보장제도의 보험가입·준비금 적립 기준

적용대상 사업자의 가입금액 산정요소		최저가입금액 (최소적립금액)
이용자 수	매출액	
100만 명 이상	800억원 초과	10억원
	50억원 초과 800억원 이하	5억원
	5천만명 이상 50억원 이하	2억원
10만 명 이상 100만 명 이하	800억원 초과	5억원
	50억원 초과 800억원 이하	2억원
	5천만명 이상 50억원 이하	1억원
1천명 이상 10만 명 미만	800억원 초과	2억원
	50억원 초과 800억원 이하	1억원
	5천만명 이상 50억원 이하	5천만원

개인정보보호 배상책임보장제도의 적용 대상 기업은 개인정보보호 배상책임보험 가입을 대신하여 사고 발생 시 사용할 유출사고 책임이행 준비금을 적립할 수 있다. 이때 준비금은 보험 보상한도에 준하는 금액이어야 하며, 임의적립금으로 적립하여 주주총회 결의 등을 통해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제32조의3의 의무이행을 위한 것임을 명확히 하여야 한다. 만약 보험 의무가입 대상자임에도 불구하고 보험 또는 공제 가입, 준비금 적립 등의 필요한 조치를 취하지 아니하는 경우에는 법률 위반행위 횟수와 무관하게 2천만 원의 과태료를 부과하여야 한다(방송통신위원회, 2019).

3. 개인정보 손해배상책임 보장제도의 현황 및 문제점

3.1 개인정보 손해배상책임 보장제도의 운영 현황

개인정보 유출사고 발생 시 피해자에 대한 손해배상 책임 이행을 보장하기 위해 도입된 '개인정보 손해배상책임 보장제도'는 지난 6월 13일부터 시행되었다. 하지만, 구체적인 대상범위, 준비금 적립 방법 및 시기, 업종 관련 유무, 피해발생 시 보험금 지급 과정 등 제도 운영대책이 제대로 수립되어 있지 않은 채 시행되면서 여러 혼란을 불러일으켜 왔다. 또한, 제도 도입 과정에서 소관부처, 보험사 그리고 정보통신서비스 사업자 등과의 논의가 부족했던 탓에 상품 개발이 늦어지면서 정부는 현장 혼란을 최소화하고 제도 도입 안착을 위해 금년 말까지 계도 기간을 운영하겠다는 방침을 내렸다.

보험업계는 소관부처, 정보통신서비스 사업자 등과의 논의 끝에 지난 7월 15일을 시작으로 의무보험 상품인 '개인정보보호 배상책임보험(Ⅱ)'을 출시하였다. 아울러, 8월 8일에는 공제상품으로는 유일하게 소프트웨어공제조합이 '개인정보 손해배상책임 공제상품'을 출시하였다(한국정보산업연합회, 2019). 현재까지 출시된 보험 상품을 살펴보면, 소유·사용·관리하는 개인정보의 우연한 유출·분실·도난·위조·변조 또는 훼손으로 인한 피보험자의 법률상 손해배상금과 소송비용 및 변호사 비용 등을 기본으로 보상하고 있는 것으로 확인된다. 또한, 특별약관으로 보장하고 있는 손해의 경우에는 회사별로 조금씩 상이한 것으로 확인된다. 주로 기업 평판 회복을 위한 홍보비용·전문가 컨설팅 서비스 비용 등의 위기관리컨설팅비용, 사고 원인 조사비용·콜센터 구축비용·사죄광고 비용 등의 위기관리실행비용, 신용정보유출 등으로 인한 손해보장 및 과징금 보장 등에 대하여 특별약관으로 규정하고 있다. 의무 가입 대상인 정보통신서비스 제공자 등이 보험 상품에 가입하고자 하는 경우에는 보험사별로 준비된 가입 질문서를 작성하여 보험료 견적 산출을 받아야 한다.

반면, 개인정보 손해배상책임 보장제도에 따라 가입 가능한 공제상품의 경우에는 현재까지 소프트웨어공제조합의 공제상품이 유일하다. 공제상품의 경우에는 일반 보험 상품 보험료에 비해 10% 저렴하며, 보험 상품과 동일한 수준의 보험금을 지급하고 있음을 확인할 수 있다. 소프트웨어공제조합의 경우, 상품 출시 이전 3개 손해보험사와 업무협약을 체결하여 제휴한 손해보험사가 공제계약자의 보험금 지급을 보장할 수 있도록 하고 있다. 또한, 온라인 시스템을 구축하여 의무가입 사업자가 안심하고 공제 상품에 가입할 수 있도록 간편한 가입절차를 마련하였다.

한편, 보험업계는 「신용정보법」과 「정보통신망법」에 의한 동시 의무 대상자의 경우 기존의 의무보험 형태인 '개인정보보호 배상책임보험(Ⅰ)'과 함께 신용정보 의무보험 확장담보 특별약관에 가입되어 있는 기업에 대해서만 「정보통신망법」에 따른 손해배상 보장 조치를 이행한 것으로 인정하고 있다. 이처럼 현재 대부분의 손해보험사가 상품구성 및 보험약관 준비절차 등을 거쳐 보험 상품을 줄줄이 출시하고 있으며, 공제상품 또한 함께 출시되면서 개인정보 손해배상책임 보장제도의 적용대상 기업들의 가입 움직임이 확산될 것으로 예상된다.

3.2 개인정보 손해배상책임 보장제도의 문제점

3.2.1 준비금 적립 기업에 대한 관리 문제

현재 정부가 제시한 개인정보 손해배상책임 보장제도에서는 정보통신서비스 제공자가 개인정보 유출로 인한 손해배상책임 이행을 위하여 개인정보보호 배상책임보험에 가입하는 것을 대신하여 사이버 사고 발생 시 사용할 전자금융사고 책임 이행을 위한 준비금을 적립할 수 있도록 하고 있다. 보험 가입과 마찬가지로 정보통신서비스 제공자 등은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」시행령 제18조의2에서 정한 최저가입금액의 기준을 참고하여 준비금을 적립하여야 한다. 아울러, 보험 가입 및 준비금 적립 등 필요한 조치를 취하지 아니하는 정보통신서비스 제공자 등의 경우에는 앞서 살펴본 바와 같이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제76조 제2항 제4호의2에 따라 위반횟수와 상관없이 매회 2,000만 원의 과태료를 부과하여야 한다.

