정보보호 법제도와 정보보호 서비스산업 활성화

김범수*, 이창진**
연세대학교 정보대학원

The Information Privacy Protection Law and its Impact on the IT Security and Privacy Industry in Korea

Beomsoo Kim*, Changjin Lee**
Graduate School of Information, Yonsei University
E-mail : *beomsoo@yonsei.ac.kr, **cjlee@yonsei.ac.kr

요 약

지난 2008년 6월 13일 개정된 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'은 우리나라 IT 업계의 활성화뿐만 아니라 개인의 정보를 보호하는 제도와 절차를 규정하는 매우 중요한 법이다. 이 법은 우리사회에서 정보프라이버시의 보호와 관련하여 매우 긍정적인 역할을 수행하고 있으나, 일부 규정에서는 여전히 그 영향과 효과를 종합적으로 분석하고 검토하여야 할 여지가 있다. 이 연구에서는 관련 법제도가 IT 관련 산업과 기업에 미치는 영향을 검토하고, 법 제정시 정보보호서비스 산업의 특성(예, 공공성, 가변성, 상대성, 다차원성, 불완벽성)을 보이고, 이를 반영하여야 함을 설명하였다. 또한, 정보관리자의 책임과 과실 처벌에 관한 법규의 실효성과 형평성을 분석하였다. 법의 논리 연구, 관련된 해외 법률과 사례의 분석을 통하여 세가지 정책 대안, i) 관련 법률의 개정과 새로운 정책제도 마련, ii) 선고형에서 작량감경/집행유예 등의 적극적 적용, iii) 개인정보 관련한 기술적·관리적 조치의 합리적이고 구체적인 기준 마련을 제시하였다.

1. 서론

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 유출사고는 프라이버시에 관한 사회적 관심을 확산시키고, 관련법의 개정을 유도하는 결과를 낳았다.

이 연구에서는 사례 분석을 통하여 정보보호 관리 정책 수립에 결정적인 영향을 미치는 관련 서비스의 특성을 정리한다. 또한, 2008년에 개정된 '정보통신망이용촉진 및 정보보호 등에 관한 법률(정보통신망법)'의 기능과 벌칙의 범죄 예방 기능의 효율성에 대해 검토한다. 이러한 검토를 바탕으로 국내외 법률 비교와 정보보호 관리 사례를

검토하여 현행 법률과 제도의 개선을 통한 범죄 억제 및 예방 기능 향상에 기여할 수 있는 정책 대안을 제시한다.

2. 정보보호의 공격 및 방어

정보보호 법제도의 검토에 앞서, 정보보호의 현황과 주요 시사점의 이해를 통하여, 이 연구에서 다루고자 하는 정보보호 분야와 문제의 특수성과 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[3]. "간접재화", "공공재화"의 성격외에도 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 제3의 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" 및 "상대성"을 중심으로 정리한다.

3. 정보통신망법 과실범 처벌 규정의 합리성

3.1. 형법상 처벌의 원칙

오늘날의 형법은 일반적으로 보호적 기능, 보장적 기능, 사회질서 유지 기능을 수행한다[6]. 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 사회질서유지 기능은 형벌이라는 수단에 의하여 범죄로부터 사회질서를 지키고 유지하며 보호하는 기능을 의미한다. 또한 이러한 세가지 기능이 보장적 기능의 기초 위에 시대상황이나 정치상황에 부응할 수 있도록 보호적 기능과 사회질서유지 기능을 함께 고려한다.

형벌[1]은 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.[6] 한편, 특별 예방적 기능도 있지만, 이는 이 연구의 범위를 벗어나므로 논의를 생략한다.

3.2. 형법상 범죄 처벌의 전제조건

형법은 민법과 달리 다음과 같은 처벌의 전제조건을 두고 있다[1].

(1) 의도적인 행동을 하여야 한다.
(2) 범인에 의한 피해가 개인적이며 공공적 성격을 띈다.
(3) 소의 제기 당사자는 개인이 아니라 정부이다.
(4) 일반 민사상 소송에서보다 형사소송에서는 증거에 대한 높은 수준의 검증이 필요하다.
(5) 피고가 유죄이면 처벌된다.

