

연이은 개인정보 유출 사고로 인한 향후 변화

이강신 건국대학교 겸임교수



1. 머리말

개인정보의 유출은 어제오늘의 이야기가 아니며 국내의 문제만도 아니다. 전 세계에서 발생하는 개인정보 유출사건을 집계하여 현황을 실시간으로 보여주고 있는 datalossDB에 따르면 2013년 한해만도 2,187건이 발생된 것으로 집계되었는데 이는 매일 평균 6건에 해당할만큼 매우 빈번하다. 이렇게 빈번하게 발생되고 있는 이유는 개인정보를 도용하여 명의 변경, 금융사기, 피싱, 스미싱, 마케팅 등을 함으로써 금전적 이득을 얻을 수 있기 때문이며 때로는 개인 사냥을 하기 위한 수단으로 사용할 수 있기 때문이다.

국내의 경우는 주민등록번호 등이 매우 식별성이 강하기 때문에 더더욱 악의적인 자가 바라볼 때는 세계 어느 곳보다도 더 매력적이라고 할 수 있을 것이다. 주민등록번호를 수집함으로써 개인을 언제든지 마음만 먹으면 찾아낼 수 있다는 점에서 전자금융,

게임 등을 비롯한 인터넷 사업자뿐만 아니라 제조업, 판매 등 전형적인 오프라인 사업자에게도 매우 중요한 정보이기 때문에 온라인이든 오프라인이든 가장 우선적으로 수집하는 대상이 되어 왔으며 악의적인 자에 의하여 도용됨으로써 각종 경제활동은 물론 사회 및 문화적인 활동을 대신할 수 있었다.

2008년 옥션, GS칼텍스 사건을 시작으로 최근에는 은행과 카드사에서 대량의 개인정보를 유출하게 됨에 따라 국가에서는 그동안 유출되었던 사건과는 비교도 되지 않을 만큼 중요하게 생각하고 있다. 또한, 국회 및 시민단체에서도 개인정보를 수집 및 이용 등 처리하는 개인정보처리자에게 막중한 법률적인 책임을 부과하고자 하는 움직임이 급격하게 일어나고 있다.

이에 본 고에서는 그동안의 유출 사건 등으로 인하여 최근 개정된 법률적 사항들과 금번 카드사고 등 금융권의 유출 사고로 촉발된 제도적인 개선 움직임에 대하여 살펴보고, 핵심 쟁점이 될 만한 사항들을

고찰해 보고자 한다.

2. 최근 개정 및 시행 예정 제도 현황

2.1 개인정보보호법

2011년 9월 30일에 개인정보를 처리하는 전 분야를 대상으로 일반법 성격으로 시행에 들어간 개인정보보호법은 시행 이후 경과된 시간이 많지 않기 때문에 최근까지는 별도의 개정에 대한 움직임이 없었다. 그러나 법 시행이 얼마 되지 않은 2013년 8월 6일에 개정되어 2014년 8월 7일부터 시행에 들어가는 사항들이 있다.

첫째, 주민등록번호를 원칙적으로 처리를 금지시켰다. 여기서 처리라 함은 법상으로 개인정보의 수집부터 파기까지 모든 과정을 처리라고 하고 있기 때문에 도래하는 8월 7일까지는 주민등록번호를 법령의 근거가 있을 경우, 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우, 안전행정부 장관이 정하는 경우를 제외하고는 수집은 물론 저장되어 있는 경우는 파기까지 하여야 한다.

둘째, 그동안 없었던 과징금 제도를 주민등록번호가 분실, 도난, 유출, 변조 또는 훼손된 경우에 5억 원 이하의 과징금을 부과 및 징수할 수 있도록 하고 있다. 이로써 개인정보처리자의 책임성을 높였다고 할 수 있다.

셋째, 개인정보처리자가 개인정보 관련 법규를 위한 시 징계 권고 가능한 '책임이 있는 자'에 대표자 또는 책임 있는 임원이 포함됨을 명확히 규정함으로써 이제는 어느 분야든지 징계가 가능한 형태가 되었다고 할 수 있다.

그리고 2016년 1월 1일부터는 부득이하게 처리해야 하는 주민등록번호는 어떤 환경에 있다고

하더라도 반드시 암호화하도록 개정되었다.