반면, 관련 법 및 시행령을 살펴보면 보험 가입을 하지 않고 준비금을 적립한 정보통신서비스 제공자 등에 대한 관리·감독 방안이 제대로 수립되어 있지 않은 것을 확인할 수 있다. 뿐만 아니라 지난 6월 공개된 방송통신위원회의 '개인정보 손해배상책임 보장제도 안내서'에 따르면, 보험 가입을 대신하여 준비금을 적립한 경우에는 이행 여부에 대한 신고 및 보고 의무가 없어 향후 감사 및 이행점검 시 보험증권·회계장부·주주총회 의사록 등이 자료제출 요구 대상이 될 수 있음만을 설명하고 있다(방송통신위원회, 2019).

우리나라는 '개인정보 손해배상책임 보장제도' 시행 이전부터 사이버 사고에 따른 손해배상책임 이행을 위해 각 분야의 관련 법률에 의해 보험 가입을 의무화해왔다. 특히, 금융기관의 경우 개인정보 유출사고로 인해 정보 유출뿐만 아니라 금전적 피해와 부정거래 등 2차 피해 발생의 우려가 크며 그 범위가 광범위함에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하도록 규정하여 배상책임을 담보하는 보험 등의 가입을 의무화하였다. 하지만 2014년 금융감독원이 국내 주요 금융회사(은행, 생명보험사, 손해보험사, 여신전문금융사, 증권사 등) 총 78개의 기업을 대상으로 배상책임보험 가입 현황을 조사한 결과, 대부분의 금융기관은 「전자금융거래법」 및 「전자금융감독규정」상 보험 보상 한도액 이상의 준비금을 적립하면 된다고 명시하고 있으며, 이행 여부에 대한 신고 및 보고 의무가 없어 보험 가입의 필요성을 크게 느끼지 못하고 있었던 것으로 확인되었다(유진호, 2018). 이에 2016년 정부는 외부 보험사가 지급하는 보험과는 달리 준비금을 적립하는 기업의 경우에는 자체적으로 관리·지급함에 따라 신속한 보상이 이루어지지 못할 우려가 있으므로 「전자금융감독규정」을 일부 개정하여 피해보상이 신속하게 이루어질 수 있도록 준비금을 적립하는 금융회사의 준비금 관리 및 지급과 관련하여 내부 절차를 수립·운영하도록 하였다. 이처럼 준비금 적립 기업의 신고·보고 의무 규정이 부재한 경우, 기업은 준비금 적립을 정보보호 투자가 아닌 단순 비용으로 인식하는 문제가 발생할 수 있다.

일반적으로 준비금은 보험으로 충당하지 못하는 예기치 못한 미예상 손실에 대한 완충 자본의 역할을 한다(김종환 외, 2014). 따라서 개인정보 손해배상책임 보장제도를 시행함에도 불구하고 준비금 적립 기업에 대한 제재 수단이 확립되지 않은 채 운영된다면 손해배상책임을 이행하지 않는 자가 발생할 수 있는 위험성이 있다. 이에 「전자금융거래법」에 따른 금융기관의 보험 가입 의무화 정책을 통해 경험한 문제점을 참고하여 준비금 적립 기업에 대한 제재 방안을 마련하여야 할 것이다.

3.2.2 가입 관리의 체계화 부족 문제

보험가입 대상에 대한 관리와 점검 시스템의 부재로 인해 개인정보 손해배상책임 보장제도에 대한 실효성 확보가 어려워지는 문제점이 발생될 수 있다. 이러한 문제를 해결하기 위해서는 의무가입 대상 기업을 합리적으로 규율할 수 있는 일관된 체계가

필요하다. 하지만 현재 우리나라의 개인정보보호법제의 경우, 일반법적 성격의 「개인정보보호법」 이외에 정보통신, 금융, 의료 등의 개별영역에서 개인정보 처리를 규율하는 다양한 개별법이 산재해 있다. 일반법 성격의 「개인정보보호법」의 경우에는 행정안전부가, 「정보통신망법」의 경우에는 방송통신위원회가 담당하고 있으며, 이외에 금융 관련 법률의 경우에는 금융위원회가 담당하는 등 개별법과 영역별로 담당기관이 다양하게 존재한다(강철하, 2018). 이처럼 개인정보보호 관련 법률이 분야·영역별로 산재되어 일관적인 대응이 어려운 상황이며, 수범자에 대한 이중 규제의 위험이 야기될 수 있다.

〈표 3〉 주요 영역별 개인정보보호 개별법률

분류	관련 분야	법률명	
일반법	-	개인정보보호법	
개별법	공공부문	전자정부법	
		공공기관의 정보공개에 관한 법률	
		공공기록물 관리에 관한 법률	
		민원 처리에 관한 법률	
		보안업무규정(대통령령)	
	민간부문	정보통신 분야	정보통신망 이용촉진 및 정보보호 등에 관한 법률
			클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률
			통신비밀보호법
			위치정보의 보호 및 이용 등에 관한 법률
			정보통신기반 보호법
			정보통신사업법
		금융 분야	전자금융거래법/ 전자금융감독규정
			신용정보의 이용 및 보호에 관한 법률
			금융실명거래 및 비밀보장에 관한 법률
			보험업법
			자본시장과 금융투자업에 관한 법률
		상거래 분야	전자문서 및 전자거래기본법
			전자상거래 등에서의 소비자보호에 관한 법률

실제로 하나의 기업이라고 하더라도 전자금융거래, 정보통신서비스 등 다양한 사업을 영위하는 사업자가 많아지면서 사업의 성격에 따라 「개인정보보호법」상의 '개인정보처리자', 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상의 '정보통신서비스 제공자' 등의 법적 지위를 동시에 겸유하고 있다. 이에 복수의 법률에 의한 보험가입 의무의 중복 문제가 발생하고 있으며, 법 준수에 있어 혼란을 겪고 있다(강철하, 2018). 모바일지급결제서비스 사업자의 경우를 통해 현재의 문제점을 확인해 볼 수 있다. 대다수의 모바일지급결제서비스 사업자는 이미 「전자금융거래법」에 의한 의무보험인 '전자금융거래 배상책임보험'에 가입되어 있으며, 이와 함께 개인정보 유출사고에 대비하여 '개인정보유출 배상책임 특별약관'에 가입하고 있는 상황이다. 하지만 최근 도입된 '개인정보 손해배상책임 보장제도'가 시행됨에 따라, 보험가입 대상자인 모바일지급결제서비스 사업자는 기존에 가입한 '개인정보유출 배상책임 특별약관'에서 보상하는 손해가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제32조 및 제32조의2에 따른 손해배상책임을 담보(보상)하는지의 여부를 자체적으로 보험사에 확인해보아야 하며, 보장범위를 충족하지 않는 경우에 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정한 의무보험(개인정보보호 배상책임보험 Ⅱ)을 추가로 가입하여야 하는 상황이다. 이처럼 전자금융거래, 정보통신서비스 등을 동시에 제공하는 사업자에 대하여 담당하는 소관부처가 제각기 달라 보험 가입자에 대한 관리의 체계성 문제가 제기될 수밖에 없는 실정이다. 이처럼 가입대상 기업들에 대한 보험가입 현황 분석의 어려움 등의 문제가 해결되지 않는 이상 보험 가입자에 대한 관리체계 및 시스템을 구축하기 어려워진다. 이러한 문제점을 해결하기 위하여 방송통신위원회·금융위원회 등의 소관부처는 보험업계와 협업하여 가입대상 기업들의 보험가입 현황 및 손해발생 현황 등을 파악할 수 있어야 한다.

