한국인터넷기자협회 언론개혁시민연대 시큐리티뉴스

(100-745) 서울 중구 태평로1가 25 한국언론회관 1807호 전화 02)732-7077(代) 전송 02)732-7076 http://www.pcmr.or.kr E-mail pcmr@pcmr.or.kr

[보도자료] 2008년 5월 2일

수 신 각 언론사 편집국장 · 보도국 - 미디어담당기자

발 신 언론개혁시민연대(약칭 언론연대), 한국인터넷기자협회, 시큐리티뉴스

제 목 [긴급토론회] '옥션 해킹사태와 정보인권 보호대책'

- 평소 진실보도와 언론개혁을 위해 애쓰시는 기자여러분께 감사드립니다.

- 언론개혁시민연대는 한국인터넷기자협회, 시큐리티뉴스와 더불어 최근 발생한 옥션 해킹 사태 등 개인정보 유출에 따른 정보인권 보호대책 마련을 위한 [긴급토론회] '옥션 해킹사태와 정보인권 보호대책'을 5월 2일(금) 오후 3시부터 5시까지 서울 중구 태평로 한국언론회관(프레스센터) 18층 외신기자클럽에서 개최합니다.

- 이번 긴급토론회를 통해 논란 중인 옥션 해킹 사태 등 개인정보유출 사고의 근본원인을 진단하고 개인정보보호기본법 제정 등 책임있는 사회적 대안을 논의하고자 합니다.

- 이번 긴급토론회는 옥션해킹 사태 이후 처음 열리는 공개토론회로써 의미를 지닙니다. 이번 토론회는 정부-인터넷업계-소비자-언론-법조계 등을 대표하는 인사들이 참석해 옥션 해킹 사태의 원인을 진단하고, 공론장의 책임있는 논의와 토론을 통해서 합리적인 대책방안을 도출하는 계기점을 마련할 것으로 전망합니다.

- 이번 토론회에는 진보네트워크센터 장여경 정책실장(활동가)이 '옥션해킹 사태를 통해 본 정보인권의 문제점'을, 김홍선 안철수연구소 부사장이 '해킹 등 사이버 테러와 개인정보보호 방안'에 대해서 각각 주제발제를 진행합니다.

- 토론에는 △조영훈 방송통신위원회 개인정보보호과장 △성동진 (사)한국인터넷기업협회 차장 △김학웅 변호사(법무법인 창조) △전응휘 녹색소비자연대 이사 △백의선 한국정보보호산업협회 부회장 △김동준 공공미디어연구소 연구실장 등이 참석할 예정입니다.

- 기자 여러분들의 많은 관심과 적극적인 취재, 보도를 부탁드립니다. <끝>

[긴급토론회] '옥션 해킹사태와 정보인권 보호대책'

■ 제목 : [긴급토론회] '옥션 해킹사태와 정보인권 보호대책'
■ 주최 : 한국인터넷기자협회, 언론개혁시민연대, 시큐리티뉴스
■ 일시 : 2008년 5월 2일 15~17시
■ 장소 : 서울 중구 태평로 한국언론회관(프레스센터) 18층 외신기자클럽
■ 발제 및 토론 순서

○ 인사말씀

○ 사회 : 이준희 / 한국인터넷기자협회 회장 (언론개혁시민연대 운영위원)

○ 발제

1) 개인정보 보호와 주민등록번호 : 장여경 진보네트워크센터 활동가

2) 사이버 위협과 개인정보보호대책 : 김홍선 안철수연구소 부사장

○ 토론

- 전응휘 / 녹색소비자연대 이사

- 김학웅 변호사 / 법무법인 창조

- 성동진 / (사)한국인터넷기업협회 차장

- 조영훈 / 방송통신위원회 개인정보보호과장

- 백의선 / 한국정보보호산업협회 부회장

- 김동준 /공공미디어연구소 연구실장

개인정보 보호와 주민등록번호

2008. 5. 2 토론회 <옥션 해킹사태와 정보인권 보호대책> 발제문

장여경 (진보네트워크센터 활동가)

옥션 회원 1천81만 명의 개인정보 유출 사고에 이어 업계 2위의 하나로텔레콤이 600여 만 명의 고객정보 8천530여 만 건을 유출한 것으로 드러났다. 특히 하나로텔레콤은 본사 차원의 조직적 지시로 텔레마케팅 업체 등으로 개인정보를 유출하였다는 점에서 지금까지의 사건들과 또 다른 충격을 주고 있다.
그러나 이 사건들은 우발적으로 일어난 것이 아니다. 대규모 개인정보 유출은 정보 사회의 전형적인 문제이며 반복적으로 발생하는 문제이다. 따라서 문제에 대한 분석과 대책 또한 보다 근본적으로 이루어질 필요가 있다.

