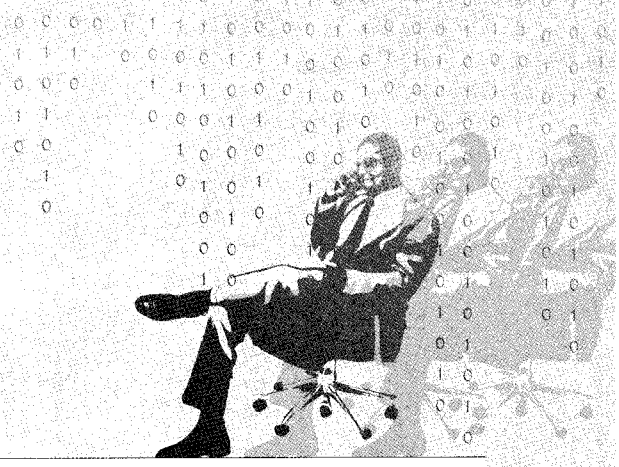
Ambulance Chaser와 개인정보보호

금년 들어 미국의 신용카드 결제처리업체인 하트랜드 페이먼트 시스템즈(Heartland Payment Systems)에서 사상 최악의 신용카드 정보 유출 사건이 발생했으며, 이로 인한 금융 피해금액이 수억 달러에 이를 것으로 추산되고 있다. 이 회사는 매달 1억 건에 달하는 신용카드 거래를 처리한다고 하니 그 유출된 개인 금융정보의 양은 상상을 초월할 것으로 보인다. 이렇게 유출된 정보는 카드복제, 신용도용 등 쉽게 예상할 수 있는 범죄 이외에도 어떠한 형태의 범죄로 당사자들에게 피해가 되돌아 올 지는 가늠하기 어렵다. 최근 국내에서 발생한 일련의 개인정보 유출사건과 마찬가지로 정보화와 개인정보보호 문제에 경종을 울리는 또 하나의 사건이라 하겠다.



김일섭 | 한영회계법인 상무_ Il-Seop.Kim@kr.ey.com

개인정보보호는 개인의 문제가 아니다

미디어의 바다라고 표현되는 지금 세상에서 우리는 자신의 몹시도 민감한 정보를 제공하는 대가로 전자메일, 인터넷 뱅킹, 인터넷쇼핑, VoIP, 영상전화, 인터넷 예매 등 엄청난 생활의 편익을 누리고 있다. 심지어 어느 생존게임에서처럼 전혀 집 밖으로 나가지 않고 인터넷으로만 필요한 모든 것을 해결할 수 있다고 할 만큼 말이다. 얼마 전까지 우리는 이러한 편익의 이면에 감내해야 하는 불편과 비용에 대해서는 별로 관심을 두지 않다가, 국내에서도 하루가 멀다 하고 터져 나오는 개인정보 유출 사건과 그로 인한 피해 소식에, 그 불편과 비용이 생각보다 크다는 걸 여실히 느끼고 있다. 원하지 않는 텔레마케팅의 대상이 되어야 하고, 스팸메일과 스팸메세지에 시달려야 하고, 바이러스 감염위험에 불안해 하고, 명의와 신용을 도용당해야 하고, 그에 따른 시간과 금전의 손실을 입어야 한다.