3.2.3 일부 사업자에 대한 보험계약 인수 거부 문제

신속하고 원활한 피해 복구와 피해자 보상을 위해 도입된 '개인정보 손해배상책임 보장제도'가 현재 제한된 대상을 위주로 시행되고 있어 주요 정보통신서비스에 대한 정보유출 위험에 대하여 보험 사각지대가 발생할 수 있으며, 포괄적인 피해 구제 및 복구가 이루어지지 못할 위험성이 있다. 현재 본 제도에 의해 출시된 보험 상품을 살펴본 결과, 포탈·암호화폐거래소·신용정보집중기관 등 일부 사업자에 대하여 가입가능 대상에서 제외하고 있으며, 인수가 불가능한 업종으로 규정하고 있다. 이처럼 개인정보 손해배상책임 보장제도 전용 보험 상품에서 제외되는 정보통신서비스 제공자 등이 존재함에 따라 개인정보 유출사고 발생 시 보상공백이 존재할 위험성이 있다. 실제로 포탈·암호화폐거래소 등의 경우에는 사이버 사고 발생 시 개인정보 유출 사태를 넘어 사회적·경제적 손실이 크게 발생될 수 있어 보험제도를 통한 위험관리의 필요성이 수년 전부터 제기되어 왔다(방송통신위원회, 2019). 또한, 2017년 12월 암호화폐거래소 유빗의 파산신청 사건을 계기로 방송통신위원회는 '암호화폐거래소에 대한 사이버 보안 및 개인정보보호 체계 강화 추진 방안'을 발표하며 개인정보 유출시 이용자의 피해를 효율적으로 구제하기 위해 '손해배상책임보험·공제 가입 의무화 제도'를 도입하겠다며 정보통신서비스 제공자 등에 대한 개인정보보호 배상책임보험 가입 의무화의 필요성을 계속해서 주장해왔다(방송통신위원회, 2017). 이러한 논의를 거쳐 신속하고 원활한 피해 복구와 피해자 보상을 위해 현재의 개인정보 손해배상책임 보장제도가 도입되었다. 하지만 제한된 가입대상자를 위주로 시행되고 있기 때문에 포탈·암호화폐거래소 등에 대한 개인정보 유출사고에 대해서는 보험 사각지대가 발생하여 포괄적인 피해자 구제 대책이 이뤄지지 못할 가능성이 존재한다.

현재 개인정보 손해배상책임 보장제도에 따라 보험에 의무적으로 가입해야 하는 사업자는 업종에 관계없이 인터넷·모바일 상에서 영리를 목적으로 웹사이트·앱·블로그 등을 운영하며 이용자(고객) 정보를 보유한 정보통신서비스 제공자 등을 말한다. 하지만 위에서 살펴본 바와 같이, 일부 정보통신서비스 제공자 등에 대하여 보험회사들로부터 보험계약이 인수 거부되고 있다. 보험회사들이 사이버 사고 발생 위험이 높은 고위험자에 대한 보험계약을 계속해서 거부함에 따라 이에 대한 사업자들의 민원이 발생할 수밖에 없을 것이다.

국내 대형 암호화폐거래소의 경우, 피싱·스미싱·랜섬웨어 등 사이버 위험으로부터 사업상 손실 및 이용자 보호를 위해 자체적으로 손실비용을 보장해줄 수 있는 내부보상안을 만들거나 내부 준비금을 적립해두도록 하고 있는 것으로 확인되었다. 또한, 일부 대형 암호화폐거래소의 경우에는 보험회사와 '맞춤형'으로 제작한 보험 상품에 가입하고 있는 것으로 알려졌다. 반면, 자금여력이 부족한 규모가 작은 암호화폐거래소의 경우에는 보험을 활용하여 사이버 위험에 대비하려 함에도 불구하고 보험회사의 인수 거부로 인해 '개인정보 손해배상책임 보장제도'를 준수함에 있어 큰 어려움이 발생할 수 있다. 이와 같은 문제는 다른 분야의 강제가입 형태의 정책성 보험에서도 찾아볼 수 있다. 자동차손해배상보장법 등 일부 법률을 제외하고는 보험회사의 보험 인수 거부 금지규정의 부재로 인해 수렵보험, 수상레저보험 등 손해율이 높은 분야의 경우 계약거절 사례가 지속적으로 발생하고 있는 것으로 알려졌다(보험개발원, 2015).

이러한 문제점을 해결하기 위하여 소관부처는 보험회사의 계약 거절 사례에 따른 민원 발생과 본 제도의 입법 취지인 피해자 보호에 문제가 발생할 수 있으므로 이에 대한 해결책을 강구하여야 한다.

4. 실효성 있는 개인정보 손해배상책임 보장제도를 위한 개선과제

4.1 보험가입 기업에 대한 혜택 제공

사이버 위험 관리 수단으로 도입되는 개인정보

손해배상책임 보장제도의 기반 환경을 조성하기 위해서는 보험 가입자에 대한 관리 및 혜택이 적절하게 이루어져야 한다. 특히, 1,000여 명 이상의 이용자 정보를 저장·관리하고 있는 정보통신 서비스 제공자 등이 가입 대상에 포함되면서 대기업뿐만 아니라 온라인 쇼핑몰, 핀테크 기업, 스타트업 등의 신생·중소기업 또한 보험에 의무적으로 가입하여야 한다. 규모가 크지 않은 중소기업의 경우에는 사이버위험관리 역량 측면에서 대기업과 상당한 차이가 있을 수밖에 없다. 따라서 개인정보 손해배상책임 보장제도 활성화 전략 수립 시 대기업과는 차별적인 접근이 필요하다고 생각된다(임준, 2019). 대다수의 중소기업의 경우에는 사이버 위험에 대한 이해도가 낮으며, 개인정보보호 필요성에 대한 인식 또한 매우 낮은 편이다. 이에 개인정보 유출위험에 대한 인식이 부족한 중소기업이 본 제도를 통한 보험 가입을 투자가 아닌 단순 비용으로 인식하는 상황이 발생될 수 있으며, 가입을 강제한 정부에 불만과 사회적 불신을 가지게 될 수도 있다.