1. 개인정보 유출의 사회경제적 배경

정보사회에서 개인정보 유출은 필연적이다. 수기로 기록이 이루어지고 수집되던 과거와 달리 디지털화된 정보는 대규모로 수집되고 집적될 수 있다. 가공하여 이용하기에도, 제3자에게 제공하기에도 훨씬 용이한 형태이며 그에 따른 권리 침해 또한 일상적으로 일어날 수밖에 없다. 개인정보 유출이 해킹이나 실수로 이루어지건, 아니면 의도적으로 팔아넘겨지건, 개인정보 유출, 무단이용, 조작이 대규모로 이루어질 수 있는 기술적 환경이 갖추어져 있는 것이다. 정보사회에서 개인정보 문제가 심각해지는 이유이다.
특히 온라인화에 따른 비대면 접촉이 늘어나면서 원격 거래와 원격 행정이 발달하고, 이는 곧 개인정보를 매개로 한 신원확인 요구가 사회적으로 증가한다는 것을 의미한다. 타인의 개인정보에 대한 수요 역시 과거보다 급증한다.
다른 한편으로 정보 경제의 발달로 개인정보의 상업성 또한 증가한다. 개인정보를 이용한 직접 발송우편(DM : Direct Mail) 마케팅 기법은 이미 미국 우편법이 제정된 1938년부터 널리 사용되어 왔지만, 통신 수단이 발달하면서 유선전화, 휴대전화, 이메일 개인정보를 이용한 마케팅 또한 확산되었다. 이와 더불어 기업들은 불특정 다수를 대상으로 한 대중 마케팅의 한계를 넘어 개인별 특성에 맞춘 마케팅 기법(데이터베이스 마케팅)을 개발해 왔으며, 여기서 개인정보가 매우 중요한 역할을 수행한다. 주소, 전화번호, 이메일 주소 뿐 아니라 직업, 계층, 구매이력, 취향 등 특성별로 분류한 고객의 개인정보를 보유하고 있으면, 구매력을 중심으로 한 고객관리(CRM : Customer Relationship Management)와 정교한 타겟 마케팅이 가능하다. 따라서 개인정보의 상업적 가치는 급증해 왔으며 개인정보의 확보는 기업 경쟁력의 주요 요소로 간주된다.
이런 사회경제적 배경은 종합적으로 개인정보의 수집과 이용, 그에 따른 유출을 유발하는 요인이 되고 있다.

2. 개인정보에 대한 인권규범의 발달

개인정보 유출에 따른 권리 침해로 주로 거론되는 것은 그로 인한 2차 피해이다. 즉 유출된 개인정보를 부정하게 이용한 명의도용이나 자격도용으로 경제적 손실이나 공공적 불이익이 발생할 것에 대한 우려이다. 이는 또한 사생활과 안전에 대한 위협으로 이어질 수 있기 때문에 중대한 문제임에 분명하다.
그러나 개인정보에 대한 인권규범은 개인정보의 유출로 인한 2차적인 권리 침해에 대한 문제에

서 더 나아가, 정보주체가 자신의 개인정보에 대해 권리를 행사하는 것을 기본적인 인권으로 인정하는 수준에까지 이르고 있다.
2003년 우리 사회에서 큰 논란을 빚었던 교육행정정보시스템(NEIS)와 관련한 국가인권위 결정에서 볼 수 있듯이 헌법 제17조 <사생활의 비밀과 자유>의 불가침의 내용으로 자기정보접근권, 자기정보정정청구권, 자기정보사용중지청구권을 포함한 정보관리통제권, 즉 개인정보에 대한 자기결정권이 인정되고 있다.[1)]
또한 국제적으로는 1980년 <개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인(OECD가이드라인)>과 1990년 <컴퓨터화된 개인 정보파일의 규율에 관한 UN 가이드라인>이 규범적으로 잘 정립되어 있다. OECD 가이드라인과 UN가이드라인에서 모두 공통적으로 내세우고 있는 제1원칙은 '수집제한의 원칙'이다.[2)] 개인정보의 수집은 명확한 목적 내에서 법률에 의하거나 정보주체의 동의 혹은 고지 후에 가능하다. 이러한 조건이 충족된 후에야 수집된 개인정보를 이용하고, 보호하는 것이 정당화될 수 있다. 이는 '수집'이 개인정보 보호와 관련한 첫 단계이자 가장 중요한 단계라는 것을 의미한다. 따라서 개인정보로 인한 권리 침해가 일어났을 때 우리가 가장 먼저 문제를 삼아야 하는 것은 어떤 조건에서 어떤 개인정보가 수집되었으며 그것이 어떻게 정당화될 수 있는가에 관한 것이다.
즉 개인정보 보호란 개인정보 오-남용을 방지하는 것으로 충분하지 않다. 정당한 목적을 위하여 필요한 최소한도의 개인정보만이 수집 처리되고, 그렇게 하고 있는지가 상시적으로 통제, 감독되어야 하며, 이를 위한 법제도적인 대책이 갖추어져야 개인정보 보호를 논할 수 있다.