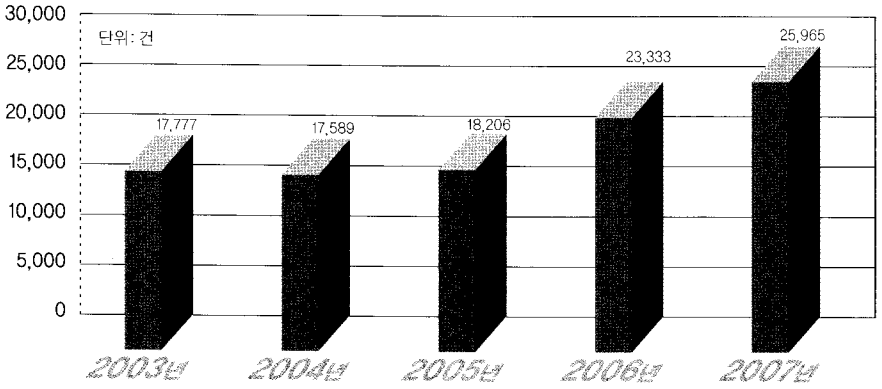
이러한 불편과 비용은 왜 발생하는 것일까? 서비스 제공자가 고객정보를 많이 가질수록 세분화된(합법적이든, 불법적이든) 타깃 마케팅을 통해 더욱 많은 수익을 올릴 수 있고, 합법적인 방법보다는 불법적인 방법으로 많은 개인정보를 더욱 쉽고 저렴하게 수집할 수 있기 때문이다. 그리고 이제는, 서비스를 제공하지 않고도 개인정보를 불법으로 이용하여 거액의 돈을 벌 수 있는 방법과 사례가 늘어가면서 이런 방법을 택하는 사람이 점점 많아지고 있기 때문이다.

어느 글로벌 컨설팅사의 조사에서 전 세계는 지난 3년간 개인정보 침해사고로 약 2.8억 명의 개인정보가 유출된 것으로 집계되었으며, 2007~2008년 동안 악의를 가진 해킹에 의한 개인정보 유출은 약 6천만 명으로 추정되고 있다. 국내에서도 얼마 전 옥션 해킹 사건으로 1,080만 명의 개인정보가 유출된 것을 포함해 우리나라 전 국민 50% 이상의 개인정보가 이미 유출된 것으로 추정된다. 정보화의 진전으로 이러한 개인정보 침해의 위험은 전 사회의 위험요소가 되어가고 있으며, 이 위험요소가 해결되지 않는다면 금융, 시장거래, 의료, 교육 등 서비스 전반에 대한 신뢰는 상실될 것이고, 개인의 피해를 넘어 사회 전체의 기반이 흔들릴 수 있다는 데 그 심각성이 있다.

국내 개인정보 유출 사건들과 관련해 알려진 개인정보 유출 원인은 참으로 다양하다. 개인정보 파일 암호화 소홀(엔씨소프트), 개인정보 파일을 실수로 메일에 첨부하여 발송(국민은행), 채용사이트에서 타인의 개인정보 조회 제한 기능 미비(LG전자), 회원정보 파일 해킹(옥션), 고객정보의 고의적 불법이용(하나로텔레콤), 고객정보 사이트 보안 소홀(LG텔레콤), 메일주소 유출(다음), 내부직원의 조작(GS 칼텍스) 등등. 마치 이처럼 다양한 방법으로 개인정보가 유출될 수 있다는 것을 깨우쳐 주려는 듯하다. 이러한 사례들 중 외부 해커의 기술에 의한 유출은 옥션의 경우밖에 없고, 나머지는 모두 기본적인 보안에 소홀했거나, 내부직원에 의한 불법적인 불법이용, 실수 또는 조작 때문이라는 것이 흥미롭다. 옥션의 경우 최신 해킹기술에 의한 것인지, 기본적인 보안취약점 때문인지는 아직 알 수 없다.

여기서 기업에 의한 정보유출만을 언급했지만, 기업을 경유하지 않고 개인의 정보가 유출되는 경로는 훨씬 다양하며, 많은 경우 자신의 정보가 유출되고 있다는 것을 의식하지 못하는 사이에 유출되기도 한다. 굳이 바이러스, 스파이웨어라든가 피싱(Phishing), 파밍(Pharming) 같은 사기에 눈뜨고 당하는 사례가 아니더라도 다음과 같은 사례에 머리가 끄덕여진다.

- 연말정산을 위한 기부금 영수증을 요청하면 성명, 주소, 주민등록번호, 전화번호 등을 모두 요구한다.
- 동네 마트에서 주최하는 경품행사에 참여하기 위해 경품권에 성명, 전화번호, 주소를 적어 제출한다.
- 차량 접촉사고가 났을 때 피해자는 당연한 듯이 성명, 주민등록번호, 전화번호를 요구하고, 가해자는 순순히 알려준다.