2.2 정보통신망법

개인정보가 누출되면 통지, 신고, 게시의 의무 대상을 1건 이상인 경우로 하고 있다. 2012년 8월 18일부터 시행 중인 법령으로서 개인정보보호법의 경우 신고와 게시를 1만 건 이상 유출된 경우도 한정하는 점이 다르다.

주민등록번호는 개인정보보호법과 같이 다른 법령의 근거, 본인확인기관, 영업상 목적으로 불가피하다고 방송통신위원회가 인정한 경우를 제외하면 2012년 8월 18일부터 수집을 금지하고 있고, 시행일부터 2년 이내에 파기하도록 규정하고 있어 현재 보유하고 있는 주민등록번호는 상기의 근거가 없을 경우 금년 8월 18일부터 보관되어 있으면 법적인 위반이 되게 된다.

2.3 전자금융거래법

가장 많은 내용이 개정된 분야이다. 2013년 3.20, 6.25 사이버 테러로부터 금융권이 영향을 받아 12월부터 개정 전자금융거래법 시행에 들어간 내용을 살펴보면, 해킹이 발생된 경우 이용자에게 손해를 배상, 정보기술부문 계획을 수립하여 CEO 승인 후 금융위 제출, 전자금융기반시설에 대한 취약점 분석·평가 의무화, 금융위에 '침해사고대응전담반' 운영, 법 위반에 대한 제재 수준을 영업정지까지 강화, 보안강화 요구에 불응 또는 보안인증수단의 대여 등을 고의 및 중과실 범위에 추가, 2016년 말까지 금융자산 망분리 의무화, 금융회사 내 정보보호위원회 설치 및 운영, 보안규정 위반에 따른 내부 처벌규정 마련 의무화, 내부통신망에서 파일 배포 시 무결성 검증 필수, 임직원에게 교육, 침해사고 대응 및 복구 훈련 매년 1회 이상 실시 등을 담고 있다.

또한 2013년 12월 은행, 2014년 1월 카드 3사 등의 개인정보 유출 사고로 인하여 2014년 3월 10일에 ‘금융회사 고객정보 유출 재발방지 종합대책’을 발표하게 되었다. 아직 동 대책에 근거하여 법령에 대한 개정은 되지 않았으나 현재 개정안이 활발하게 제안되고 있다.

3. 최근 개정 발의된 내용

앞서 언급하였던 것처럼 2013년 은행 고객정보 유출, 2014년 1월 카드사 고객정보 유출 건, 2014년 3월 KT 해킹 건 등이 과거 어느 때 보다도 심각한 사회문제가 되면서 국회의 의원입법안 제출이 매우 활발하게 이루어지고 있다. 개인정보보호법에서 22건, 정보

통신방법에서 8건, 신용정보보호법에서 12건, 전자금융거래법에서 4건이 제안되어 있는 상태이다. 이러한 발의된 법안의 내용은 <표 2>~<표 5>와 같다.

정보통신방법의 경우 2014년 5월 2일자로 제안된 개정 내용을 종합하여 위원회 발의로 본회의에서 통과되기에 이르렀다. 이후 동 법안은 국무회의 심의를 거쳐 대통령의 재가가 이루어지면 관보에 게시한 후 6개월 뒤에 시행에 들어가게 된다. 개정된 내용을 살펴보면 <표 1>과 같다.

이와 같이 발의된 법안들의 내용을 종합해 보면, 크게 국가 통제부서의 일원화, 책임자의 지정과 책임성 강화, 손해배상제도의 도입, 처벌의 강화 등이 핵심 사항들이라고 할 수 있다. 핵심 사항별로 내용 4장에서 살펴보기로 한다.