사이버 위험에 대한 국민의 균형적인 인식과 합리적인 제도 도입에 대하여 선진화된 인식을 제고하기 위해서는 보험에 가입한 정보통신서비스 제공자 등으로 하여금 보험 가입이 메리트가 될 수 있는 사회적 공감대를 형성하는 노력이 필요하다.(오한나, 2019) 미국의 사례를 살펴보면, 2016년 사이버 보험 활성화를 위한 정책으로 보험 가입자에 대한 세금 공제 법안인 「Data Breach Insurance Act」가 발의되었다. 이 법안은 기업이 데이터 침해 보험에 가입하고, NIST의 보안 가이드라인을 준수하는 경우 보험료의 15%에 해당하는 세금 공제 혜택을 부여하는 법안이다(Congress GOV, 2016). 기업으로 하여금 보안을 위한 최선책을 선택하고 사이버 보험 시장의 발전을 장려하기 위한 목적으로 발의된 이 법안은 기업에게 사이버 침해를 방어할 수 있는 보안기준을 제시하였으며, 기업이 비즈니스 보호와 사이버 위협에 대응하기 위해 필요한 역량과 조치를 취하는데 도움이 되도록 하고 있다. 또한 미국의 Beazley 보험사는 보안기업, 법률자문사 등과 협력체계를 구축하여 전 단계에 걸쳐 전문적인 서비스를 제공하며, 사고 대응과 손해 경감 방안을 확보하는데 노력하고 있다(보험개발원, 2019).

금융기관 및 대기업의 경우, 정보유출에 따른 손해배상책임이 커짐에 따라 사이버 위험에 대한 이해 및 대비 계획을 수립하기 위하여 내부 보안조직을 통해 정보보호 교육, 외부 보안 컨설팅을 실시하는 등 사이버 위험 관리를 위해 자체적으로 많은 노력을 하고 있다. 반면, 규모가 작은 중소기업의 경우에는 내부적으로 사이버 위험 관리 조직을 운영하기 어려울 뿐만 아니라 외부 컨설팅 업체와의 파트너십도 약한 편이다. 보험회사의 경우에는 자체적으로 사이버 위험 컨설팅 능력을 보유하고 있지 않으므로 정책당국은 한국인터넷진흥원(KISA)을 통해 위험관리자문단을 꾸려 보험가입 기업이 사이버 위험 관리 능력을 키울 수 있도록 사이버위험관리 자문 등의 혜택을 제공하여야 한다. 최근 중소벤처기업부에서 중소기업 기술보호 역량 수준 강화 및 기술탈취 행위 근절을 통한 공정기술거래 환경 조성을 위해 '중소기업 기술보호 지원사업'을 시행하고 있다(중소벤처기업부, 2019). 한국산업기술보호협회 등 관련 기관들과 협업하여 사전예방부터 피해구제, 인식개선, 제도개선까지 종합적으로 지원하여 기업의 기술보호 역량 수준을 강화할 수 있도록 자문 서비스를 제공하고 있다.

개인정보 손해배상책임 보장제도의 소관부서인 방송통신위원회는 본 제도가 정착할 수 있도록 해외 사례, 다른 분야의 의무보험제도 운영 사례, 다른 부처에서 진행되고 있는 지원사업 등을 참조하여 보험가입 기업에 대한 혜택 제공 방안을 강구하여야 한다. 보험료 할인·세액 공제·정보보호 컨설팅 자문·기술 지원 등 다양한 혜택들이 보험 가입 기업들에게 제공된다면 사고발생률 감소 효과를 볼 수 있을 것이며, 동시에 사고발생률이 낮아지면서 기업과 국가의 사회적 비용 또한 줄어들어 국가 전체적으로 사이버 사고에 대한 리스크가 감소하게 되는 현상을 가져올 것으로 기대된다(유진호, 2018).

4.2 가입자 관리에 대한 제재 및 관리 규정 마련

우리나라의 기업인식은 경쟁사회에서 타 기업보다 경쟁우위를 가지기 위해 기업성장에 많은 초점을 맞추고 있어 정보를 보호하는 활동에는 아직까지도 인색한 상황이다(상명대학교 서울산학협력단, 2013). 또한 기업들이 이익을 창출할 수 있는 정보 활용 측면에서는 투자를 아끼지 않는 반면, 이를 보호하는 정보보호 활동에서는 투자가 이루어지지 않아 정보유출을 예방하기 위한 사이버 배상책임보험 등에 가입하지 않고 대부분의 기업이 준비금으로 대처하고 있는 실정이다. 현재 많은 기업이 기업 자체적으로 적립해 두어 정보보호 관련 사고를 대비하고 있으나 빅데이터, AI 등 정보통신기술의 발달로 활용되고 있는 정보의 범위가 확대되고 있어 개인정보 유출사고 발생으로 인한 피해 손실이 점점 더 커질 것으로 예상된다. 이에 기업별 개별 대응책인 준비금 적립만으로는 정보보호 유출사고에 완벽히 대응할 수 없으므로 보험·공제 가입을 대신한 준비금 적립 방안을 인정하기 보다는 회사가 보안 사고를 상시적 위험으로 인식할 수 있도록 보험에 의한 위험전가와 회사 내부의 준비금 적립이 병행될 필요성이 있다(김종환, 2014).

아울러, 보험·공제를 대신하여 준비금을 적립하고 있는 기업에 대한 관리·감독 방안이 반드시 수립되어야 한다고 생각한다. 최근 개정된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 시행령을 살펴보면 보험 가입을 하지 않고 준비금을 적립한 정보통신서비스 제공자 등에 대한 관리 방안이 수립되어 있지 않은 것을 확인할 수 있다. 이에 개인정보 손해배상책임 보장제도에 따르면 보험에 가입하지 않고 내부적으로 준비금을 적립한 기업의 경우에는 준비금 적립 이행 여부에 대한 신고·보고 의무가 없으므로 정책당국은 보험 및 공제 가입 기업과 동일한 제재 조치를 취하기 어려울뿐더러, 준비금을 적립하여 운영되고 있는 기업의 파악 및 현황 관리가 더욱 더 어려워질 것으로 판단된다. 개인정보 유출사고 발생 시 신속한 정보유출 피해자에 대한 피해 구제를 위해 본 제도가 시행되었으므로, 정책당국은 반드시 준비금 적립 기업에 대한 공평하고 엄격한 관리·감독 방안을 수립하여야 한다. 앞서 살펴보았듯이, 「전자금융거래법」에 의해 개인신용정보를 다루는 금융기관에 대한 전자금융거래 배상책임보험 가입 의무화 제도를 시행하였을 당시에도 현재와 같이 준비금 적립 기업에 대한 관리·감독 문제가 불거졌었다. 이에, 당시 금융당국은 「전자금융감독규정」 제5조 제2항을 신설하여 정보유출 사고에 대한 피해보상이 신속하게 이어질 수 있도록 준비금을 적립하는 금융회사의 경우에는 준비금 관리 및 지급에 관하여 내부 절차를 수립하여 운영하여야 함을 규정하였다.