연도별 개인정보 침해건수 ▲

한국정보보호진흥원 통계분석 자료에 따르면, 국내에서 2005년 이후 개인정보 침해신고 건수가 급격히 증가해 2007년에 약 2만 6천 건이 집계되었고, 이러한 추세로 보아 2008년도에는 3만 건에 육박했을 것으로 추정된다.

여기에는 신용정보 침해, 주민등록번호 등 도용, 개인정보의 동의없는 수집 및 이용제공, 동의철회 불응 등이 모두 포함된다. 그런데, 이는 자신의 개인정보가 침해되었음을 인지하고 신고한 것만 집계된 것이며, 인지하지 못했거나 인지했지만 신고를 포기한 경우까지 고려할 때, 2008년의 경우 매일 100건 이상의 개인정보 침해가 발생하고 있다고 할 수 있을 것이다.

이렇게 기업의 잘못으로, 또는 개인의 잘못으로 유출된 개인정보 중 누구의 것이 불법 사용되어 당사자에게 어떠한 피해로 나타날 지는 아무도 모른다. 기업에 의한 개인정보유출 사건이 발생하면 당사자인 개인은 향후의 피해 가능성 때문에 집단소송을 제기하지만, 정작 그 피해가 발생할 것인지, 발생한다면 얼마나 클 것인지에 대해서는 전혀 예상을 하지 못한 채 안개 속에서 소송을 진행해야 하는 한계성을 갖게 된다.

집단소송의 긍정적인 면과 부정적인 면

2008년 12월에 개정된 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'을 비롯하여 국내의 많은 정보보호 관련 법률에서 개인정보 보호를 위한 규제가 점점 강화되고 있으며, 기업들에게 무거운 개인정보 보호책임을 지우고 있다. 이에 따라 규제대상이 공공기관, 단체 등으로 확대되고, 보호대상은 수기문서까지 포함되며, 개인정보 처리자에 대한 의무와 처벌이 대폭 강화될 예정이다.

일반 사용자들의 개인정보에 대한 의식 향상과 함께 이러한 규제 강화에 힘입어 중요한 개인정보 유출 사건이 발생할 때마다 어김없이 집단소송이 제기되고 있다. 미국에서는 오래 전부터 개인정보 유출과 관련한 집단소송이 일상화되었으며, 앞서 언급한 하트랜드 페이먼트 시스템즈사의 고객정보 유출 사건과 관련해서도 이미 집단소송이 제기되었다. 국내에서도 2005년 5월 엔씨소프트의 리니지 온라인게임 회원 정보유출 사건 이후 여러 건의 집단소송이 진행되고 있다.

▼ 개인정보 유출로 인한 집단소송 일지

회사명	일시	정보유출 건수	집단소송 진행상황
GS칼텍스	2008. 9	1100만 명	검찰 무혐의 처분
다음	2008. 7	55만 명	소송인단 모집중(1인당 30~50만원)
LG텔레콤	2008. 4	780만 명	1인당 100~200만원 소송 진행중(수만 명 예상)
하나로텔레콤	2008. 4	600만 명	1인당 100~200만원 소송 진행중(수만 명 예상)
옥션	2008. 2	1080만 명	1인당 100~200만원 소송 진행중(13만 명 1심 진행)
LG전자	2006. 9	2만 명	240명에 30만원씩 배상 판결(항소심), 상고중
국민은행	2006. 6	3만 명	1000여 명에 20만원씩 배상 판결(2심)
엔씨소프트	2005. 5	40~50만 명	3명에 10만원씩 배상 판결(2심)

가장 오래된 엔씨소프트 사건의 경우, 2심에서 3명에게만 10만원씩 배상하라는 판결이 났지만, 4년 가까이 끌어 온 소송은 좀처럼 종결되지 않을 듯하다. 다른 집단소송 건에 대해서도 마찬가지로 상당히 오랜 기간 소송이 진행되면서 언론과 세인의 관심을 끌게 될 것이며, 지속적으로 해당 기업의 이미지에 부정적인 영향을 미칠 수밖에 없다. 설사 해당 기업이 소송에서 이기더라도 실추된 이미지는 단기간에 회복되지 않으며, 그 때까지 매출 감소 등 이미 많은 유무형의 손실을 입게 된다. 또한, 하나로텔레콤은 집단소송 결과에 관계없이 방송통신위원회로부터 40일간의 영업정지 처분을 당하기도 했다. 가장 염려스러운 것은 수만 내지 수십만 명이 집단소송에 참여한 사건의 경우 해당 회사의 존폐를 좌우할 만큼 막대한 손해배상을 해야 할 수도 있다는 것이다.

