韓國IT서비스學會誌
第10卷 第4號
2011年 12月

개인정보관리자의 책임과 벌칙의 형평성

김 범 수*

The Legal Justice of Conferring Criminal Negligence on Chief Privacy Officers(CPO)

Beomsoo Kim*

■ Abstract ■

The recently revised "Telecommunications Business Promotion and Personal Data Protection Act" is an important legal milestone in promoting the Korean telecommunications infrastructure and industry as well as protecting individuals' personal data and individuals' rights to privacy. Special characteristics of information security and privacy protection services including public goods' feature, adaptiveness, relativity, multi-dimensionality, and incompleteness, are reviewed. The responsibility of chief security/privacy officers in the IT industry, and the fairness and effectiveness of the criminal negligence in the Telecommunications Act are analyzed. An assessment of the rationale behind the act as well as a survey of related laws and cases in different countries, offers the following recommendations : i) revise the act and develop new systems for data protection, ii) grant a stay of execution or reduce the sentence given extenuating circumstances, or iii) use technical and managerial measures in data protection for exemption from criminal negligence.

Keyword : Privacy, Information Privacy Protection, Personal Data Protection, Technical and Managerial Measures for Protecting Security and Privacy

논문투고일 : 2011년 05월 21일 논문수정완료일 : 2011년 08월 21일 논문게재확정일 : 2011년 09월 06일
* 연세대학교 정보대학원 교수

1. 서 론

정보통신기술의 발달과 새로운 정보서비스의 등장과 함께 개인정보가 다양하게 사용됨에 따라 개인정보의 부적절한 관리에 대한 염려와 불안감이 갈수록 커지고 있다. 또한 최근에 발생한 여러 건의 개인정보 대형 유출 사고는 프라이버시에 관한 사회적 관심을 확산시키고, 관련 법률과 제도의 보완 및 개정을 유도하는 결과를 낳았다.

관련 법률의 개정 과정에서 다양한 의견이 수렴되고 새로운 정책 방향과 기조가 수립되지만, 여러 가지 제약에 의해 법률의 효과에 대한 연구는 선행되기 어려운 경우가 많다. 이에 이 연구에서는 사례 분석을 통하여 정보보호 관리 정책 수립에 결정적인 영향을 미치는 정보보호 업무의 특성을 정리한다. 또한, 최근에 개정된 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망 법)'의 기능과 벌칙이 범죄의 예방에 미치는 기능의 효율성에 대해 검토한다. 이러한 검토를 바탕으로 국내외 법률 비교와 정보보호 관리 사례를 검토하여 현행 법률과 제도의 개선을 통한 범죄 억제 및 예방기능을 향상에 기여할 수 있는 정책 대안을 제시한다.

2. 정보보호의 공격 및 방어

정보보호 법제도의 검토에 앞서, 정보보호의 현황과 주요 업무의 이해를 통하여, 이 연구에서 다루고자 하는 정보보호 문제의 특수성과 그 특성을 살펴본다. 정보보안 및 보호는 개인이나 기업에게 있어서 필요하지만, 직접적으로 이익이나 이해 관계에 긍정적인 효과를 기대하기 어렵기 때문에 "간접재(indirect goods)"의 성격을 강하게 띈다. 또한 자신이 직접 적극적으로 문제를 해결하기 보다는 다른 누군가가 대신해서 해결책을 모색하기를 바라는 "공공재(public goods)"의 성격도 함께 갖추고 있다[1]. "간접재화", "공공재화"의 성격 외에도 정보보호의 기술(방어 기법)의 변화에 따라 침해의 기술(공격 기법)도 진화하는 "가변성(adaptiveness)"을 가지고 있다. 또한, 해커나 범인이 직접 공격을 하거나 침해행위를 하지 않고 제 3의 기관, 장비 등을 이용할 수 있기에, 가해자와 피해자가 1 : 1이 아니라 1 : N, M : N의 "다차원적 특성(multi-dimensionality)"을 가진다. 간접재와 공공재의 특성은 기존의 경제학에서 연구가 많이 진행되었고, 관련법에 따른 처벌에서 고의와 과실에 대한 분류와 직접적인 상관관계가 없으므로, 이 연구에서는 다루지 않는다. 즉, 이 연구에서는 형사처벌의 기준과 직접적인 관련이 있는 해킹과 프라이버시 침해의 특성 중 "가변성", "다차원성", 그리고 보안의 "불완벽성(Incompleteness)" 및 "상대성(Relativity)"을 중심으로 문헌 연구와 사례 분석을 통해 정리한다.

2.1 정보보호 관련 공격 및 방어의 특성

과거에는 정보시스템 및 네트워크에 대한 침입이 주로 기술적인 우월성, 공격의 수월성을 과시하기 위한 경우가 많이 있었다. 그러나 최근의 경향은 해킹이나 크래킹 등의 행위가 금전적인 이익이나 시스템 장악 후 일정기간 활용, 정치적 목표물 공격 등 특정한 목적을 가지고 광범위하게 조직적으로 추진되고 있는 것으로 관찰되고 있다. 또한 기술적 공격과 더불어 사회공학적인 공격의 비중도 늘어나고 있다[10, 21].