<표 1> 정보통신방법 개정안 주요 쟁점

변경 또는 신설 조항	미이행시 제재	비고
개인정보유출 사실을 안 때 24시간 이내에 이용자에게 통지하고, 방통위나 한국인터넷진흥원에 신고해야함 (제24조의 3)	3천만원 이하의 과태료	24시간 경과와 정당한 사유를 소명하면 과태료 부과 안됨
개인정보 파기시 복구·재생할수 없도록 해야 함 (제29조 1항)	2년 이하의 징역 또는 2천만원 이하의 벌금	73조에 정보보호인력에 해당될 수 있는 벌칙이 추가된 것임
개인정보가 유출된 경우로서 사업자가 이 법 4장(개인정보의 보호)을 위반한 경우 이용자는 300만원 이하의 법정손해배상을 청구(제32조의2)	1인당 300만원 이하의 손해배상 법원 판결	방법 4장에서 규정한 개인정보 보호조치 엄수
일정 기준에 해당하는 사업자는 정보보호 최고책임자 지정(제45조의3)	3천만원 이하의 과태료	시행령에서 기준을 정할 것임. 점검 가능
위탁자가 관리·감독을 소홀히 하여 수탁자가 제4장의 규정을 위반한 경우(64조의3 과징금 1항 5의2호)	위반행위 매출액의 3/100 이하 과징금	수탁자와의 계약과 점검 등 관리·감독 방법 검토
개인정보가 유출된 경우로서 개인정보 보호조치(28조 1항2호~5호)가 미비(64조의 3 과징금 1항 6호)	위반행위 매출액의 3/100 이하 과징금	개인정보 보호조치 관련 조항, 시행령, 시행규칙, 고시업수

<표 2> 개인정보보호법

의안 발의자	제안일자	주요내용
김경협 의원 등 12인	2014. 4. 28	수사기관이 과도하게 이용하지 못하도록 개인정보의 목적 외 이용·제공을 보다 엄격화
유대운 의원 등 17인	2014. 4. 10	공공기관의 개인정보보호 교육과 매년 실태평가 의무화
이상직 의원 등 10인	2014. 4. 7	징벌적 손해배상, 집단소송 및 배상명령제 도입
정청래 의원 등 11인	2014. 3. 18	고유식별정보 암호화에 대한 안전행정부의 정기적 조사 및 벌칙 강화
김영주 의원 등 13인	2014. 3. 13	금융분야는 안전행정부 장관의 권한을 금융감독원에 위임
박남춘 의원 등 11인	2014. 3. 7	개인정보처리방침 내용의 명확화 및 고유식별정보 등의 유출 신고 기준 하향
이원욱 의원 등 12인	2014. 2. 28	벌금형의 현실화 (징역 1년당 1천만원)
문희상 의원 등 17인	2014. 2. 19	개인정보보호법의 우선 적용, 과징금 부과 요건을 주민등록번호 누출 외 고유식별정보, 민감정보 누출로 확대, 위반행위에 대해 경제적 이익 박탈
인재근 의원 등 25인	2014. 2. 19	목적 달성 이후 10일 이내 파기, 과징금을 연간 매출액의 1% 이하 부과, 유출한 자, 유출 당한 자에 대해 징역과 벌금 2배 강화
최원식 의원 등 11인	2014. 2. 14	현행법 위반 유무와 관계없이 정보주체에 발생한 손해에 대해 손해배상책임 부담
박대동 의원 등 15인	2014. 2. 14	손해배상을 위한 보험가입 의무화
진선미 의원 등 20인	2014. 2. 14	개인정보보호와 관련된 규제 및 감독의 주체를 개인정보보호위원회로 일원화
권은희 의원 등 10인	2014. 2. 3	고의 또는 과실로 피해 발생 시 법정 손해배상제도의 도입 및 입증책임 부과
이찬열 의원 등 10인	2013. 12. 23	고유식별정보 정의를 시행령이 아닌 법으로 격상하고 암호화 조치 명시
변재일 의원 등 14인	2013. 9. 30	손해배상에 재산적 손해와 비재산적 손해를 명시
김상민 의원 등 18인	2013. 8. 27	내부통제 신설
강은희 의원 등 11인	2013. 6. 26	개인정보 파기 위반 시 처벌규정 신설
최민희 의원 등 10인	2013. 4. 12	유출신고 기준을 1만 명 이상에서 1건 이상으로 변경
정청래 의원 등 10인	2013. 3. 11	사생활의 비밀과 자유를 침해할 수 있는 CCTV 설치 시 국민에게 고지하고 기본 요건을 규정
정청래 의원 등 10인	2012. 9. 4	분쟁조정 신청 시효중단 효력의 명시
이상민 의원 등 10인	2012. 8. 29	단체소송의 즉각 제기 가능하도록 함
강기윤 의원 등 10인	2012. 8. 24	컴퓨터 화면 해킹 등 보호조치 의무화