[1] 대한민국은 죄형법정주의(罪刑法定主義)를 따르기에, 어떤 행위가 범죄로 되는지 또 그 범죄에 대하여 어떤 형벌을 과할 것인지는 미리 성문의 법률에 규정되어 있어야 한다. 또한, 구성요건타당성, 위법성, 책임 등이 만족될 때 형법상 범죄가 성립된다. 형법이 신속성(swiftness), 확실성(certainty), 엄격성(severity)의 원칙에 따라 적용될 때 범죄 억제효과가 극대화된다.

또한, 대한민국 형법은 원칙적으로 고의범의 경우에만 처벌되고, 과실범은 각칙에 그 처벌이 있는 경우에만 예외적으로 처벌된다. 이러한 특성은 '정보통신망법'에서 형사적 과실책임에 대한 벌칙을 포함하도록 개정한 배경, 그로 인한 긍정적, 부정적 효과에 대한 포괄적이고 심층적인 검토를 통하여 향후 관련 법제도의 개선 필요성을 제기한다.

3.3. 정보통신망법상 과실범의 처벌 규정

2008년 6월 13일 일부 개정되고, 2008년 12월 14일 시행된 '정보통신망법' 제73조 1항은 '제28조 1항 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 1천만원 이하의 벌금에 처한다'라고 법정 형량을 기술하고 있다.

3.4. 벌칙 제73조 1항의 입법취지와 목적

정보통신망법 제4장은 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.

제73조 1항은 개인정보 보호를 위하여 의무화한 기술적·관리적 조치를 취하지 않아서 정보프라이버시 침해 사고가 발생하는 경우에 대해 설명하고 있다. 즉, 정범(正犯)이 개인정보를 불법적으로 이용하는 경우에 정보통신서비스제공자에게 필요한 사전적·사후적 보호 조치를 제대로 취하지 않은 것에 대한 과실 책임을 묻는 것이다.

이 조항의 제정 목적은 개인정보관리자가 보다 적극적으로 개인정보 보호의 의무를 수행하도록 하여 정보프라이버시 침해 가능성을 낮추고 궁극적으로는 사고를 예방하는데 있다고 할 수 있다.

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 정보통신서비스제공자가 관련된 인적 자원, 기술적 자원, 제도적 자원에 대한 적극적 투자와 관심이 필수적으로 동반되어야 한다. 관련 예산의 확보 및 투자를 통해 기존에 미비되었던 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 형평성 위배

정보통신망법 제73조 2항부터 8항까지 2년 이하의 징역이나 1천만원 이하의 벌금이 정보프라이버시를 침해하는 정범에 대한 벌칙을 제시하는 반면에, 같은 수준의 처벌을 법정형으로 제시하고 있는 73조1항은 과실범의 사례를 들고 있다. 또한, 개인정보의 보호를 위한 관리의 수준이 미비한 상태에서 부과되는 제76조3항 3천만원 이하의 과태료 규정과 73조2항의 정보통신망서비스제공자의

정보보호수준이 같은 경우에 제3자에 의해 개인정보가 유출된 경우 더 적은 금액의 벌금을 납부할 가능성이 있다.

4.2.2. 징역형의 제한된 억제효과

기존의 형법의 효과분석 연구[3][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) 등의 선고형으로 결정될 수 있다. 이는 법 집행의 엄격성이 상쇄된 것이다. 즉, 개인정보 유출 사고의 가변성, 다차원성, 불완벽성 등의 특성을 고려할 때, 과실범의 징역 등 신체의 자유를 구속하는 자유형 벌칙은 그 좋은 효과를 기대하기 어렵다.

4.2.3. 정보보호 전문인력 양성과 인재 확보

정보통신망법은 개인정보 관리책임자의 지정 및 관리제도의 운영을 의무화하고 있다. 그러나, 정보보호 전문인력의 양성과 수급 측면에서 전문가의 공급이 절대적으로 부족하다. 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.

4.3. 형법의 억제 및 예방 효과 개선안

4.3.1. 과실범에 대한 징역형의 완화

일반 형법의 처벌과의 균형, 해외의 사례 등을 고려하면 73조1항은 벌금형으로 개정될 필요가 있다. 또한 피해의 규모와 관리수준의 미비점 등을 고려하여 그에 상응하는 수준의 벌금형이 선고될 수 있도록 수정을 검토할 필요가 있다.