시스템과 네트워크에 대한 공격과 방어는 창과 방패의 싸움으로 자주 묘사된다. 즉, 정보기술이 발달함에 따라 새로운 형태의 취약점을 통한 침입이 이루어지고, 이를 방어하는 보안기술과 제도가 고도화되면, 불법적 침입이나 가해가 중단되는 것이 아니라, 또 다른 형태로 변형되고 새로운 대상을 찾아 움직이는 현상을 보이기 때문에 이러한 비유가 적절하다고 할 수 있다. 즉, 시스템과 네트워크 침해 유형과 그 방법이 지속적으로 적응 또는 진화하고, 경우에 따라서는 변형, 혁신 등의 과정을 통하여 계속해서 변화하고 확산하는 "가변

성”을 가진다.

서동일[5]이 작성한 [그림 1]은 정보보호 관련 공격 및 침해의 유형을 시간의 변화에 따라 간략히 정리하였다. 이를 통하여 보면, 보안기술이 발달됨에 따라, 관련 공격기술 또한 지속적으로 더 정교하고 파괴적으로 변화하고 있으며, 디지털 정보사회가 더욱더 고도화 됨에 따라 그 피해와 영향의 범주가 확산되고 있음을 알 수 있다.

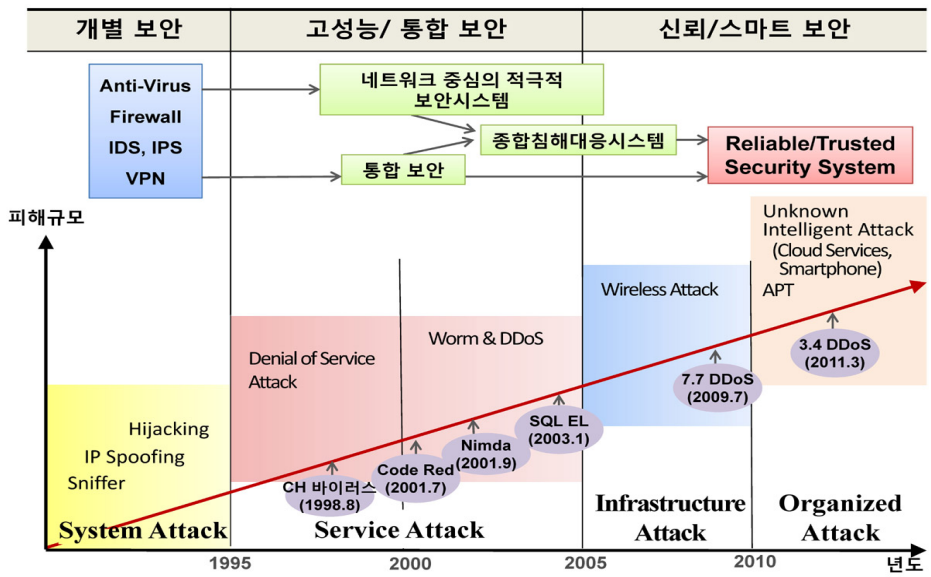
정보보호의 “불완벽성”과 “상대성” 또한 고려되어야 할 주요한 특성이다. 이준택[10]은 “모든 정보시스템은 공격에 취약하며, 완벽하게 안전한 시스템은 존재하지 않는다”라고 하였고, Lininger and Vines[19]등은 물리적 안전뿐만 아니라 사회적 침입으로부터 시스템과 정보를 보호하는 것이 불가능하다고 언급하고 있다. 즉, 정보보호 및 보안에 있어서 100% 완벽한 방어는 불가능하다. 생물학적인 비유를 들자면, 인간이 감기의 원인과 대비책은 알고 있지만, 감기의 세균은 계속해서 변화하므로, 손을 씻고 백신을 맞는 등 알려진 예방조치를 취하지만 사회생활을 하는 한 이러한 병원균에 노출을 피할 수 없다. 결국, 면역이 없는 새로운 형태의 감기 균에 노출되고 병에 감염되어 저항력이 생길 때까지 물리적인 고통을 이겨내야 하는 현상과 유사하다. 즉, 정보시스템과 네트워크로 구성된 정보자산을 이용하고 있는 한 정보보호 및 보안을 통해 항상 완벽하게 위험을 제거할 수는 없다. 또한, 창과 방패의 상대성 비유가 완벽하게 상대를 제압할 수 있는 기술이 없음을 시사하는 바처럼, 정보와 시스템, 네트워크를 노리는 범죄행위는 하나의 보호 장비나 제도로 관련된 모든 문제를 해결하거나 미래의 모든 위협을 막는 데는 그 한계가 엄연히 있다.

다음 절에서는 시스템과 네트워크 침해방법의 특성인 “가변성”과 더불어, 침해나 범죄자가 직접적인 공격뿐만 아니라 제 3의 주체를 이용한 간접적인 공격을 시도하는 “다차원성” 위주로 사례를 들어 설명한다.