3. 개인정보 보호와 주민등록번호

1) 개인정보로서 주민등록번호

한국사회에서 개인정보 유출 문제가 특히 심각한 이유는 주민등록번호 때문이다. 대한민국 국민은 각자 출생시 고유한 번호가 단 한번 부여되고 사망시까지 그 번호로 평생을 관리된다. 이처럼 만인부동성(유일독자성), 영구성(종신불변성), 전속성의 특성을 가진 주민등록번호는 단 한번만 유출되어도 정확히 그 주체를 겨냥한 피해가 평생토록 반복될 수 있다. 주민등록번호를 도용하면 단지 허위의 인격을 창출하여 다른 사람을 속이는 데 그치는 것이 아니라 실제 존재하는 완벽한 타인의 행세를 할 수 있는데, 피해가 발생한다 하여도 피해자는 주민등록번호를 바꿀 수 없는 상황이다. 따라서 주민등록번호는 극도의 보호가 필요한 매우 민감한 개인정보이다.
또 주민등록번호는 그 자체만으로도 다른 여타의 보조자료 없이 주민등록번호 소지자의 생년월일, 성별, 출신지 등 기본적인 개인정보를 보여주기 때문에, 광범위하고 무분별한 주민등록번호의 사용은 필수적인 개인정보를 무방비 상태로 노출하는 것이나 다름없다.
더욱 큰 문제는 주민등록번호가 수많은 개인정보 데이터베이스를 연결시키는 고리가 된다는 점이다. 한국에 존재하고 있는 개인정보 데이터베이스는 민간이나 공공 영역을 가릴 것 없이 대부분 주민등록번호를 사용하고 있다고 해도 과언이 아닐 것이다.[3)] A라는 데이터베이스에 있는 신상정보가, B라는 데이터베이스에 있는 이력정보와 결합되고, 그것이 다시 C라는 데이터베이

---

1) 국가인권위원회 2003.5.17 교육행정정보시스템(NEIS) 관련 권고.
2) Collection Limitation Principle : There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
3) 한상희 등, 「주민등록번호 사용현황 실태조사」, 2005년도 국가인권위 인권상황실태조사 연구용역보고서.

스에 있는 인터넷방문기록과 결합될 수 있는 역할을 주민등록번호가 하고 있다. 이렇게 서로 분리되어 있는 데이터베이스를 연동하고 결합하고 통합시키는 순간 특정인에 대한 완벽한 정보를 구성할 수 있다. 신용정보도, 의료기록도, 인터넷실명제 아래 글을 쓴 기록도, 모두 주민등록번호와 함께 저장되어 있으니, 주민등록번호를 통해 개인의 삶을 구체적으로 재구성[묘사]해 볼 수 있는 것이다. 어디 살고, 가족은 몇이고, 무슨 일을 하고, 어떤 성향의 글을 쓰고, 어떤 비디오들을 즐겨보는지 등. 이것이 전사회로 확대될 때 감시사회가 도래한다. 그래서 주민등록번호는 단순한 숫자조합이 아니다. 정보사회에서 인간바코드로 작용하는 것이다.
특히 이러한 개인정보 데이터베이스 통합은 정보주체가 모르는 새 이루어질 수 있기 때문에 당사자가 자신의 개인정보를 언제, 어디서, 무엇이, 얼마만큼 침해되고 있는지를 전혀 또는 거의 모를 수 밖에 없는 상황이고, 나중에 침해 사실을 알게 되어도 그 구제가 거의 불가능하다. 이러한 상황은 정보주체의 개인정보에 대한 자기결정권을 무력화시킨다. 그래서 개인정보는 정확한 목적별로 수집, 관리, 이용되어야 하며 서로 분리되어 있어야 하는 것이다.

2) 다른 나라의 개인식별번호 보호

주민등록번호는 그 활용적 측면 이전에 하나의 번호로 국민을 총체적으로 관리한다는 점에서 이미 인권침해의 소지가 있다. '시ㆍ군ㆍ구의 주민을 등록하게 함으로써 주민의 거주관계등 인구의 동태를 상시로 명확히 파악하여 주민생활의 편익을 증진시키고 행정사무의 적정한 처리를 도모함을 목적으로' 도입된 주민등록법에서 그 목적상 필요하지도 않은 개인식별번호를 부여하는 것이 위헌이라는 주장이 제기되고 있다. 현재 주민등록번호는 국가의 국민으로서 신분 또는 신원을 확인하기 위한 목적 이외에도 공공과 민간을 모두 포괄하여 개인 식별번호로서 사용되고 있는 것이다.
국가권력이 헌법적으로 충분히 통제되지 않았던 우리나라가 정보사회로 진입하면서 주민등록번호라는 기존의 잘못된 관행에 의존하여 손쉽게 국민에 관한 기록들을 전자화, 정보화할 수 있었던 것이다. 반면 외국에서는 어느 정도 국가권력이 헌법적으로 통제되고 있는 상황 하에서 국민에게 이러한 개인식별번호를 부여하는 것에 대하여 헌법적인 검토와 반대가 제기되어 왔다.[4)]
우리나라와 유사한 주민등록번호를 가지고 있는 스웨덴은 광범위한 사회보장체계를 위해서만 그 번호가 사용될 뿐, 국가에 등록된 개인정보의 범위와 사용용도가 한정되어 있다. 프랑스는 중앙주민등록시스템(NIR : National Identification Register)에 개인식별번호를 포함하고 있는데 이 번호는 강제적인 방식이 아니라 자발적인 요청에 의하여 부여되며 그 수집과 이용을 법률을 통해 엄격히 규제하고 있다.
우리나라와 비슷한 전입신고 제도를 가지고 있는 독일은 주민등록번호가 없으며 선거준비, 조세카드발급, 여권발급, 병역사항 등을 위해서 번호가 사용될 뿐이다. 미국은 주거등록제도와 개인식별번호, 국가신분증 제도가 없다. 다만 신청지역, 발급그룹, 발급순서를 나타내는 각 3자리 숫자 총9개로 이루어진 사회보장번호(SSN: Social Security Number)가 개인식별번호와 같은 역할을 하고 있지만, 사회보장번호를 민간이 이용하는 것을 금지하고 있다. 캐나다의 경우는 사회보험번호(SIN : Social Insurance Number)를 사용하고 있는데 그 용도가 벌금부과, 소득세 징수, 실업급여 등 15개 행정업무에만 사용할 수 있도록 엄격히 제한되어 있으며 그 외의 이용은 법률의 규정을 따라야 한다.
네덜란드에서는 개인확인번호(주민등록번호)가 존재하기는 하였으나 이러한 번호는 오로지 행