4.3.2. 작량감경과 집행유예제도의 활용

정보통신서비스사업가 관심있는 것은 법정형보다는 선고형이다. 그래서, 법의 개정이 이루어질 때까지는 법원이 필요에 따라 작량(酌量)하여 형을 감경(減輕)하여야 한다. 또한 정범이 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. 요구되는 관리의 수준을 가시화하는 제도 수립

정보보호기술은 지속적으로 변화하기 때문에, 일정수준의 관리에 대한 상세한 정보를 법령에 기술하기 어렵기 때문에 서비스제공자의 혼돈과 높은 위험의 인지로 이어질 가능성이 높다. 정부나 정보보호 협회, 학회 등 관련된 민간기구에서 적절한 수준의 기술적·관리적 개인정보보호 조치의 기준을 마련하고, 이 수준을 따른 경우 형사적 처벌을 면할 수 있도록 하는 방안을 고려할 수 있다. 또한, 산업별, 정보보호 수준별로 민간기구를 통하여 자율적으로 바람직한 관리수준을 설정하고 이

를 적극적으로 활용할 수도 있다. 이 기준이 보편적으로 확산되고 준수되려면 해당 정보통신서비스 제공자는 역시 관련 벌칙으로부터 자유로워야 한다.

4.4. 외국의 관련 법과 사례

영국은 개인정보피해에 관해서는 정보보호법과 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[5].

구체적인 관련 사례로 지난 2009년 2월 25일 Camden Primary Care Trust에서 관리하는 2,500여명의 건강정보가 수록되어있는 개인용컴퓨터가 St. Pancras Hospital내에서 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) USB메모리, 랩탑, 데스크탑 등에 저장된 자료의 암호화, iii) IT장비 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)[1]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 통지의무 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 목적외 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 '컴퓨터 사기 및 남용방지법(Computer Fraud and Abuse Act)'에 의해 컴퓨터 보안 및 개인정보의 불법적 접근에 대한 형사적 책임을 묻는다[2]. 이 경우에도 과실범이 아니라 문제를 지각하고 고의적으로 범죄를 행한 경우에 대해서 벌금, 1년·5년·10년 등의 징역형을 규정하고 있다. 이 법에서는 이 연구의 관심사

항인 과실행동 또는 무과실행동에 대한 처벌은 규정하고 있지 않다. 개인정보 유출 등의 사고시에 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 정보프라이버시 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. 결론

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 2년징역 또는 1천만원 이하의 벌금을 부과하는 73조 1항은 정보통신망사업자의 정보보호 관리수준의 향상과 관심의 고취, 정보보호 관련 투자의 증대라는 비교적 긍정적인 효과를 가져올 수 있다.

그러나 이러한 긍정적인 측면과 함께, 타 법률과의 벌칙의 형평성 위배, 범죄 예방 및 억제의 제한적인 효과, 전문인력 유치와 양성의 어려움 가속화 등의 문제를 야기함에 따라, 이 연구에서는 해외 사례와 국내 사례를 분석하여 필요한 정책 대안을 제시하였다. 즉, 개인정보의 효과적인 보호 및 관리를 위해서는 개인정보의 불법적 유출이 있을 때 정보보호관리책임자의 과실책임에 대해서 징역 2년이나 벌금 1천만원을 법정형으로 규정한 법률을 벌금형으로 다시 개정할 필요성이 있음을 제시하였다. 그리고, 법의 개정이 이루어지기 전까지는 보다 현실적 대안으로 i) 작량감경, 집행유예의 적극적 활용, ii) 보다 체계화되고 구체화된 기술적·관리적 개인정보보호 조치를 마련하고 이를 자율적으로 활용할 것 등을 제안하였다.

효과적인 정보보호를 위한 관련 법과 제도의 운영은 법의 실효성을 높일 뿐만 아니라 관련 정보통신서비스, 보안서비스 산업의 활성화를 통하여 새로운 IT기술에 대한 신뢰를 바탕으로 보다 행복한 사회로 나아가는 밑거름이 될 수 있으므로, 이러한 제도에 대한 다양한 시각에서의 고찰과 체계적인 분석이 요구된다.

[참고문헌]

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

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

[3] 기광도, “법위반에 대한 처벌의 억제효과분석,” 형사정책, 2004, 16권 2호.

[4] 박상기, “형법상 법익유형과 법정형에 관한 소고,” *형사법연구*, 2007, 19권.

[5] 이창범, 김본미, *개인정보피해구제 및 배상기준에 관한 연구*, 2004, 한국정보보호진흥원/개인정보분쟁조정위원회.

[6] 정영일, *형법개론*, 2009, 3판, 박영사.