<표 3> 정보통신망법

의안 발의자	제안일자	주요내용
임수경 의원 등 10인	2014. 3. 27	보호조치 항목을 규정하지 않고 일반화(사업자책임 강화)
박대출 의원 등 10인	2014. 3. 19	ISMS 의무대상자를 이용자 수 기준에 저장 개인정보 수 기준 추가
노웅래 의원 등 10인	2014. 3. 12	불법 이용자에 대한 통신사업자의 제한 조치 구체화 함
박대동 의원 등 15인	2014. 2. 14	손해배상을 위한 보험가입 의무화
유승희 의원 등 10인	2014. 2. 13	정보보안 최고책임자 지정 의무화
진선미 의원 등 20인	2014. 2. 12	온라인상의 개인정보보호와 관련된 규제 및 감독의 주체를 개인정보보호위원회로 일원화 (개인정보보호법도 개정하는 것을 전제)
유승희 의원 등 13인	2014. 2. 6	동의 예외사항에 대해서도 수집 후 7일 이내 통지 사생활정보 수집 금지 및 개인정보 미제공을 이유로 서비스 미제공 불가 위탁, 양도/합병 시 동의
권은희 의원 등 10인	2014. 2. 3	고의 또는 과실로 피해 발생 시 법정 손해배상제도의 도입 및 입증책임 부과

<표 4> 신용정보보호법

의안 발의자	제안일자	주요내용
김재경 의원 등 13인	2014. 4. 7	필수와 선택사항의 구분 동의
김기준 의원 등 10인	2014. 3. 31	총자산, 종업원 수 등이 대통령령으로 정한 기준에 해당하는 신용정보회사들은 신용정보 관리·보호인을 임원으로 지정
부좌현 의원 등 10인	2014. 3. 25	신용정보회사 등이 개인신용정보를 제공받는 자의 신원과 이용 목적을 확인하지 않는 등 행정상의 질서를 위반한 경우에는 과태료 2배로 상향
이학영 의원 등 10인	2014. 3. 18	집단소송제 도입
인재근 의원 등 25인	2014. 2. 19	신용정보제공·이용자가 개인신용정보를 타인에게 제공할 때 해당 개인으로부터 미리 동의를 받지 않거나 신용정보주체가 신청한 목적 외에 사용할 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 과징금 제도를 추가 도입
김영주 의원 등 12인	2014. 2. 18	개인신용정보 누설 시 통지 및 금융위원회에 신고
박대동 의원 등 15인	2014. 2. 14	손해배상을 위한 보험 가입 의무화
김용태 의원 등 10인	2014. 2. 14	금융회사 등과 업무위탁계약을 체결하여 대출상품 소개 및 상담 등의 중개 업무를 수행하는 모집인 및 금융회사에 대한 처벌 조항 신설
강기정 의원 등 18인	2014. 2. 10	징벌적 손해배상제도 도입, 집단소송제도 도입
김정훈 의원 등 11인	2014. 2. 7	신용정보 보유기간 조정, 대표자 및 임원의 책임 확보, 과징금제도 도입
김기식 의원 등 16인	2014. 2. 7	개인신용정보와 개인식별정보를 제공·활용할 때에는 매번 사전 동의를 받도록 하고, 필수적 동의 사항과 선택적 동의 사항을 구분 신용정보를 이용하거나 제공하는 경우 휴대전화 문자 메시지 등의 방법으로 정보 이용·제공 내역을 즉시 신용정보주체에게 통보
김상민 의원 등 15인	2014. 1. 29	신용정보가 유출된 경우에는 이를 신용정보주체의 손해로 보아 손해배상책임을 지도록 함
이상일 의원 등 19인	2014. 1. 28	수탁사에 대한 보호조치 강화 신용정보회사가 안전보호조치를 이행하지 아니하여 신용정보가 분실·도난·유출된 경우 등에는 해당 신용정보회사에 대하여 영업정지를 명하거나 이에 갈음한 과징금을 부과
김희선 의원 등 34인	2014. 1. 6	신용정보회사 등이 채권이 무효 또는 존재하지 않거나 소멸시효가 완성되어 채무가 없음을 법원의 판결로 확인된 경우에는 판결이 확정된 날부터 3개월 이내에 해당 신용정보를 등록관리 대상에서 삭제