---

4) 김일환, "개인식별번호(주민등록번호)의 위헌성 여부에 관한 고찰", 국가인권위 주최 토론회 <주민등록번호제도 이대로 좋은가?>(2005.4.6) 중에서.

정부 내에서 사용할 목적으로만 이용되고 있으며, 일본은 주민표 코드의 민간부문 수집 및 이용을 금지하고 있다. 포르투갈은 1975년 헌법 제35조에서 '5. 시민들은 모든 목적의 국가적인 확인번호를 가져서는 안 된다'고 규정하고 있다.
즉 다른 나라에서는 우리와 같이 국민 전체에게 주민등록번호를 부여하는 데 대하여 제한을 두어 왔고, 더구나 그것을 민간기업과 공공기관에서 두루 사용하는 경우는 거의 찾아볼 수 없다. 그런데도 대부분의 국가에서는 주민등록번호 없이 시장을 보고, 은행을 이용하고, 공공서비스를 이용하고 일상생활을 영위하는 데 큰 문제가 없다.

3) 제도적 대책

우리는 오프라인 시장에서 물건을 살 때는 시시콜콜한 신상정보를 적지 않는다. 정당하게 댓가를 지불한 순간 거래 관계는 종료된다. 거래를 할 때 신원과 본인확인을 필수적인 조건으로 할 이유가 없는 것이다. 유독 인터넷에서만 주민등록번호, 휴대전화번호, 계좌번호, 심지어 취향까지 기업들이 적어내라는대로 순순히 적어내고 있다.
주민등록번호의 유출, 오남용으로 인해 소비자의 사생활과 안전까지도 위협받기에 이른 지금, 더 이상 사업자의 관리와 비용상의 편익만을 이유로 소비자 개개인의 고유번호인 주민등록번호를 수집하는 것을 허용해서는 안될 것이다.
전국민의 사분의 일에 해당하는 대규모 주민등록번호 유출 사태에 대하여 취할 수 있는 우선적인 해결조치는 원하는 사람의 주민등록번호를 변경해주는 것이다. 유출된 주민등록번호를 그대로 방치하면 앞으로의 상황이 더욱 악화될 수 밖에 없다. 피해자는 주민등록번호의 불법적 이용을 속수무책으로 보고만 있거나, 언제 어떻게 자신의 주민등록번호가 부정이용될 지 알 수 없어 전전긍긍할 수밖에 없기 때문이다.
장기적으로는 주민등록번호를 폐지하고 납세번호 등 목적별 번호로 대체해야 한다. 목적별 번호란 해당 목적으로만 사용되는 번호를 의미한다. 특정한 행정 번호는 해당 목적 내에서만 쓰여야지, 다른 목적으로 여기저기 쓰여선 안된다는 것이다.
이것이 장기적인 대안이라면, 주민등록번호의 민간 사용을 금지하는 것은 당장 도입할 수 있는 대안이다. 심지어 정부에서도 대체번호가 필요하다고 인정하고 있으니 더이상 머뭇거릴 이유가 없다. 기업이 보유한 기존의 개인정보 데이터베이스에서 주민등록번호를 삭제해야 함은 물론이다. 그렇지 않으면 의미가 없기 때문이다.

4. 개인정보보호 법제도

1) 기존의 법제도와 대책 비판

개인정보 유출 사태에 대하여 그간 정부가 내놓은 대책은 '처벌'과 '주민등록번호 대체수단'으로 요약될 수 있다.[5] 특히 주민등록번호 대체수단으로 방송통신위원회의 아이핀(i-PIN) 의무화나 행정안전부의 지핀(G-PIN) 도입이 제시되고 있다.
그러나 인터넷에서 아이핀과 같은 대체번호가 의무화된다면 그것은 제2의 식별번호이며 그것이 널리 사용되면 될수록 지금의 주민등록번호와 같은 유용성을 갖게 될 것이다. 또한 아이핀 사업자들이 개인별 사이트 가입 내역 등 민감한 개인정보를 수집하는 것은 그 자체로 개인정보 자기결정권에 대한 위협이다. 아이핀 사업자들이 보유하고 있는 개인정보가 유출되는 사상 초유의 사태가 벌어지지 않으리라고 아무도 장담할 수 없다.