2.2 정보보호 관련 범죄의 사례

2.1.1 최초의 웜(Worm)의 개발

1988년 11월 2일 코넬대학의 박사과정 학생이었



[그림 1] 정보보안기술과 침해기술 발전방향

던 Robert T. Morris는 인터넷의 크기를 짐작하기 위하여 웜을 개발하여 MIT의 컴퓨터를 통해 배포하였다[16]. 이 때, 다른 프로그래머가 Morris의 프로그램을 인지하거나 차단하기 어렵게 만들기 위하여, 그 당시 정보보호 전문가들이 생각하던 컴퓨터 바이러스(virus)의 확산방식과 차별되도록 하였다. 또, 프로그램이 이미 특정 컴퓨터에 복제되었는지를 스스로 확인하는 기능과 이 기능을 역이용하여 보안책임자들이 프로그램을 무력화하는 것에 대비하여 확인 결과와는 무관하게 다시 복제하도록 하는 기능을 추가하였다. 바로 이 사실이 침해 공격의 상대성 및 가변 특성의 자연발생적 기원을 보여주고 있다. 자신의 프로그래밍 역량을 과시하고, 새로운 형태의 프로그램 제작이 가능하다는 점을 보여주기 위해 만든 이 웜 프로그램은 Morris의 예상보다 훨씬 급속하게 확산되었고, 결국 6,000여 컴퓨터 시스템이 마비되는 사태로 이어졌다. 그 결과, 본인이 직접 나서서 해결책을 제안하였지만 이 행동에 따른 피해가 이미 발생한 후였다. 그래서 Morris는 1984년 제정된 미국의 '컴퓨터 사기 및 남용방지법'(Computer Fraud and Abuse Act)에 따라 처벌을 받은 첫 사례로 3년간 집행유예, 사회봉사, $10,050벌금형을 받았다[16].

이 사례를 통하여 악의가 없더라도 누구나 해커가 될 수 있다는 점과 새로운 형태의 공격은 기존의 방어체계를 반드시 넘는 수준의 것으로 만들어진다는 것을 알 수 있다. 또한, 미국 해커의 경우처럼 직접 해킹을 실행한 고의범의 경우에도 실형을 선고 받지 않은 사례가 있음을 알 수 있다.

2.1.2 한국의 슬래머웜과 1.25 인터넷 대란

2003년 1월 25일 오후 2시 10분경 시작된 슬래머웜(Slammer Worm) 공격은 KT 혜화전화국을 비롯한 국내 주요 인터넷 서비스 제공자(ISP, Internet Service Providers)의 DNS 서버를 다운시켰다[1, 10]. 이 공격은 마이크로소프트(Microsoft)사의 MS-SQL Server 2000 프로그램의 취약점(bug)을 이용하여 256개의 불특정 다수 서버 컴퓨터에 복제하면서 과다한 네트워크 트래픽을 발생시켜 네트워크를 마비시키는 악성 프로그램에 의해 발생하였다.

이 사건의 직접적인 책임을 추궁할 수 있는 사람, 즉, 의도적으로 이 문제를 만든 사람으로 웜의 개발 및 초기 유포자를 지목할 수 있다. 이 범죄의 흥미로운 특성의 하나는 의도적으로 웜을 개발하거나 이를 의도적으로 유포한 자가 현실적으로 누구인지를 확인하기 거의 불가능하다는 것이다. 또한, 확인된다고 하더라도 대한민국 법이 미치지 않는 장소에 범죄자가 있는 경우라면 그 처벌이 현실적으로 어렵다. 반면, 자신에게 주어진 선량한 관리자로서의 주의 의무를 준수하지 않은 사람이나 기관 즉, 과실의 책임을 물을 수 있는 대상은 MS-SQL Server 2000을 버그 없이 만들지 못한 마이크로소프트, 보안패치 프로그램을 설치하지 않은 서버관리자, 사고 예방과 처리를 위한 적절한 조치와 관리를 하지 못하였거나 약관에 규정한 바와 같이 네트워크 서비스를 제공하지 못한 인터넷 서비스 제공자, 국가기간 시설 운영에 대한 관리 감독을 잘 수행하지 못한 국가 등으로 어렵지 않게 가시화할 수 있다. 즉, 고의범은 찾기가 현실적으로는 어렵지만, 과실범은 쉽게 확인되며, 과실범과 피해자는 한 기관이나 조직에 한정되지 않고 개인부터 국가까지 다수라는 점이 특이하다. 한가지 더 주목하여야 할 점은 이들이 가해자로서 과실 책임의 당사자임과 동시에 신뢰도 하락과 더불어 서비스 제공 약정 위반으로 인한 민사 소송의 피해자가 될 수 있다는 사실이다.

2.1.3 리니지 사용을 위한 명의 도용사건

지난 2006년 3월 중국에서 온라인 게임을 이용하는 사람들이 (주)엔씨소프트사에서 운영하고 있는 리니지 및 리니지 II 게임을 사용하기 위한 계정을 만드는데 대한민국 국민 122만 명의 이름과 주민등록번호를 이용한 사건이 발생하였다. 사건을 인지한 엔씨소프트사는 휴대폰 인증 서비스 등 본인 등록여부를 확인하는 시스템을 추가로 고안·운영하고, 17만 5천여 계정을 폐쇄하는 조치를 취했다.

가해자이자 실제로 명의도용을 한 자인 온라인

게임을 하는 중국인들은 당시 현행법으로 처벌하기 어려워 2006년 3월 24일 주민등록법이 개정되었으나, 중국에 소재한 명의 도용자들에 대한 위법의 집행과 적용은 사실상 불가능하다. 한편, 명의도용 피해사실을 인지한 개인 중 8,574명은 엔씨소프트사를 상대로 과실책임을 묻는 손해배상청구의 집단민사 소송을 제기하였다.

이 사례에서도 엔씨소프트는 기업의 신뢰, 영업기회의 상실, 추가적인 보안조치의 실행 등 많은 손해가 발생하여 이 사건의 피해자로 볼 수 있지만 동시에 관리소홀의 책임을 지는 사건의 간접적인 가해자로서 인지될 수 있는 소지가 있다.