정책당국은 이러한 금융 분야에서의 정책 경험을 참고하여 준비금 적립 기업에 대한 제재·관리 규정을 신설하는 등의 제도적 조치를 취할 필요가 있다고 생각한다. 이로써 보험·공제 가입을 대신하여 준비금 적립을 하고 있는 정보통신서비스 제공자 등에 대한 파악 및 현황 관리가 가능해질 것이며, 이들에 대하여 보험가입 기업과 동일하게 관리·감독을 할 수 있을 것으로 판단된다. 아울러, 본 제도가 실효성 있는 위험관리 수단으로 자리 잡기 위해서는 보험에 의한 위험전가와 회사 내부의 준비금 적립이 선택적으로 수행되는 것이 아닌 함께 병행될 필요가 있다.

본고에서 제안하는 준비금 적립기업에 대한 제재·관리 규정은 다음과 같다.

〈표 6〉 준비금 적립기업에 대한 제재·관리 규정 제안안

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령
제18조의2(손해배상을 위한 보험 등 가입 대상자의 범위 및 기준 등) ①다음 각 호의 요건을 모두 갖춘 정보통신서비스 제공자 등(이하 이 조에서 "가입 대상 사업자"라 한다)은 법 제32조의3제1항에 따라 보험 또는 공제에 가입하거나 준비금을 적립해야 한다. 1. 직전 사업연도 매출액이 5천만 원 이상일 것 2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일 평균 1천 명 이상일 것
②정보통신서비스 제공자 등(가입 대상 사업자)이 개인정보유출사고 책임이행을 위해 보험 또는 공제에 가입할 때 최저 가입 금액의 기준은 별표1의2와 같다.
③정보통신서비스 제공자 등(가입 대상 사업자)이 개인정보유출사고 책임이행을 위한 준비금을 적립하는 경우에는 별표1의2에서 정한 최저가입(적립)금액의 기준 이상을 보유하고, 책임이행이 신속히 이루어질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야 한다.
④정보통신서비스 제공자 등(가입 대상 사업자)이 보험 또는 공제 가입과 준비금 적립을 병행하는 경우 보험 또는 공제 가입금액과 준비금 적립 금액을 합산한 금액이 별표1의2에서 정한 최저가입(적립)금액의 기준 이상이어야 한다.

4.3 사이버보험관리시스템 구축을 통한 관리 체계 정립

개인정보 손해배상책임 보장제도뿐만 아니라 현행 강제가입 형태의 다른 정책성 보험에서도 문제점으로 나타나고 있는 미가입자에 대처하기 위하여 보험 가입 대상자의 가입 여부, 손해상황 등에 대한 통합관리시스템을 구축하는 것이 필요하다. 현재 시행되고 있는 대부분의 의무보험제도의 경우에는 일정한 체계 없이 시행되면서 보험 종목간의 보상금액 수준이 차이가 나거나, 의무보험임에도 불구하고 미가입자에 대한 처리방안 등의 문제점 등이 다양하게 나타나고 있다. 반면, 일부 의무보험제도에서는 이러한 문제점을 해결하기 위하여 관련 조항을 신설하거나 안내서를 제작하는 등의 노력을 하고 있는 것으로 알려졌다. 대표적으로 자동차 보험의 경우 「자동차 손해보장보험법」 제6조의2에 의거하여 보험가입자 가입관리 전산망을 운영 중이며, 재난배상책임보험의 경우에도 각 지자체간 정보 연계를 위해 보건복지부, 국토교통부 등의 시스템과의 연계를 추진하고 있는 것으로 알려졌다(국민안전처, 2017).

지난 2017년 1월 8일부터 시행된 재난배상책임보험을 살펴보면 정책당국에서 '업무처리절차서'를 발간하여 의무보험 도입배경, 보험가입 대상, 보장위험 및 한도, 과태료 기준 등의 내용을 설명하고 있으며, 손해보험협회와 협업하여 보험 상품 설명, 가입 전 확인사항, 보험사의 연락처 및 홈페이지 현황 등 보험가입 대상자의 이해를 돕기 위해 '재난배상책임보험 길라잡이'를 발간하였다(국민안전처 · 손해보험협회, 2017). 이뿐만 아니라, 담당 부처인 국민안전처는 행정안전부를 통해 가입 대상 시설 정보와 보험개발원의 보험 가입 정보를 국가재난관리시스템(NDMS)을 통해 연계하여 시설 정보와 가입 정보를 매칭하여 미가입자를 추출하고 있다. 재난관리시스템 운영을 통해 현재 국민안전처는 미가입자에 대하여 가입 안내문을 전송하고 있으며, 재난배상책임보험에 대하여 업종별, 보험사별로 구분하여 비교 · 조회하는 등 효율적인 위험관리 체계를 갖추는데 총력을 기울이고 있다.

개인정보 손해배상책임 보장제도가 효용성을 충분히 발휘하기 위해서는 업종별 가입 대상 기업에 대한 현황 파악이 우선되어야 하며, 이들의 보험 가입 여부를 확인하고 보험 미가입자에 대한 제재 · 감독 방안이 함께 구축되어야 한다. 이를 위해 방송통신위원회는 재난배상책임보험 등 다른 분야의 보험 가입 의무화 정책에 대한 관리 · 감독 동향을 참고하여 효율적인 제도 운영방안을 마련하여야 한다. 아울러, 원활한 보험 가입자 관리를 위해 다른 법률에 의해 개인정보 유출 등 사이버 사고에 대비한 보험에 의무적으로 가입하여야 하는 사업자에 대한 파악이 필요하므로 방송통신위원회는 금융위원회 등 다른 부처와의 협업을 통해 관리시스템을 연계하여야 한다.