---

5) 방송통신위원회, "인터넷상 개인정보 침해방지 대책"(2008. 4. 24).

아이핀 의무화는 오히려 민간에 의한 '번호' 수집을 법률에 의해 보장하려는 잘못된 결과를 가져올 것이다. 또 아이핀을 도입한다는 명목으로 실명확인 사이트를 일일방문자수 10만 명 이상 사이트 210곳으로 확대하는 것은 현재 위헌논란에 휩싸여 있는 인터넷실명제를 널리 확대하는 결과만 가져올 것이다.[6] 그러나 현재의 사태는 인터넷실명제처럼 신원 확인을 명목으로 해당 사이트의 목적상 꼭 필요하지 않은 '번호'를 비롯한 개인정보를 수집한 데서 비롯된 문제라는 점을 상기할 필요가 있다.

즉 공공부분 뿐만 아니라 민간부분에서도 주민등록번호 등 개인정보를 광범위하게 수집하고, 정부가 이를 방치함으로써, 주민등록번호의 해킹과 유출을 조장하고, 그로 인한 피해의 부담을 고스란히 피해자에게 전가시킨 데 문제가 있는 것이다. 따라서 이에 대한 대책 또한 개인정보 수집에 대한 현행 법제도의 태도에 대한 비판으로부터 이루어져야 한다.

국내 사이트 가운데 73%가 회원 가입시 주민등록번호를 요구한다고 한다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서는 개인정보를 필요 최소한으로 수집하라고 하고 있지만, 이는 선언적인 의미일 뿐, 개인정보 수집에 대한 제한이 사실상 거의 이루어지지 않는 것으로 드러났다.[7]

이러한 한계는 인터넷 영역의 개인정보 보호를 담당하는 부처나 관련 법률이 '개인정보 보호'와 '정보통신 산업 육성'이라는 두 마리 토끼, 아니 후자에 더욱 힘을 써온 데서 기인한다. 연달아 발생한 대규모 인터넷 개인정보 유출 사건으로 옛 정보통신부와 관련부처들이 기업들의 개인정보 보호 여부를 제대로 감독하지 못한다는 점은 분명해졌다. 심지어 하나로텔레콤 사건 때는 옛 정보통신부 직원들이 직접 가담했다고 하니 고양이한테 생선을 맡긴 꼴이다.

최근 개인정보보호의 사각지대를 일소하겠다며 "공공·민간을 포괄하는 개인정보보호법을 연내 제정"하고 나선 행정안전부 또한 결격임에 분명하다. 주민등록제도 소관부처로서 이 모든 사태의 책임을 피해갈 수 없기 때문이다. 특히 공공기관 사이의 '개인정보의 공동이용'을 전자정부의 개념요소로 당연시하고 있는 현 상황에서 행정안전부가 전자정부의 가치와 상반되는 개인정보보호의 가치를 충실히 실현하는 개인정보감독기구로서 기능할 것을 기대하는 것은 애초부터 무리이다.

특히 옛 정보통신부와 행정안전부는 주민등록번호를 수집하지 않았던 인터넷 업체에도 주민등록번호 수집을 의무화하는 인터넷실명제를 도입하고 국가적인 주민등록망을 그 용도로 사용하면서 사태를 키운 장본인들이다.

지금까지 한국의 개인정보 보호는 해당 업무 영역을 담당하는 정부 부처가 담당해 왔다. 공공부문은 행정자치부(행정안전부)가, 민간부문은 정보통신부가, 금융부문은 금융감독원이 담당하는 식이었다. 그러나 행정안전부는 전자정부의 주무 부처이자 경찰청의 상급 부처이며, 주민등록정보를 비롯하여 중요하고 민감한 개인정보들을 대량으로 수집하는 최대의 개인정보 수집자로 주요 감독 대상이다. 또한 정보통신부와 금융감독원은 각각 정보통신 산업과 금융 산업의 발전을 고유의 임무로 자임하면서 개인정보 보호를 소홀히 해 왔다. 더불어 지금까지 개인정보 보호를 담당해온 정부 산하 기관들은 조사권이나 분쟁조정권, 정책권고권을 가지고 있어도 당사자가 응하지 않으면 강제력을 발휘하는데 한계가 많았다. 실효성을 담보할 수 있는 조치가 뒷받침될 필요가 있는 것이다.

2) 대안적인 개인정보보호법의 제정

---

6) 현행 정보통신망 이용촉진 및 정보보호 등에 관한 법률 상 인터넷실명제 대상 사이트는 일일 평균이용자수 30만 이상의 포털과 UCC 사이트, 20만 이상의 인터넷언론으로, 총 37개이다.

7) 경제정의실천시민연합, "온라인사이트, 개인정보의 상업적활용 위반실태 고발"(2008.4.23).

지금까지의 법제도와 규제 기구의 한계를 극복하는 방안은 대안적인 법제도와 기구 마련에 있다.

특히 (통합)개인정보보호법을 제정함으로써 개인정보 보호에 대한 국가적인 규범을 마련해야 하고, 이 법에서 규정하는 감독 업무를 수행하는 전문적이고 독립적인 개인정보보호기구를 설립해야 한다.