2.1.4 GS칼텍스의 직원에 의한 고객정보 유출

2008년 9월 5일 GS칼텍스 자회사 GS넥스테이션의 직원이 자신의 영리를 목적으로 GS칼텍스 보너스카드의 고객정보 11,517,125건을 DVD에 복사하여 유출한 사고이다. 이 사건의 경우 개인 피해자는 다수이며, GS칼텍스도 기업의 신뢰도 하락 등의 손실을 입었지만, 직원의 관리 감독에 대한 책임 여부를 물을 수도 있다. 또한, 보너스카드를 사용하는 개인 8,184명이 GS칼텍스를 상대로 손해배상을 요구하는 민사소송을 2009년 1월 제기하였다. 즉, 이 사건에서 보듯이, 일반 기업이나 공공기관에서 개인정보유출 사고가 발생하면 주로 손해배상 소송 등 민사적인 책임의 유무를 판별하여 범죄의 사회적 효익이 없어지도록 하고 있다. 즉, 이와 같은 관리감독의무를 소홀히 한 경우에 정보누설업체는 민사책임을 지게 되므로 피해자 구제는 이루어진다고 할 수 있다. 따라서 위와 같은 경우에 형사처벌의 가벌성이 있는지 의심이 된다.

3. 정보통신망법 과실범 처벌 규정의 합리성

3.1 형법상 처벌의 원칙

오늘날의 형법은 일반적으로 보호적 기능, 보장적 기능, 사회질서 유지 기능을 수행한다[12]. 보호적 기능은 형법이 일정한 행위를 범죄로 규정하고 이에 형벌을 부과함으로써, 일정한 가치 또는 이익을 범죄적 침해나 침해의 위험으로부터 보호하는 기능이다. 보장적 기능은 국가의 형벌권의 발동을 제한하여 개인의 자유를 보장하는 기능이다. 형법의 사회질서 유지 기능(또는, 사회 보호적 기능)은 형벌이라는 수단에 의하여 범죄로부터 사회질서를 지키고 유지하며 보호하는 기능을 의미한다. 또한 이러한 세 가지 기능이 보장적 기능의 기초 위에 시대상황이나 정치상황에 부응할 수 있도록 보호적 기능과 사회질서유지 기능을 함께 고려한다.

형벌은 국가가 범죄인에 대하여 과하는 법익박탈의 처분이며, 기본적으로 악행인 범죄에 대한 응보로서의 의미를 가진다. 또한, 일반인들에게 위하(威脅), 경고하여 범죄를 방지하는 일반 예방적 기능을 수행한다. 한편, 특별 예방적 기능도 있지만, 이는 이 연구의 범위를 벗어나므로 논의를 생략한다.

3.2 정보통신망법상 과실범의 처벌 규정

정보통신망법 제 4장은 개인정보의 수집, 이용, 제공, 파기의 절차 및 관리, 손해배상 청구권, 분쟁조정, 자율규제 등 개인정보의 보호를 위한 제도를 명시하고 있다. 이 법은 대한민국 정보통신서비스 제공자들이 개인정보보호를 위한 시스템 운영에 매우 중요한 지침을 제공하고 있다.

2008년 6월 13일 일부 개정되고, 2008년 12월 14일 시행된 '정보통신망법' 제73조 제1호는 '제28조 제1항 제2호부터 제5호까지의 개인정보의 보호조치의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자'에 대하여 '2년 이하의 징역 또는 1천만 원 이하의 벌금에 처한다'라고 법정 형량을 기술하고 있다.

"2년 이하의 징역 또는 1천만 원 이하의 벌금"

규정은 2002년 12월 18일 개정된 정보통신망법에 청소년유해물표시 및 청소년유해물 광고금지를 위반하는 경우의 벌칙으로 처음 포함되었다. 이후 개인정보보호의 필요성과 피해 가능성을 인지하여, 2008년 2월 29일까지 6번의 개정을 통하여 2개의 호에서 7개호로 늘었다. 기존 7개호의 공통점은 정보통신망법의 규정을 고의적으로 위반하거나 규정에 의한 명령을 이행하지 아니한 경우에 한하고 있다. 2008년 6월 개정된 내용에 1개호가 추가되었으며, 이 호는 다른 호와 달리 침해 사고를 고의로 일으키지는 않았지만 과실의 책임이 인정되는 경우에 나머지 7개호와 같은 수준의 벌칙을 받도록 개정되었다.

제73조 제1호는 개인정보보호를 위하여 의무화한 기술적·관리적 조치를 취하지 않아서 정보프라이버시 침해 사고가 발생하는 경우에 대해 설명하고 있다. 즉, 고의로 개인정보를 불법적으로 이용하는 것에 대해 필요한 사전적·사후적 조치를 취하지 않은 것에 대한 과실 책임을 정보통신서비스제공자에게 묻는 것이다.

이 호의 제정 목적은 개인정보관리자가 보다 적극적으로 개인정보보호의 의무를 수행하도록 하여 정보프라이버시 침해 가능성을 낮추고 사고를 예방하는데 있다. 이 규정에 대한 형평성에 대한 논의가 법개정 이후에도 지속적으로 언급되며, 관련 기관 및 기업들의 규정에 대한 이해와 해석이 통일되지 못하고 있다. 그래서 이 연구에서는 과실범에 대한 '2년 이하의 징역' 벌칙의 적절성에 대하여 사례를 들어 분석한다.