현재 유럽연합 · 일본 등 일부 주요국의 현황을 살펴보면, 개인정보제도의 일원화를 위한 법 · 제도 환경을 구축하고 있는 것으로 확인된다(김동영, 2018). 유럽연합의 경우, 공통의 지침을 바탕으로 각기 다른 법제를 운영했던 과거와는 달리 회원국간 합의에 기초한 공통의 상호보완적인 개인정보제도를 운영하고 있다. 또한, 일본의 경우에도 개인정보보호법 개정을 통해 개인정보보호위원회를 신설하고 민간과 정부를 모두 포괄하는 법체계를 정립하여 개인정보 거버넌스의 단순화 · 일원화를 통해 제도 발전의 추진력을 확보하고 있다. 반면, 한국의 현행 정보보호법제는 복잡한 법제지형을 가지고 있어 정보보호에 관한 대응체계 및 방식에 있어 혼란을 가중시키고 있다(심우민, 2018). 이에 최근 분산되어 있는 개인정보보호 법령과 감독기구에 대한 체계적인 정비를 위한 논의가 활발히 이뤄지고 있다. 따라서 개인정보 손해배상책임 보장제도 또한 효과적인 위험관리적 대응체계를 마련하는데 일조할 수 있도록 개인정보보호 배상책임 뿐만 아니라 전자금융거래 배상책임보험 등 다른 개인정보보호 법률에 의한 사이버 보험이 함께 관리될 수 있도록 사이버보험관리시스템을 구축하여

운영할 필요가 있다. 보험관리 전산망을 통해 효율적인 위험관리 체계가 구축될 수 있다면 본 제도가 개인정보의 보호 및 데이터 경제 사회의 정착에 크게 기여할 수 있을 것이다.

4.4 개인정보보호기금 도입을 위한 근거 규정 마련

「정보통신망법」제32조 제2항, 제32조의2에 따라 법정 손해배상제도 및 징벌적 손해배상제도가 도입되었음에도 불구하고 기업의 배상능력이 부족하여 이용자가 손해배상을 청구해도 피해구제가 어려운 경우가 대다수이다. 이에 정부는 정보유출 사고기업의 배상자력을 마련해주고, 피해자에 대한 현실적인 보상이 가능할 수 있도록 '개인정보 손해배상책임 보장제도'를 도입하였다. 하지만 전자금융거래 배상책임보험 등 이미 다른 분야에서 시행되고 있는 사이버 보험 운영 현황을 검토해 본 결과, 대부분의 보험가입 기관·기업이 법에서 정해진 최소한의 보험에 가입하고 있어 피해자에 대한 확실한 보상이 이뤄지기 힘든 구조를 띠고 있다(유진호, 2018). 이에 따라 정부는 개인정보 유출사고가 빈번하게 발생하지 않도록 사업자의 책임을 강화하고, 의무보험제도 뿐만 아니라 이용자에 대한 피해구제를 실질적으로 지원하는 기금 운영 등의 정책도 함께 고려할 필요가 있다. 실제로 개인정보보호기금 설치·운용에 대한 필요성 검토와 요구가 시민단체와 연구기관을 중심으로 이뤄지고 있다.

현재 정부는 이용자의 개인정보를 유출한 사업자의 정보보호 인식, 개인정보 보호조치 의무 등에 대한 책임을 강화하기 위해 과징금·과태료·벌금(형사벌)의 세 가지 제재수단을 도입해 시행하고 있다. 하지만, 이러한 정부의 행정처분이 오히려 대규모 정보유출 사고를 조장하고, 기업들이 과징금 제도라는 방패를 통해 배상책임에서 숨어버리는 형태를 취하고 있다. 또한, 개인정보보호에 대한 정책을 총괄하는 방송통신위원회의 2019년 예산 2천 569억 원 가운데 개인정보보호와 안전한 활용에 102억 원, 불법 스팸 대응체계 구축에 31억 원을 편성하였으나 이 중 실제로 정보유출 피해자들의 구제에 직접 쓰이는 예산은 없는 것으로 확인되었다(방송통신위원회, 2018). 실례로, 방송통신위원회는 2016년 5월 해킹으로 인해 2,500여만 건의 회원정보를 유출한 인터파크에 대하여 개인정보 유출사고 중 최대 금액인 44억 8,000만 원의 과징금 및 2,500만 원의 과태료를 부과하였음에도 불구하고, 실제 개인정보 유출사고의 피해자인 정보주체의 피해보상이나 권익증진에 쓰이지 않고 국고에 귀속되어 전액 정부예산으로 쓰이고 있다(김남우, 2011). 이에 따라 과징금을 예외적으로 특별회계나 특정기금으로 귀속시키거나 특정사업으로 용도를 한정해야 한다는 입장의 입법례가 늘고 있다. 또한, 법 구조상 과징금을 국고로 환수하는 대신 특별회계나 특정기금에 귀속·특정사업에 한정하는 사례가 있다(지광석, 2012). 따라서 개인정보 유출사고로 인한 정보주체의 피해를 원인으로 하여 징수된 과징금 역시 정보유출 피해자 구제·권익증진 기금의 재원으로 활용할 수 있도록 '개인정보보호기금'설치 및 운용에 대한 적극적인 논의가 필요하다.

미국과 캐나다, 인도 등 일부 국가에서는 당국이 환수한 부당이득금·제재금·벌금·과태료·손해배상금·민간 기부금을 통해 기금을 조성한 뒤 이를 피해보상과 소송지원, 교육 등에 사용하고 있는 것으로 알려졌다.(지광석 외, 2012) 현재 우리나라의 경우에도 「응급의료에 관한 법률」, 「자동차손해배상 보장법」, 「석면피해구제법」등 총 70여 개의 개별법에서 국가재정법 제5조에 의거하여 기금을 설치·운용하고 있다. 개인정보 유출·침해사고에 대한 감독기관의 과태료·과징금 처분 등 행정 제재가 단순히 솜방망이 처벌로 그치는 것이 아닌 기업의 정보보호 인식·대책 제고를 위해 시행되기 위해서는 개인정보보호기금이 도입될 필요성이 있다. 개인정보 유출사고로 인한 과징금 부과원인은 이용자 피해에 있으므로 부과된 과징금을 이용자 피해구제 및 권익증진과 관련된 기금의 주요 재원으로 사용함으로써 정보유출로 인한 피해구제 체계가 구축될 것으로 보인다.