여기서 핵심적인 논쟁지점은 개인정보보호위원회가 공공 영역과 민간 영역의 개인정보 수집부처로부터 독립적이어서 실질적인 감독 기능을 수행할 수 있어야 한다는 것이다.

이와 관련하여 <컴퓨터화된 개인 정보파일의 규율에 관한 UN 가이드라인>에서는 "모든 국가들은 열거된 원칙들의 준수를 감시할 '독립된' 기관을 설치해야만 하고 이러한 원칙들을 위반한 경우에 대비하는 처벌규정 및 개인보호규정들도 만들어야 한다.(강조 필자)"라고 명시하고 있다.[8] 1995년 발표된 EU의 <개인정보보호에 관한 유럽의회와 각료회의 지침(95/46/EC)>에서도 "각 회원국은 이 지침에 의하여 회원국이 채택한 규정의 영토내의 적용에 대한 감시를 책임지는 하나 이상의 공공기관을 설치하여야 한다. 당해 기관은 위임받은 임무를 완전히 '독립적으로' 수행한다."라고 규정되어 있다.[9]

따라서 세계 많은 국가들이 이 규범에 부합하는 개인정보보호위원회와 그를 규정한 개인정보보호법을 가지고 있다. 우리의 인권시민사회단체들의 요구 또한 여기에 맞추어져 있다.

지금까지 한국의 개인정보 보호는 해당 업무 영역을 담당하는 정부 부처가 담당해 왔다. 공공부문은 행정자치부(행정안전부)가, 민간부문은 정보통신부가, 금융부문은 금융감독원이 담당하는 식이었다. 그러나 행정안전부는 전자정부의 주무 부처이자 경찰청의 상급 부처이며, 주민등록정보를 비롯하여 중요하고 민감한 개인정보들을 대량으로 수집하는 최대의 개인정보 수집자로 주요 감독 대상이다. 또한 정보통신부와 금융감독원은 각각 정보통신 산업과 금융 산업의 발전을 고유의 임무로 자임하면서 개인정보 보호를 소홀히 해 왔다. 더불어 지금까지 개인정보 보호를 담당해온 정부 산하 기관들은 조사권이나 분쟁조정권, 정책권고권을 가지고 있어도 당사자가 응하지 않으면 강제력을 발휘하는데 한계가 많았다. 실효성을 담보할 수 있는 조치가 뒷받침될 필요가 있는 것이다.

유럽 대부분의 국가와 캐나다, 호주, 뉴질랜드 등 대부분의 선진국들은 독립적인 개인정보 전담기구에 개인정보 보호의 임무를 부여하고 있다. 특히 EU의 경우 1997년에 제정된 EU 개인정보보호칙령에서 조사권, 조정권, 제소권 및 의견개진권을 갖는 독립 감독기구의 설립을 강제하고 있다. 개인정보보호법이 제정되면, 우리도 개인정보 보호만을 전담하는 독립 기구를 갖게 된다. 이 기구는 국가 권력이나 기업으로부터 완전히 독립된 기구로서, 어떠한 다른 고려도 없이 개인정보 보호를 위해 활동할 것이다. 또한 이 기구에는 실효성을 보장하는 여러 조치들이 부여될 것이다.

2004년 인권시민단체가 제안하고 노회찬 의원이 발의하여 아직까지 17대 국회에 계류되어 있는 <개인정보보호기본법안>에서도 강력하고 다양한 개인정보보호위원회의 역할을 규정하고 있다. 위원회의 침해 조사에 응하지 않는 경우 처벌받게 된다. 위원회가 분쟁조정에서 내린 결정은 1개월 내에 항소하지 않으면 확정판결과 같은 효력을 갖게 된다. 위원회로부터 정책권고를 받은 기관이 이를 받아들이지 않을 경우 서면으로 그 사유를 설명해야 하며 그렇지 않은 경우 역시 처벌받게 된다.

또한 이 법안은 다양한 개인정보보호 규정을 포함하고 있으며, 주민등록번호와 같은 고유식별자를 보호하고[10], 개인정보에 대한 익명처리 선택권을 부여하고 있다.[11] 개인정보의 침해를 이

---

8) ⑧감독과 제재(Supervision and Sanctions) 항목.

9) 제28조 (감독기관) 1항.

10) 안 제15조(고유식별자의 보호) ①누구든지 다음 각호의 어느 하나에 해당하는 경우를 제외하고 공공기관이 개인을 고유하게 식별하기 위해 부여한 식별자(이하 "고유식별자"라 한다)를

유로 한 손해배상청구의 경우 피해자 중의 1인 또는 수인이 법원의 허가를 받아 대표당사자가 되어 소송을 제기할 수도 있다. 대량의 개인정보나 민감한 개인정보를 처리하려는 개인정보 보유자는 개인정보 데이터베이스를 새로 구축하거나 새로운 정보를 생성할 때 개인정보 사전영향평가를 신청해야 한다.