4. 정보프라이버시 침해 관련 과실범의 형사적 처벌과 기대 효과

4.1 법 개정의 긍정적 효과

정보통신망법 제28조는 개인정보의 보호조치, 제10장 벌칙은 개인정보의 수집·관리·이용·삭제의 과정에서 정보프라이버시를 적극적으로 침해하는 행위, 명예훼손 등에 대하여 징역형이나 벌금형을 법정형으로 제시하고 있다. 이 조항은 고의적인 정보프라이버시 침해 행위를 처벌함으로써 대한민국 국민들의 개인정보를 보호하는데 그 목적이 있다. 이러한 공식적 제재를 명확하게 제시하여 범죄행위의 직접적 억제 및 예방 효과를 기대할 수 있다.

보다 강화된 벌칙에 대한 인지된 두려움이 기술적·관리적 개인정보보호 수준을 높여서 결국 보다 향상된 개인정보 보호라는 기대 효과를 얻을 수 있다.

이를 위해서는 정보통신서비스 제공자가 관련된 인적 자원, 기술적 자원, 제도적 자원에 대한 적극적 투자와 관심이 필수적으로 동반되어야 한다. 관련 예산의 확보 및 투자를 통해 기존에 미비 되었던 개인정보보호에 필요한 자원이 확보되고, 조직 내에서 개인정보보호 담당자의 상대적 지위향상, 전문성 인정 등의 계기가 마련될 수 있다.

4.2 법 개정의 부정적 효과

4.2.1 처벌의 불균형과 적정성

정보통신망법 제73조 2호부터 8호까지 2년 이하의 징역이나 1천만 원 이하의 벌금이 정보프라이버시를 침해하는 고의범에 대한 벌칙을 제시하는 반면에, 같은 수준의 처벌을 법정형으로 제시하고 있는 제73조 제1호는 과실범의 사례를 들고 있다.

4.2.2 공공기관의 개인정보보호에 관한 법률과의 형평성

정보통신망법은 정보통신 서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하기 위하여 정보통신사업자 및 준용사업자의 개인정보보호의 의무와 책임을 규정하고 있다. 즉, 민간부문에서 개인정보의 보호를 위한 법률이다. 한편 공공기관에서 개인정보보호는 2010년 2월 4일 개정된 '공공기관의 개인정보보호에 관한 법률(공공

기관 개인정보법)'이 대표적이다.

공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호하기 위한 공공기관을 대상으로 한 개인정보보호에 관한 법률이다. 대한민국의 정부는 주민등록제도, 전자정부 시스템 등의 다양한 제도와 시스템을 운영하여 국민에 대한 많은 정보를 처리하고 국민과 기업에 서비스하고 있다. 이러한 시스템에서 사용되는 개인정보의 보호에 필요한 기술적 관리적 제도 및 개인정보 보호를 위한 제도 운영의 수준의 일반 기업과 비교하여 상당히 높은 수준에서 이루어지기를 기대하고 있다. 미국, 유럽 등의 해외 사례를 보더라도, 정부에서 관리하는 개인정보의 보호와 더불어 정부로부터 개인의 프라이버시의 보호가 프라이버시 및 개인정보 보호법과 제도의 핵심이며 상대적으로 민간부분에서의 개인정보의 보호는 자율적 규제와 이를 보완하는 법제도에 의존하는 경우가 많다. 즉, 공공부문에서 개인정보보호의 필요 및 중요성이 민간부분의 그것에 비하여 상대적으로 낮지 않다.

그렇다면 대한민국의 공공부문의 법률과 민간부분의 법률이 개인정보 유출과 관련된 과실범에 대한 벌칙을 어떻게 규정하고 있는지 조사할 필요가 있다. 공공기관 개인정보법에서 제23조 벌칙은 다음의 세 항으로 나뉜다. 제1항, 공공기관의 개인정보처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경 또는 말소한 자는 10년 이하의 징역에 처한다. 제2항, 제11조의 규정을 위반하여 개인정보를 누설 또는 권한없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적으로 사용한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 제3항, 부정한 목적으로 제4조의2제2항을 위반하여 폐쇄회로 텔레비전의 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자와 거짓 그 밖의 부정한 방법으로 공공기관으로부터 처리정보를 열람 또는 제공받은 자는 2년 이하의 징역 또는 700만 원 이하의 벌금에 처한다. 벌칙의 조항들은 고의적으로 법을 어기는 경우에 처벌하는 것으로 일관하고 있다. 즉, 현재 공공기관 개인정보법은 기술적 관리적 조치의 미비로 인한 사고시 처벌 조항처럼 개인정보 유출 및 프라이버시 침해사고와 관련된 과실범 처벌 조항은 포함하고 있지 않다.

4.2.3 징역형의 제한된 억제효과

기존의 형법의 효과분석 연구[1, 4]에서 벌칙이 억제적 효과를 발휘하기 위해서는 인지된 처벌의 신속성, 확실성 등이 담보되어야 한다. 그러나, 정보통신망법의 처벌조항은 다음과 같은 이유로 인해 큰 억제효과를 기대하기 어렵다. 첫째, 관리부주의에 따른 개인정보 유출 등의 사건은 그 피해를 인지하는 시점까지 상당한 시간이 소요되는 경우가 많고, 오랜 기간 동안 그 유출 사실을 파악하지 못하는 경우가 많다. 이러한 경우, 처벌의 신속성이 떨어지게 된다. 둘째, 현행법상 과실범에 대한 처벌은 감경(減輕), 또는 집행유예(執行猶豫) 등으로 선고될 수 있다. 이는 법 집행의 엄격성이 상쇄된 것이다. 즉, 개인정보 유출 사고의 가변성, 다차원성, 불완벽성 등의 특성을 고려할 때, 과실범에 대한 징역 등 신체의 자유를 구속하는 자유형 벌칙은 그 좋은 효과를 기대하기 어렵다.