개인정보 유출로 인해 예상되는 피해를 고려할 때 고객정보 보호의 책임을 다하지 못한 기업에 준엄한 책임을 묻는 것은 당연하며, 우리는 이제 그럴만한 의식수준에 도달해 있다. 사실, 고객들이 기업에 개인정보를 제공하지만 그 고객들이 자신의 개인정보가 어떻게 이용되고 얼마나 보호되고 있는지에 대해서는 전혀 정보를 얻을 수 없는, 이른바 정보의 비대칭성(Asymmetric Information)이 존재한다. 따라서 우리가 기업의 잘못에 대해 책임을 묻는 관행이 정착될수록 기업은 개인정보를 보호하기 위한 노력을 강화하기 마련이므로 이러한 정보의 비대칭성을 어느 정도 해소할 수 있을 것이다.

실제로, 개인정보 유출사건에 연루됐던 상기 회사들은 그 후 정보보호 전문가를 영입하거나 컨설턴트를 고용하여 정보보호 수준을 진단하고, 정보보안위원회를 구성하고, 보안 규정 및 절차를 보완하고, 자산의 등급별 관리체계를 수립하고, 고객정보보호 프로세스를 개선하고, 보안사고 대응 프로세스를 갖추는 등 전사적인 정보보호 관리체계 구현을 위한 투자를 완료했거나 진행하고 있다. 따라서 개인정보 유출로 받게 될 피해에 대한 정당한 보상은 물론이고, 우리가 제공한 개인정보의 안전을 보장받을 정당한 권리를 행사하여 기업으로 하여금 정보보호를 강화하도록 유도한다는 점에서 집단소송은 매우 긍정적인 측면이 강한 소비자 행동이다.

그런데 문제는, 개인정보 유출 피해자들의 정당한 목적 및 필요성과 함께 정당하지 못한 목적이 개입되어 무분별하게 집단

소송을 확대하고 부추김으로써, 극단적인 경우 건실한 기업을 그 부작용의 여파로 무너뜨리는 지나친 결과를 가져 올 가능성 또한 높다는 데 있다. 또한 이러한 집단소송 추세는 집단소송을 유도하기 위한 의도적인 개인정보 유출로도 번지고 있다. 최근 발생한 고객정보 유출 사건의 피의자들이 "정보유출을 문제화해 피해자들의 대규모 소송을 유발시킬 계획"이라고 밝힌 대목에서 우리는 앞으로 유사한 사례가 많이 발생할 수 있음을 감지할 수 있다.

개인정보보호 책임을 소홀히 한 기업이 쓰러지는 것은 그럴 수 있다고 하더라도, 많은 사회적 책임을 이행해 왔고, 개인정보보호 책임을 다하려 노력하는 기업들까지 정당하지 못한 소송참여자들에 의해 큰 피해를 입게 된다면, 우리가 얻고자 하는 바에 비해 사회적으로 엄청난 손실을 초래하며, 이는 곧 우리 자신에게 돌아오게 될 것이다.

그리고 집단소송과 관련하여 물론 법원에서 가장 합리적인 판단을 할 것으로 믿지만, 그 이전에 소송을 제기하는 변호사를 포함하여 집단소송에 참여하는 모든 이들이 건전한 양식을 발휘하여야 한다. 하나의 사건에 대해 100개가 넘는 인터넷 카페에서 무분별하게 소송단을 모집하여 소송을 제기하고, 정작 피해자들에게는 남는 게 없도록 만드는 변호사 성공보수 조건 등은 집단소송의 긍정적인 측면을 고려하더라도 우리를 씁쓸하게 한다.