5. 나가며

개인정보의 유출은 우발적으로 발생하는 문제가 아니며 강력한 사회경제적 요인을 가지고 있다. 따라서 이에 대한 대책 또한 기술적인 수준에서 더 나아가 이러한 상황에 실질적으로 대처할 수 있는 사회 규범의 마련이 필요하다.
특히 전국민의 사분의 일에 해당하는 대규모 주민등록번호 유출 사태에 있어 원하는 사람의 주민등록번호를 변경해주는 제도적 대책이 시급하며, 민간의 주민등록번호 사용을 금지하고 목적별 번호로 대체해야 한다.
또한 전문적이고 독립적인 개인정보보호위원회의 설립을 규정한 개인정보보호법의 제정 등 개인정보보호 법제의 일대 쇄신이 필요하다. 대책이 이러한 수준에서 이루어지지 않는다면, 2년 전 리니지 사건 때와 마찬가지로 대규모 유출 사건이 또다시 발생하는 사태를 지켜볼 수 밖에 없을 것이다.

수집하거나 이용 또는 제3자에게 제공해서는 안 된다.
1. 공공기관이 법률의 규정에 따른 업무를 수행하기 위해 고유식별자의 처리가 반드시 필요한 경우로서 그 처리의 목적이 고유식별자가 부여된 목적과 직접적으로 관련이 있는 경우
2. 법률의 규정이 있거나 당사자의 동의가 있는 경우
②공공기관은 법률에 규정이 없는 경우 다른 공공기관이 부여한 고유식별자를 그 개인에 대한 고유식별자로 부여할 수 없다.
11) 안 제16조(개인정보의 익명처리) 개인정보는 익명으로 처리할 수 있으며, 이 법 또는 다른 법률의 규정에 의하여 금지되지 아니하는 한 정보주체에게 개인정보 익명처리 선택권을 부여해야 한다.

옥션 해킹 사태와 정보인권 보호 대책 토론문

Auction 有感

김학웅(변호사 / 법무법인 창조)

1. 해킹의 유혹[12)]

o 상품으로서의 정보.
o 정보의 연결고리이자 핵심으로서의 주민등록번호.
o 주민등록번호 입력을 강제하는 사회

2. 현행 법제도

o 처벌은 제대로 이루어지고 있는가?[13)]
o 손해배상은 제대로 이루어지고 있는가?[14)]
o 처벌과 손해배상은 문제의 근본적 해결책이 될 수 있는가?

3. 작금의 소송 사태

o 권리 의식의 향상? 옥션 로또?

4. 주민등록제도의 역사

o 시·도민증 : 한국전쟁으로 인한 신분확인의 필요성
o 1962. 1. 15. 기류법 제정 : 무장공비 침투로 인한 간첩 및 범죄자 색출의 목적
o 1962. 5. 10. 기류법 대체 입법으로 주민등록법 제정

5. 아이-핀(I-PIN)은 주민등록번호의 대안이 될 수 있을까?

o 개인정보 유출이 낮아질 가능성 有.
o but 문제의 근본 원인은 주민등록번호. 이 주민등록번호에 기반한 이상 미봉책.

---

12) 개인정보 유출의 유혹은 개인정보를 수집한 회사도 느낄 수밖에 없다. 하나로텔레콤 사태에서도 보여 지듯이...

13) <정보통신망이용촉진및정보보호등에관한법률> 제24조(개인정보의 이용 제한), 제24조의2(개인정보의 제공 동의 등), 제28조의2(개인정보의 누설 금지), 제48조(정보통신망 침해행위 등의 금지) 제2항, 제3항, 제49조(비밀등의 보호) 위반시 제71조에 의하여 5년 이하의 징역 또는 5천만원 이하의 벌금.
제48조(정보통신망 침해행위 등의 금지) 제1항, 제66조(비밀유지 등), 제49조의2(속이는 행위에 의한 개인정보의 수집금지 등) 제1항 위반시 제71조에 의하여 3년 이하의 징역 또는 3천만원 이하의 벌금.

14) 손해배상 소송 인용액은 20여 만원에 불과.

6. 개선 방안

o 주민등록번호 제도의 폐지, 대체입법 마련
o 과거 수집된 주민등록번호에 기반한 정보를 어떻게 처리할 것인지에 대한 고민이 입법에 반영되어야.
o 통합개인정보보호법 제정
o for 해킹의 유혹, 정보를 수집·관리하는 회사의 유출 유혹 차단

옥션 교훈과 개인정보보호의 발전방향

한국정보보호산업협회
상근부회장 백 의 선

1. 2007년의 정보보안 사고 동향

국내 최대의 전자상거래사이트인 옥션에서 현재까지 확인된 개인정보 유출건수만도 1,000만명이 훨씬 넘는다. 이는 옥션 회원의 60%로 이들의 이름은 물론 주민등록번호, 아이디, 주소, 전화번호, 계좌번호 등 핵심적인 개인정보가 그대로 유출됐다. 이중 일부는 이름과 아이디 등 부분적인 정보만 유출된 것으로 확인되고 있으나 더욱 피해가 우려되는 것은 보이스 피싱 등을 이용한 2차 피해가 발생할 수 있다는 것이다.