4.2.4 정보보호 전문인력 양성과 인재 확보 어려움

정보통신망법은 개인정보관리 책임자의 지정 및 관리제도의 운영을 의무화하고 있다. 그러나, 정보보호 전문인력의 양성과 수급 측면에서 전문가의 공급이 절대적으로 부족하다. 관련 법은 정보보호 관리책임자 및 전문인력이 개인정보를 다루도록 요구한다. 이러한 전문인력이 실질적으로 정보보호 기술적 관리적 조치의 필요와 특성을 이해하고 임무를 적극적으로 추진하기 위해서는 체계적인

교육과 훈련, 리더쉽 등이 필요하다. 이러한 자질을 갖춘 인력의 확보가 현재는 쉽지 않다.

또한, 공공기관이나 기업 내 개인정보관리 책임자의 권한이나 가용자원의 규모가 다른 부서나 업무의 책임을 맡고 있는 경우보다 상대적으로 제한적이다. 즉, 권한은 상대적으로 적고, 정보보호의 의무와 사고 발생시 징역형까지 선고받을 수 있는 매우 위험이 높은 직종으로 인식될 수 있다. 높게 인지된 위험은 결국 우수한 새로운 인력이 관련 과정이나 교육, 경력개발 프로그램을 거쳐 정보보호전문가로 자리매김하는데 큰 걸림돌이 된다.

개인정보 관리책임자로 우수한 전문인력이 배치되지 않으면, 궁극적으로 개인정보 보호의 수준이 낮아지므로 결국 더 많은 개인정보 유출 사고를 경험하게 되며, 이는 곧 사회적인 손실로 이어질 수 있다. 전문인력이 상대적으로 위험이 낮고, 보상이 높은 다른 직종으로 옮겨가거나 정보보호 분야를 기피한다면 실질적 우수 인력 확보에 더욱 어려움이 예상된다.

4.3 형법의 억제 및 예방 효과 개선안

4.3.1 과실범에 대한 징역형의 완화

일반 형법의 처벌과의 균형, 해외의 사례 등을 고려하면 제73조 제1호는 과태료나 벌금형 등으로 개정될 필요가 있다. 또한 피해의 규모와 관리수준의 미비점 등을 고려하여 그에 상응하는 수준의 벌칙이 선고될 수 있도록 수정을 검토하여야 한다.

4.3.2 작량감경과 집행유예제도의 활용

정보통신 서비스 사업가 관심있는 것은 법정형보다는 선고형이다. 그래서 법의 개정이 이루어질 때까지는 법원이 필요에 따라 작량(酌量)하여 형을 감경(減輕)하여야 한다. 또한 고의범이 아니라 과실범이라는 범죄의 성격을 고려하여, 집행유예의 적극적 활용이 필요하다. 즉, 관련 법의 개정 이전이라도 현재 활용할 수 있는 작량감경(酌量減輕)과 집행유예 등의 제도를 통해 정보보호 책임자의 형사처벌을 회피할 수 있는 방안을 모색할 수 있다.

4.3.3 기술적 관리적 개인정보보호 조치 기준 보편화와 면책

정보보호 기술은 지속적으로 변화하기 때문에, 일정수준의 관리에 대한 상세한 정보를 법령에 기술하기 어렵기 때문에 서비스제공자의 혼돈과 높은 위험의 인지로 이어질 가능성이 높다. 정부와 정보보호 협회, 학회 등 관련된 민간기구에서 협의 하에 만들어진 적절한 수준의 기술적·관리적 개인정보보호 조치의 기준을 마련하고, 이 수준을 따른 경우 형사적 처벌을 면할 수 있도록 하는 방안을 고려할 수 있다. 현재, 준용사업자중 정보통신망을 사용하지 않는 경우 행정안전부장관이 정한 별도의 기준을 따르게 되어 있다. 이 기준 또한, 산업별, 정보보호 수준별로 정부와 민간기구를 협의를 통하여 자율적으로 바람직한 관리수준을 설정하고 이를 적극적으로 활용하여야 한다. 이 기준이 보편적으로 널리 확산되기 위해서는 우선 이 기준의 실효성이 공공기관, 기업 등 민간기구, 개인 등에 이해되고 적극적으로 수용되어야 한다. 이러한 이해를 바탕으로 기준을 따르는 기업은 개인정보 유출 사고가 발생하더라도 관련 규정에 따라 제73조 제1호의 과실 처벌을 받지 않도록 보장되어야 한다.

4.4 외국의 관련 법과 사례

영국은 개인정보 피해에 관해서는 정보보호 법과 정보공개법의 규정에 따라 독립적인 기관인 Information Commissioner's Office(ICO)가 정보프라이버시에 대한 불만사항 접수, 분쟁조정, 피해구제 등의 기능을 맡고 있다. 또한, 직권으로 개인정보보호 실태조사를 실시하여 위법성 여부를 심사하기도 한다. 그러나, ICO는 민사상 손해배상에 대해서는 결정을 내릴 권한이 없으며, 법원이 이에 대한 판단을 할 수 있다[11].