정보화와 개인정보보호의 조화

사실, 지금까지도 일부를 제외하고는 우리 기업들의 개인정보보호에 관한 의식수준과 노력은 상당히 낮은 편이다. 한국정보보호진흥원이 2008년도 한 해동안 실시한 정보보호관리체계인증(ISMS) 심사분석 자료에 의하면, 심사대상 중 약 63%의 기업에서 정보자산 보안관리에 중요한 취약점이 있는 것으로 나타났다. 그 밖에도 사용자 계정관리, 비밀번호 설정, 암호화 등 가장 기본적인 정보보호 활동에서도 결함을 가지고 있음을 보여주고 있다. 필자는 연간 약 200개 기업의 IT감사를 수행하고 있는데, 여기에서도 앞서 밝힌 한국정보보호진흥원의 심사분석 자료와 유사한 결과를 보이고 있다.

이 밖에도, 금융위원회가 국가정보원에 전달한 '2008년도 정기 보안업무 지도점검 실시결과' 보고서에서도, 국내 대표적인 시중은행을 포함하여 일부 금융기관의 보안업무에 적지 않은 허점이 있는 것으로 드러났다. 금융기관에서는 정보보호를 위한 인력, 조직, 장비에 일반기업보다 상대적으로 많은 투자를 하고 있음에도, 금융기관 해킹 사건 뉴스가 심심치 않게 들리고 있다. 이는 금융기관에서부터 아직도 고객의 정보보호를 위해 많은 보완이 필요하다는 것을 말해주고 있다.

집단소송에서 현재 우리나라는 선정당사자 제도를 적용하고 있어 소송에 참가한 당사자들만 피해보상을 받을 수 있는 반면, 미국은 일괄구제제도를 적용하고 있어 피해자 대표가 소송을 제기하여 승소하는 경우 소송효력이 이해당사자 전체에 미치게 되므로, 그 결과가 기업에 미치는 영향은 실로 심대하다. 우리나라에서도 일괄구제제도를 채택해야 한다는 목소리가 점점 높아지고 있는 상황이며, 만약 그렇게 될 경우 기업이 개인정보 유출로 인한 집단소송에서 상당한 책임이 인정된다면 그 기업의 지속가능성은 더 이상 이야기할 수 없을 것이다.

정보화 사회에서 기업이 정보유출 가능성을 완벽하게 차단하는 것이 불가능하다는 것은 우리 모두 아는 사실이다. 하지만, 실제 정보유출 사건 앞에서 이 항변은 전혀 기업을 방어해 주지 못한다. 다만, 기업은 개인정보 보호를 위해 해당 기업의 상황에서 최선의 조치를 취했고, 고의와 과실이 없었다는 것을 스스로 입증해야 정보유출의 책임을 최소화할 수 있다. 그러기 위해서는 우리 기업들의 '사건이 터져야만 대책을 찾는' 위험 불감증을 이제 빨리 치유해야 하며, 가장 후순위로 미루어 두었던 투자순위 목록에서 이제 정보보호체계 수립 과제를 가장 위에 올려놓아야 하지 않을까 한다. 앞선 사례를 타산지석으로 삼아 '소 잃고 외양간 고치는' 우(愚)를 반복하지 말아야 할 것이다.

아울러 개인정보 제공자는 기업으로 하여금 개인정보를 필요한 만큼만 수집하고 수집된 개인정보를 최선을 다해 보호하면서 적절히 이용하도록 채찍을 가해야 한다. 하지만 집단소송이 두려워 개인정보 수집을 포기하거나, 수집된 정보를 깊이 묻어두고 이용을 포기할 만큼 과도한 채찍을 가한다면 달리던 말은 결국 쓰러지고 말 것이다.

정보화와 개인정보보호는 동전의 양면이지만, 우리는 어느 한 쪽도 포기할 수 없다. 지금 당장 모두에게 만족스런 방안이 만들어질 순 없겠지만, 동전의 양면을 모두 조화롭게 아우를 수 있도록 기업, 개인, 정부가 모두 지혜를 짜내야 할 때다.