지난해만도 1월에 국내 굴지의 인터넷 게임인 리니지2의 이용자 개인정보가 유출됐었으며, 11월에는 대형 은행이 고객들의 정보를 유출당해 사회적 파장을 일으키기도 했다. 또한 국내 최대의 포털사도 해킹을 당해 개인정보가 유출되는 사고가 발생하기도 했다. 여기에 지난 2월에는 웜바이러스에 의한 해킹으로 국가안전보장회의(NSC) 내부의 안보관련 여론 동향, 보고서 작성 매뉴얼과 보고서 등 일부 자료가 유출되었다고 발표된 바 있다.

이번 해킹의 대상이 된 옥션은 사건 발생 처음부터 해킹사실을 알리고 개인정보유출 현황을 파악할 수 있는 통로를 마련해 회원들 자신이 개인정보유출여부를 직접 확인할 수 있도록 했다는 점에서 그나마 사건을 은폐·축소했던 과거 사례와는 다른 모습을 일부 보였다.

2007년에 국가사이버안전센터가 접수 처리한 사고 건수는 국가기관, 지자체, 연구소 등을 모두 합하여 7,588건으로 전년도의 4,286건에 비해 크게 증가했고, 특히 지방자치단체의 경우는 3,827건으로 2006년의 1,470건에 비해 3배나 증가했다. 이 통계숫치로부터 해킹수법의 진호속도에 정보보안이 뒤따라 가지 못하고 있으며, 또한 단순 해킹시도는 점차 감소하고 있으나 경제적 이익 등 의도적 공격이 급증하고 있다는 것을 유추할 수 있다.

시만텍 보고서는 유출된 개인정보나 기업정보가 소위 지하경제서버(Underground economy server)를 통해 카드인증번호나 신용카드 번호는 1~6달러, 은행계좌나 신용카드, 생년월일, 주민등록번호 등을 포함한 세부정보는 14~18달러에 거래된다고 밝히고 있다. 이렇듯 편취된 개인정보가 해커들에게 경제적 이득을 가져다 주니 갈수록 불법적인 해킹활동이 증가할 수 밖에 없을 것이다.

2. 정보보호 산업계의 대응전략

이번에도 예외없이 “정보보호”의 중요성은 대형 사고가 발생하고 나서야 기업이나 국민들이 비로서 관심을 갖는 후발투자의 성격을 보여 주고 있다. IT 강국을 자부하는 우리나라는 국민 누구나가 원하기만 하면 초고속 인터넷에 바로 접근하여 다양한 서비스를 실시간으로 제공받을 수 있지만, 안전한 정보보호환경 구축을 위한 선투자는 여전히 부족한 것이 현실이다.

선투자는 시스템에 대한 비용적 투자만이 아니라 정보보호에 대한 인식의 중요성을 확산시키는 것도 매우 중요하다. 회원유치를 통해 비즈니스 모델을 발전시켜가는 기업들은 당연히 자사가 확보한 고객의 정보를 안전하게 관리할 책임이 있는 것이다. 이를 위해서는 CEO들이 개인

정보보호에 대한 투자가 단순한 비용지출이 아닌 기업 비즈니스의 보이지 않는 성장엔진이라는 생각을 항상 해야 한다.

지난 2003년 1.25 인터넷 침해사고를 깃점으로 현재까지 정보보호를 위한 제도적 장치로는 중요정보통신기반시설에 대한 취약성 분석·평가, 주요 인터넷 사업자에 대한 안전진단, 정보보호관리체계 인증, e-Privacy 인증마크 등이 운용되고 있다. 그럼에도 불구하고 대형 정보유출 사고가 늘고 있는 것은 무엇을 의미하는가? 그것은 개인정보를 다루는 조직 책임자와 구성원들의 정기적인 교육 등 체계적 관리가 무엇보다 중요함을 보여 준다.

이를 위해서는 기업의 개인정보보호 관리를 적정하게 규율할 수 있는 개인정보보호법의 제정을 서둘러 대형 포털이나 게임, 금융 등 개인 정보가 유출되기 쉬운 대상들은 최소한의 정보보호관련 시스템과 장비를 의무적으로 구축하고 정보보호담당관(CPO)를 지정하여 개인정보를 안전하게 관리하는 상시 관리체계를 구축해야 할 것이다. 또한 평가인증기관들은 서류 중심의 정보보호 수준 평가로는 보안사고를 충분히 예방할 수 없으므로 현장 평가가 이루어져야 한다. 더구나 정보보호를 감리할 수 있는 국내 전문가의 수는 불과 250여명으로 향후 인터넷 의존도가 더욱 가속화될 것임을 감안한다면 2012년까지 현재의 10배인 2,500명 수준의 정보보호 컨설팅 전문인력을 시급히 양성하여 각종 정보보호 감리수준의 고도화에도 대비해야 한다.

끝으로 기업의 일반직원이나 국민들도 평소에 자신의 개인정보가 유출되지 않도록 각별한 관심과 주의를 기울여야 하며, 아울러 악성 메일에 대해 세심한 배려를 요한다. 이를 위해 자신이 가입한 사이트의 비빌번호를 주기적으로 변경하고 개인 PC에도 최소한의 안전장치를 마련하는 등의 정보보호의 생활화가 무엇보다 필요하다. (끝)