구체적인 관련 사례로 지난 2009년 2월 25일 Cam-

den Primary Care Trust에서 관리하는 2,500여명의 건강정보가 수록되어있는 개인용 컴퓨터가 St. Pancras Hospital 내에서 도난된 경우가 있었다. 우선 ICO에서 이 사건에 대한 조사를 엄격히 시행하였다. 이 조사 이후에 ICO는 i) IT장비관리 방법과 절차에 대한 효과적 이해를 위한 캠페인 실시, ii) USB 메모리, 랩탑, 데스크탑 등에 저장된 자료의 암호화, iii) IT 장비 자산관리대장의 적절한 운영, iv) 폐기/파기물 관리대장의 정확한 운영, v) 개인정보보호팀을 만들어 이러한 이행조치가 실현되도록 할 것 등의 제안을 한다. 이러한 제안을 바탕으로 Information Commissioner는 i) 컴퓨터 장비를 폐기할 때 반드시 개인정보를 삭제 후 폐기한다, ii) 2009년 12월 31일까지 위의 다섯 가지 제안을 계속 수행한다, iii) 위의 제안된 내용이 어떻게 수행되는지 2009년 3월 31일 중간보고를 한다를 포함하는 이행 통지(Enforcement Notice)를 하였다. 이 사건에서는 개인정보가 관리 부주의로 유출되었으면, 형사적 처벌이 아니라 제도의 개선을 제안하고, 이를 구체적으로 준수함을 감시하는 기능을 ICO가 수행하고 있는 것을 알 수 있다.

구체적으로 영국에서 1998년 개정된 개인정보보호법(Data Protection Act)[17]에 따르면 형법상 처벌은 벌금형만 가능하다. 또한 이 벌금형의 대상이 되는 행위는 '개인정보의 불법적 수집과 활용', '불법적으로 수집된 정보의 판매나 판매의 제안', '개인으로부터 채용 등을 수단으로 과도한 정보의 수집', 'ICO에서 수집관리하고 있는 개인 정보 유출', '데이터 구성 및 기술/관리적 변경사항 ICO 통지의 무 불이행', '이행명령의 불이행', '이행명령 등에 따른 거짓문서 제공' 등이 포함된다. 즉, 영국의 Data Protection Act 1998과 Freedom of Information Act 2000은 제도적·관리적인 보호조치의 미비를 직접적인 형사처벌의 원인으로 분류하지 않는다.

프랑스는 개인정보피해 구제기구인 Commission Nationale de l'Informatique et des Libertés (CNIL, French Data Protection Authority)에서 프랑스 개인정보법(Data Protection Act)에 따라 불만사항을 접수하고 처리하여, 개인정보프라이버시 침해를 입은 자를 보호하고 그 피해를 구제하여 주는 역할을 하고 있다. 이 법에서는 개인정보 또는 민감한 정보의 수집과 관리에서 문제가 발생할 경우 최고 5년의 징역형과 €300,000의 벌금을 부과할 수 있도록 하고 있다. 수집된 정보의 목적 외 사용은 최고 3년 징역과 €45,000의 벌금이 가능하다. 그러나 정보보호과정에서 기술적이거나 관리적인 조치를 취하지 않아 정보프라이버시의 침해가 있는 경우, 이에 따른 형사적 책임과 처벌에 대한 사례는 아직 찾아볼 수 없다.

미국의 경우에는 1984년 제정한 Computer Fraud and Abuse Act에 의해 컴퓨터 보안 및 개인정보의 불법적 접근에 대한 형사적 책임을 묻는다[22]. 이 경우에도 과실범이 아니라 문제를 지각하고 고의적으로 범죄를 행한 경우에 대해서 벌금, 1년·5년·10년 등의 징역형을 규정하고 있다. 이 법에서는 이 연구의 관심사항인 과실행동 또는 무과실 행동에 대한 처벌은 규정하고 있지 않다. 개인정보 유출 등의 사고 시에 약관에 명시된 계약불이행 등의 책임을 묻는 민사적 소송을 통한 피해 보상이라는 접근 방법이 많이 활용되고 있다. 또한 범죄를 예방하고 동시에 범죄억제의 비용을 최소화하는 방법의 일환으로 징벌적 보상제도와 집단소송제 등이 활용되고 있다.

외국 각국에서 법, 제도, 접근 방식 등이 상이하지만, 기술적·관리적 조치 미비로 인하여 야기된 정보 프라이버시 침해에 대한 형사적 처벌, 특히 징역을 벌칙의 상한으로 적시한 법과 그 적용 사례는 찾기 쉽지 않다. 이는 징역형의 성격이 정보보호관련 범죄의 예방이나 사고의 위험을 낮추기 위한 조치를 활성화하기에 반드시 필요한 제도 또는 효과적인 제도의 하나라고 인식하기에는 어려움이 있음을 반증하는 것이라 할 수 있다.

5. 결 론

정보자원의 침입, 개인정보의 불법적 이용 등과

정보보안 및 보호는 항상 공격과 방어의 상대성을 가지고 있다. 즉, 이에 따라 정보보호와 관련된 서비스는 가변성, 다차원성, 불완벽성을 지니고 있기에 효과적인 법제도의 정착을 위해서는 기존의 형법의 틀에서 자주 고려되지 않는 이러한 특성을 고려한 법을 마련하여야 한다.