〈표 6〉 개인정보보호기금의 설치 · 운용에 대한 규정 제안안

개인정보보호법
제 OO장 개인정보보호기금
제OO조(기금의 설치 및 관리 · 운용) ①행정안전부장관은 개인정보 유출사고에 따른 피해자 구제 및 정보주체의 권익증진 등을 위하여 개인정보보호기금(이하 “기금”이라 한다.)을 설치한다. ②행정안전부장관은 대통령령으로 정하는 바에 따라 기금의 관리 · 운용에 관한 사무의 전부 또는 일부를 한국인터넷진흥원에 위탁할 수 있다. ③그 밖에 기금의 관리 · 운용에 필요한 사항은 대통령령으로 정한다.
제OO조(기금의 설치 및 관리 · 운용) ①기금은 다음 각 호의 재원으로 조성한다. 1. 정부 또는 그 밖의 자의 출연금 및 기부금 2. 「개인정보보호법」제34조의2, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제64조의3, 「신용정보의 이용 및 보호에 관한 법률」제42조의2에 따른 과징금 3. 제OO조에 따른 개인정보보호분담금 4. 기금의 운용으로 생기는 수익금 ②정부는 제1항제1호의 정부출연금으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제76조제2항제4호의2에 따른 과태료를 매 회계연도의 세출예산에 계상하여야 한다.
제OO조(개인정보보호분담금) ①「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제32조의3 및 제46조제2항, 「신용정보의 이용 및 보호에 관한 법률」제43조의3에 따라 손해배상책임 보험 · 공제에 가입하거나 준비금을 적립하여야 하는 정보통신망서비스 제공자 등은 기금 및 관련 사업을 위한 분담금을 행정안전부장관에게 내야 한다. ②제1항에 따라 분담금을 내야 할 자 중 책임보험등에 가입하는 자의 분담금은 책임보험등의 계약을 체결하는 보험회사등이 해당 납부 의무자와 계약을 체결할 때에 징수하여 정부에 내야 한다. ③제1항에 따른 분담금의 금액과 납부방법 및 관리 등에 필요한 사항은 대통령령으로 정한다.
제OO조(기금의 용도) 기금은 다음 각 호의 용도에 사용하여야 한다. 1. 개인정보 유출사고 피해의 보상지원 2. 개인정보 유출사고에 대한 소송지원 3. 그 밖에 정보주체의 권익을 위해 대통령령으로 정한 사업의 지원
제OO조(기금의 운용계획) 행정안전부장관은 회계연도마다 기금의 운용계획을 세워야 한다.
제OO조(잉여금과 손실금의 처리) ①기금의 결산상 잉여금이 생기면 이를 적립금으로 적립하여야 한다. ②기금의 결산상 손실금이 생기면 적립금을 사용할 수 있다.

본 연구에서 제시하고자 하는 개인정보보호기금의 용도는 개인정보 유출사고에 따른 피해구제 해결의 제도적 · 현실적 한계를 보완하기 위한 용도로서 사용하는 것이다. 아울러, 기금의 관리 · 운용 주체에 있어서는 정부가 직접 관리하되 관리 · 운용 업무의 일부를 산하기관(한국인터넷진흥원 등)에 위탁하여 운용하는 것을 제안한다. 하지만 앞서 3.3.2에서 살펴본 바와 같이, 현재 개인정보보호 법체계는 일반법인 「개인정보보호법」과 함께 산업 분야별로 「정보통신망법」, 「신용정보법」등에 따른 별도의 규제체계가 존재하므로 기금의 운용과 소관부처 선정에 어려움이 있을 수 있다. 현재 일반법인 「개인정보보호법」의 소관부처인 행정안전부가 공공기관 및 민간분야를 모두 총괄 관리하고 있는 상태이므로, 본 연구에서는 행정안전부를 개인정보보호기금의 주무부처로 지정하는 것이 가장 바람직하다고 판단하였다. 아울러, 기금의 설치 · 운용에 대한 규정은 개별법으로 기금의 내용을 정할 경우에는 별도의 입법 추진에 따른 부담이 가중될 수 있으므로, 일반법인 「개인정보보호법」의 일부 규정에서 그 내용을 정하는 것을 제안한다. 개인정보보호기금의 설치 및 운용에 대한 규정 제안안은 <표 6>과 같다.

5. 결 론

최근 사물인터넷, 클라우드 등 정보통신기술의 급진적 발전과 확산으로 해킹 등 사이버 공격에 대한 위험성이 증가하고 있다. 과거에는 단순한 정보유출로 사이버 공격이 주를 이루었으나, 인터넷의 확대를 통해 전 세계적으로 컴퓨터, 스마트 폰, 테블릿 등이 연결됨에 따라 현실 세계를 위협하는 등 물리적 피해를 수반하고 있다. 이처럼 해킹 등에 의한 대규모 개인정보 유출 사고가 계속해서 발생됨에 따라 국민들의 불안함이 계속해서 높아지고 있다.

이에 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 시행령이 일부 개정되면서 일명 ‘개인정보 손해배상책임 보장제도’라는 강제보험 형태의 정책성 보험이 시행되어 일일평균 1,000여 명

이상의 개인정보를 보유하고 있거나 매출액이 5,000만 원 이상인 정보통신서비스 제공자에 대하여 보험 또는 공제 가입, 준비금 적립 등의 필요한 조치를 취할 것을 의무화했다. 허나 사전 조사 부족, 보험 상품의 복잡성 등의 이유로 보험 가입 의무화 제도가 시행을 앞두고 보험업계와 가입 대상자인 정보통신서비스 제공자 등의 공감을 얻는데 많은 어려움을 겪었으며, 본 제도가 이미 시행되고 있음에도 불구하고 준비금 적립 기업에 대한 관리·감독의 어려움, 가입 관리의 체계화 부족, 일부 사업자에 대한 보험계약 인수 거부 등의 문제점을 이유로 정보통신서비스 제공자 등이 공감하고 만족할 만한 수준의 정책으로서 거듭나지 못하고 있는 상황이다. 하지만, 사이버 위험 관리체계가 구축되어 있지 않았던 기존의 상태에서 시행된 '개인정보 손해배상책임 보장제도' 운영의 어려움은 어찌 보면 자연스러운 현상이라고 생각된다. 사이버 위험의 유형과 수단은 끊임없이 변화해 나가고 있으며, 과거에는 대기업 중심의 공격이 이루어졌으나 최근에는 기업규모와 무관하게 공격을 시도하고 있다. 계속하여 진화해 나가고 있는 사이버 위험에 대응하기 위해서는 이제는 기업의 규모와는 관계없이 국내 모든 산업이 함께 나아가야 한다. 이에 개인정보 손해배상책임 보장제도는 사이버 사고 자료와 보험 통계를 축적하여 사이버 위험에 대한 사후적인 피해 구제뿐만 아니라 위험관리체계를 구축하는데 중요한 역할을 할 것임이 분명하다. 정책당국은 효율적인 제도 운영을 위해 보험을 통한 개인정보보호의 필요성에 대하여 사회적 공감을 얻어 강제가입 형태의 정책성 보험으로서의 정당성을 확보할 수 있어야 한다. 또한, 준비금 적립 기업에 대한 제재 및 관련 규정을 마련하고, 사이버보험관리시스템 구축을 통한 관리체계 수립 및 개인정보보호기금 설치·운용하여 사이버 위험으로부터 국민의 안전을 도모할 수 있도록 노력하여야 할 것이다.