<표 5> 전자금융거래법

의안 발의자	제안일자	주요내용
김기준 의원 등 10인	2014. 3. 31	정보기술부문 인력의 70% 이상은 내부인력으로 충원하도록 의무화
김기준 의원 등 15인	2014. 3. 17	전자금융거래기록이 불필요하게 되는 경우에는 이를 파기 (현재는 5년 보관 규정만 있음)
인재근 의원 등 25인	2014. 2. 19	안전성 확보의무를 다하지 못할 경우 현행 업무정지명령에 갈음하여 5천만원 이하의 과징금을 부과하고, 전자금융거래 정보를 제공·누설하거나 업무상 목적 외에 사용한 자는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처하고 있는데 이를 상향 조정
김정훈 의원 등 11인	2014. 2. 5	CISO 겸직 제한 금융사이버안전센터 지정근거 및 업무범위 등 전자금융거래정보의 유출 등에 대한 형벌 상향조정 전자적 안전성 확보의무 위반 시 과태료부과 근거마련

4. 쟁점사항

4.1 국가통제의 일원화

현재는 안전행정부가 개인정보보호법의 집행을 담당하고 있고, 방송통신위원회는 정보통신망법의 개인정보보호 분야를 담당하고, 개인정보보호위원회에서는 법률적 해석, 심의 등을 담당하고 있다.

이와 같은 구조를 개인정보보호위원회가 총괄하고 안전행정부부는 공공분야, 기타 타 부처는 해당 분야에 대하여 집행을 맡기자는 방향으로 제안되었다. 따라서 개정이 된다면 분야별 담당 부처가 집행의 권한을 행사할 수 있게 되고 이를 개인정보보호위원회에서 총괄하는 거버넌스 체계가 될 것이다

4.2 책임자의 지정과 책임성의 강화

CISO를 임원급으로 하고 있는 현행법률에서 이제는 IT 부서와 겸직을 하지 못하게 하고 있다. 더불어 신용정보 관리·보호인을 임원으로 지정하도록 발의된 것도 있다. 이렇게 함으로써 정보보호의 업무 특성상 감사 통제의 부서이기 때문에 효율성 측면보다는 통제자로서 독립성이 보장되도록 하자는 것이다.

4.3 손해배상제도의 도입

피해자로 하여금 피해 입증과 상관없이 법정 손해배상을 정부가 할 수 있도록 하자는 내용, 피해액의 최대 3배까지 징벌적으로 손해를 배상하도록 하는 내용, 손해배상을 위하여 반드시 보험을 들도록 하는 내용 등이 있다.

4.4 처벌의 강화

현행 최고 처벌보다 2~3배 정도를 높이자는 발의 건들도 수건이 되고 있다. 항간에는 이렇게 될 경우는 사회적 중대 범죄자에 대하여 법체계와 잘 맞지

않을 수 있다는 주장도 제기되고 있지만, 사회적 이슈 때문에 동 내용은 발의되었다고 할 수 있다.

5. 맺음말

최근에 대형이면서 빈번하게 발생하는 개인정보 유출은 사회적으로 큰 이슈가 되어 이에 상응하는 법안들을 다양하게 발의하고 있다. 이처럼 현재는 매우 중요한 국가적 차원의 문제이나 발의된 법안 간에 서로 적용할 기준 등이 상이할 가능성이 높은 만큼 일괄적이면서도 종합적으로 하나의 틀에서 검토하여야 할 필요성이 대두되었다.

이에 따라 관련 정부부처들은 개인정보 관련 태스크포스를 운영하고 본격적인 법률검토를 시작하고 있으며, 금년 6월경에 국회 상임위별로 계류된 법안에 대한 정부 입장을 정리하고 부처 실태점검 등을 반영한 '범정부 개인정보보호 대책' 발표를 준비하고 있다.

범정부 대책이 발표된다면 현행 법령보다도 상당한 규제가 만들어지게 될 것인데, 이로 인해 산업 발전에 저해된다고 우려하는 목소리도 있다. 그러나 개인의 기본권적인 성격이라는 점에서 규제 강화는 불가피해 보인다. 이럴 때 법률적 리스크는 바로 경영의 리스크라는 사실을 경영층이 이해하고 철저히 준수 노력을 하여 향후에는 보다 성숙된 환경이 되어 다시 법이 없어지고 자율 보호환경이 조성되기를 기대해본다. 