개인정보의 불법적인 이용에 대한 형사처벌의 필요성은 이론의 여지가 없다. 그러나 그 처벌의 적절성과 효율성은 재검토될 필요성이 있다. 정보통신망법에서 기술적·관리적 조치의 미비에 대하여 2년 징역 또는 1천만 원 이하의 벌금을 부과하는 제73조 제1호는 정보통신망 사업자의 정보보호관리 수준의 향상과 관심의 고취, 정보보호관련 투자의 증대라는 비교적 긍정적인 효과를 가져올 수 있다.

그러나 이러한 긍정적인 측면과 함께, 타 법률과 비교하여 벌칙의 형평성 위배, 범죄 예방 및 억제의 제한적인 효과, 전문인력 유치와 양성의 어려움 가속화 등의 문제를 야기함에 따라, 이 규정의 효과성에 대한 적극적 재검토가 필요하다. 이 연구에서는 해외 사례와 국내 사례를 분석하여 필요한 정책 대안을 제시하였다. 즉, 개인정보의 효과적인 보호 및 관리를 위해서는 개인정보의 불법적 유출이 있을 때 정보보호관리 책임자의 과실책임에 대해서 징역 2년이나 벌금 1천만 원을 법정형으로 규정한 법률을 벌칙의 형평에 맞도록 개정할 필요성이 있다. 법의 개정이 이루어지기 전까지는 작량감경, 집행유예의 적극적 활용, 보다 체계화되고 구체화된 기술적·관리적 개인정보보호 조치를 보편화하고 적극적으로 수용하고 이를 자율적으로 활용할 것을 제안하였다.

정보보호법의 효과적인 입법은 개인과 기업, 정부의 권리를 적극적으로 보장하고, 또한 법률의 실효성을 높여 한층 신뢰할 수 있는 사회로 나아가는 초석이 될 수 있다.

참 고 문 헌

[1] 기광도, “법위반에 대한 처벌의 억제효과분석”, 「형사정책」, 제16권, 제2호(2004).

[2] 김정호, 이완재, 「사이버 공간의 법경제학」, 법문사, 2004.

[3] 김혜경, “전기통신기본법상 형사처벌규정의 검토”, 「법학연구」, 제18권(2008).

[4] 박상기, “형법상 법익유형과 법정형에 관한 소고”, 「형사법연구」, 제19권(2007).

[5] 서동일, “차세대 정보보호 기술”, 「정보보호뉴스」, 2003.

[6] 손동권, “법정형의 종류와 가감에 관한 한독의 비교”, 「형사정책」, 제7호(1995).

[7] 오기두, “미국의 형벌제도,” 「저스티스」, 2004.

[8] 오길영, “인터넷 통제구조에 대한 비판적 검토-정보통신망 이용촉진 및 정보보호 등에 관한 법률을 중심으로”, 「민주법학」, 제37권(2008).

[9] 오병민, “암흑의 DDoS 공격 거래 현장 포착”, 「보안뉴스」, 2009.

[10] 이준택, 「정보보호학 개론」, 생능출판사, 2007.

[11] 이창범, 김본미, 「개인정보피해구제 및 배상기준에 관한 연구」, 한국정보보호진흥원/개인정보분쟁조정위원회, 2004.

[12] 전지연, “인터넷 피싱의 형사법적 책임”, 「형사정책연구」, 제20권, 제4호(2009).

[13] 정영일, 「형법개론」, 3판, 박영사, 2009.

[14] 조용철, “정보관련 특별법 용어, 형량 제각각”, 「법률신문」, 2000.

[15] Becker, G. S., “Crime and Punishment : An Economic Approach”, *Journal of Political Economy*, Vol.76, No.2(1968).

[16] Bellia, P. L., P. Berman, and D. Post, *Cyberlaw*, 2nd ed., Thomson West, 2003.

[17] Cary, P., *Data Protection : A Practical Guide to UK and EU Law*, Oxford University Press, 2004.

[18] Cooter, R. and T. Ulen, *Law and Economics*, 5th ed., Pearson Education, 2008.

[19] Lininger R. and R. D. Vines, *Phishing : Cut-*

ting the Identity Theft Line, Wiley, 2005.

[20] Postner, R. A., *Economic Analysis of Law*, 6th ed., Aspen Publishers, 2003.

[21] Provos, N., M. Rajab, and P. Mavrommatis, "Cybercrime 2.0 : When the Cloud Turns Dark", *Communications of the ACM*, Vol.52, No.4(2009).

[22] Schwartz, P. M. and D. J. Solove, *Information Privacy Statues and Regulations*, Wolters Kluwer, 2008.

◈ 저 자 소 개 ◈

김 범 수 (beomsoo@yonsei.ac.kr)

현재 연세대학교 정보대학원 교수로 재직중이며, 지식서비스 보안과정과 ITMS과정의 주임 교수를 맡고 있다. The University of Texas at Austin에서 Ph.D.를 하고, The University of Illinois at Chicago에서 조교수를 역임하였다. 한국정보보호학회, 한국디지털포렌식학회, 한국IT서비스학회, 한국디지털포렌식학회 등의 이사이며, 전자정부 정보보호관리 체계(G-ISMS) 인증위원회, 사이버안전협의회, 한국CSO협회, 한국CPO포럼, 지식정보보안산업진흥협의회 등의 위원, 한국정보시스템 감사통제협회 부회장을 맡고 있다. 주요 연구 및 자문 관심 분야는 디지털 비즈니스, 정보통신 및 정보보호 정책과 관리제도, 공공 및 민간 기관의 개인정보보호 법과 제도, 프라이버시 보호를 위한 국제협력 등이다.