이상 위에서 기술한 바와 같이 현대사회의 비약적 발전으로 뒤따르는 위험은 다양화·복잡화·대형화되고 있는 실정이며, 그 위험성은 날로 확대되고 있다. 대형 사이버 공격 또는 작은 사고를 막론하고, 확대되고 있는 사이버 위험에 효과적으로 대응하기 위하여 관련 법 개정을 통해 개인정보 손해배상책임 보장제도가 시행되었다. 사이버 사고 발생 이후의 보상도 물론 중요하지만 사이버 위험으로부터 국민의 안전을 도모할 수 있는 위험관리방안에 대한 정보통신서비스 제공자 등의 관심과 함께 정보보호 배상책임보험 시장이 활성화되어 보험산업, 정보통신서비스 제공자 등 그리고 서비스 사용자인 국민 모두에게 의미 있는 개인정보 손해배상책임 보장제도로서 발전할 수 있기를 기대한다.

참고문헌

강철하, "한국의 개인정보보호법제 현황과 개선 시사점-정보통신분야를 중심으로-", *법학논집*, 제22권, 제3호, 2018, 163-199.

개인정보보호위원회, "2019년 개인정보보호 연차보고서", 2019, 146-147.

국민안전처, 손해보험협회, "재난배상책임보험 길라잡이", 2017.

국민안전처, "재난취약시설 의무보험(재난배상책임보험) 업무처리절차서", 2017.

권영애, "사적 자치의 원칙과 기본권의 보호기능", *유럽헌법연구*, 제16호, 2014, 451-491.

금융보안원, "사이버리스크에 따른 국내·외 보험시장 현황", 2019.

김남우, "현행 과징금 제도의 주요 쟁점과 그 해결방안", *경제법연구*, 제10권, 제2호, 2011, 77-97.

김동영, "해외 개인정보 제도 사례와 시사점", *Research Brief*, 제14호, 2018, p.10.

김영국, "금융사고와 전자금융거래배상책임보험", 국민대학교 석사학위논문, 2015.

김종환, "금융거래 고객정보 침해사고 보상보험의 구성 및 정책방향", *한국전자거래학회지*, 제19권, 제3호, 2014, 1-21.

박세민, "보험법", 박영사, 2017, 625-627.

방송통신위원회, “개인정보 손해배상책임 보장제도 안내서”, 2019, 1-6.
방송통신위원회, “정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 규제영향분석서”, 2019.
방송통신위원회, “2017년도 방송통신위원회 심결집”, 2017.
방송통신위원회 보도자료, “방통위, (주)인터파크 개인정보 유출사고 엄정 제재”, 2016. 12. 06.
방송통신위원회 보도자료, “2019년 방통위 예산안 2,569억원 편성”, 2018. 08. 28.
보험개발원, “사이버 위험의 진화와 보험의 대응”, *CEO Report*, 2019.
보험개발원, “사회재난 정책보험 도입 및 재난보험 관리 운영체계 개선방안연구”, 2015.
상명대학교 서울산학협력단, “인터넷침해사고 보험제도 도입을 위한 피해액 산정 연구”, 방송통신정책연구, 13-진흥-089, 2013, 121.
송은지, 오남호, “사이버사고의 사회적 비용과 사이버보험 이슈”, *IITP 주간기술동향*, 1886호, 2019, 13-22.
심우민, “4차 산업혁명과 정보보호법제 개선방향”, *인터넷 법제동향*, 제132호, 2018, 47-54.
오한나, “인적 재난위험에 대비한 의무배상책임보험의 활성화 방안-재난배상책임보험을 중심으로”, 동국대학교 석사학위논문, 2019.
유진호, “국내 · 외 사이버보험 현황 및 표준화 필요성”, *전자금융과 금융보안*, 제12호, 2018, 30-31.
유진호, “사이버보험의 현황과 과제”, *KISA Report*, 제6호, 2018.
유진호, “이용자 피해구제를 위한 사이버보험 활성화 방안”, *월간손해보험*, 제592호, 2018, 61-65.
이혜은, “사이버 리스크와 사이버 보험, 현황과 향후 과제”, *KiRi Report*, 제15호, 2017.
임 준, “중소기업 사이버 보험 시장 활성화 방안”, *KiRi Report*, 제466호, 2019.
임 준, 이상우, 이소양, “디지털 경제 활성화를 위한 사이버보험 역할제고 방안”, *KiRi Report*, 2018.
전승재, “개인정보 유출로 인한 손해배상 제도에 관한 고찰”, *경제규제와 법*, 제11권, 제1호, 2018, 28-51.
중소벤처기업부, “중소기업 기술보호 지원사업”, 2019.
지광석, 김성천, 김인숙, 김영신, “소비자권익증진기금의 설치 및 운용방안”, *정책연구보고서 12-03*, 2012, 1-212.
진대화, “개인정보침해에 대한 손해배상의 근거와 피해구제제도”, *Internet & Security Focus*, 2014, 5-8.
최우석, “사이버 위험관리를 위한 보험의 역할 및 과제”, *The Risk*, 제4권, 제4호, 2017, 5-7.
한국정보산업연합회, “개인정보보호를 위한 손해배상보험 의무가입제 도입-정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정”, 2019.
홍준호, 강주명, “정보주체 보호를 위한 사이버보험 의무 가입 필요성에 관한 연구”, *원광법학*, 제35권, 제1호, 2019, 267-290.
Congress GOV., H.R. 6032-114th Congress : Data Breach Insurance Act, 2016. 09.
IBM Security, “Cost of a Data Breach Report”, 2019.
Camillo, M., “Cyber risk and the changing role of insurance”, *Journal of Cyber Policy*, Vol.2, No.1, 2017, 56-57.
Talesh, S.A., “Data Breach, Privacy, and Cyber Insurance : How Insurance Companies Act as ‘Compliance Managers’ for Businesses”, *Law and Social Inquiry*, Vol.43, No.2, 2018, 1-2.
Trang, M.N., “Compulsory Corporate Cyber-Liability Insurance : Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches”, *Minnesota Journal of Law*, Vol.18, No.1, 2017, 397-425.

About the Authors

이 수 연 (sy930616@korea.ac.kr)

광운대학교 법학과에서 학사 학위를 취득하였으며, 현재 고려대학교 정보보호대학원 정보보호학과 석사과정에 재학 중이다. 주요 관심분야는 정보보호, 정보보호정책, 금융보안, 개인정보보호 등이다.

권 헌 영 (khy0@korea.ac.kr)

연세대학교 법학과에서 학사, 석사, 박사학위를 취득하였으며, 고려대학교 정보보호대학원 교수로 재직 중이다. 주요 관심분야는 정보통신, 정보보호, 사이버보안, 사이버안보, 정보화, 전자정부, 사이버윤리 등이다. 한국인터넷윤리학회 회장을 역임하였으며, 현재 사이버커뮤니케이션학회 회장, 한국IT서비스학회 부회장, 고려대학교 사이버보안정책센터 센터장 등을 맡고 있다.