2003년도 인권상황 실태조사
연구용역 보고서

금융기관과 인터넷에서의 개인정보 공유현황 실태조사

국가인권위원회

금융기관과 인터넷에서의 개인정보 공유현황 실태조사

2003년도 인권상황실태조사 연구용역 보고서를 제출합니다

2003. 10. 13.

연구수행기관 함께하는 시민행동

책임연구원 김 동 노

연구원 하 승 창

김 영 홍

최 인 욱

목 차

표 목 차

그 림 목 차

요 약 문

정보화 시대의 도래와 더불어 개인의 프라이버시에 대한 우려가 커지고 있다. 특히 많은 학자들은 민간 영역에서 구축되는 개인정보 데이터베이스가 프라이버시에 가져오는 위험이 매우 심각해질 것이라고 전망하고 있다. 기업이 보유한 개인정보는 고객 중심 마케팅으로의 전환을 가져오기도 하지만, 다른 한 편으로는 개인정보의 유출로 인한 정신적·물적 피해를 야기하는가 하면, 스팸메일로 인한 스트레스에서부터 소비 실적에 따른 등급화, 타켓 마케팅을 통한 소비자 조작화 등 인간성 자체에 대한 위협으로까지 발전할 수 있다.

본 연구는 금융기관과 주요 인터넷 기업들의 개인정보 보호 실태와 관련 법제를 조사함으로써, 민간 영역의 개인정보 보호와 관련된 문제점을 점검하고 바람직한 환경을 만들어내는 것을 목표로 했다. 우선 개인정보 보호의 의미를 밝히고 이 개념에 비추어 개인정보 보호와 관련된 소비자의 의식과 태도를 확인했다. 이어 금융기관과 인터넷 기업들의 실제 개인정보 보호 실태를 프론트 오피스 차원과 백 오피스 차원으로 나누어 살펴보았다. 프론트 오피스 차원으로는 웹 사이트에서의 개인정보 수집 실태와 약관 / 개인정보 보호정책 게시 상태를, 백 오피스 차원으로는 고객 데이터베이스를 다루는 직원들에 대한 관리 방식과 기술적 대책을 검토했다. 이어, 관련 법제를 검토한 후 연구진이 생각하는 바람직한 방향을 가이드라인으로 제시했다. 조사대상은 금융기관이 40곳(은행 11, 카드 9, 보험 10, 증권 10), 기타 인터넷 기업이 30곳(포탈/커뮤니티 10곳, 쇼핑몰 10곳, 언론사 10곳)이었다.

본 연구에서 프라이버시 보호, 혹은 개인정보 보호라 함은 자기정보통제권이 실현되는 상태를 의미한다. 19C 후반 '혼자 있을 권리'로서의 고전적 프라이버시 개념 대신 등장한 자기정보통제권은 '자신에 관한 정보를 언제, 어떻게, 어느 정도 타인에게 유통시킬 것인지를 스스로 결정할 수 있는 권리'이다. 이 권리를 구체화한 것으로 대표적인 것이 1980년 OECD가 제정한 「개인데이

터의 국제유통과 프라이버시 보호에 관한 가이드라인』이다. 이 가이드라인에서 발표된 8가지 원칙(수집 제한, 정보내용정확성, 목적 명확화, 이용 제한, 안전성 확보, 공개, 개인 참가, 책임의 원칙)이 본 연구의 기본 개념이자 실태 조사의 기준이 되었다. 다만, OECD 가이드라인의 한계인 '계약 주체간의 정보 불균등' 상태를 극복하기 위해 집단적 참가·감독권 혹은 역감시의 권리를 도입할 것을 검토했다.

1. 개인정보 보호에 관한 이용자들의 의식과 태도

1,042명의 네티즌들을 대상으로 개인정보 보호에 관한 이용자들의 의식과 태도를 조사해 보았다.

먼저 자기정보통제권을 제약하는 정보처리 관행에 대해 조사한 결과, 인터넷 사이트 회원 가입 시 가장 입력을 꺼려하는 정보는 주민등록번호가 75.0%로 가장 높게 나타났다. 다음으로 핸드폰번호 8.2%, 전화번호 4.5%, 이름 4.4%, e-mail 주소 2.8% 등의 순이었다. 회원 가입 시 주민등록번호를 요구하는 것에 대해, 유출되지 않는다는 보장이 있다 하더라도 실명확인이 필요한 경우에만 수집해야 한다고 대답한 사람이 42.9%로 가장 많았고 주민등록번호를 대체할 만한 방법이 있는 한 수집하지 않아야 한다(41.5%)는 응답도 높게 나타났다. 인터넷 사이트에 회원 가입 시 주민등록번호가 도용되어 회원가입이 실패한 경험에 대해 질문한 결과, 네 명 중 한 명꼴(26.6%)로 주민등록번호가 도용된 경험이 있는 것으로 나타났다. 온라인 회원 탈퇴 시 신분증 사본이나 주민등록등본 제출을 요구한 사이트는 전체적으로 22.3%에 이르렀다. 또, 텔레마케팅 전화를 받았을 때 개인정보의 수집 경위에 대해 설명을 들은 비율이 50%미만인 경우가 86.8%에 달했다. .

개인정보보호정책·약관에 대한 이용자들의 관심도는 매우 낮은 것으로 나타났다. 회원가입 시 이용약관을 "꼼꼼히 읽어보는 편이다"라고 응답한 비율은

8.3%에 불과했고 “거의 읽지 않는 편이다”가 무려 57.0%로 나타났다. 이러한 현상은 개인정보보호정책에도 마찬가지였다. 이용약관을 읽지 않는 이유를 설문한 결과 양이 지나치게 많다(53.2%)는 응답이 가장 많았으며, 어느 사이트나 내용이 거의 같다(21.9%), 안 읽어도 별다른 문제가 발생하지 않는다(19.2%), 구체적인 정보를 주지 않고 있다(5.1%) 등의 순이었다. 개인정보보호정책의 경우에도, 동일한 패턴을 보여주었다.

이용자들이 약관에서 중요하게 생각하는 부분은 요금관련사항(62.7%)인 것으로 나타났으며, 개인정보 관련 사항(45.6%), 이용자권리 관련 사항(36.7%), 물품구매 관련 사항(8.0%)의 순서로 나타났다. 한편 개인정보보호정책에서 이용자들이 주로 관심을 가지고 읽는 내용은 가입, 탈퇴에 관한 사항(57.0%), 이용자 권리 관련 사항(56.4%), 제3자의 공유 관련 사항(15.5%), 등이었다.

개인정보 공유에 대한 서비스 제공자의 고지 및 이용자의 이해 부족이 심각했다. 자신이 주로 이용하는 인터넷 사이트에서 개인정보가 공유되는 업체의 수를 안내 받았는지 여부를 묻는 질문에 모든 사이트에서 80% 이상이 안내 받지 못했다고 답했으며, ‘자신의 개인정보가 공유되는 업체가 몇 개인지 아는가’라는 질문에 대해서는 90% 안팎이 모르고 있다고 답했다.

스팸 메일 실태에 대한 조사에서는, 하루에 10회 이상 스팸 메일을 수신하는 경우가 전체의 45.2%에 이르고 있으며, 하루 1회 이상 수신하는 경우는 73.4%였다. 스팸 메일이 이렇게 대량으로 살포되고 있는 반면 이용자들의 대응은 상당히 소극적인 것으로 나타났는데, 80.5%에 이르는 응답자들이 스팸 메일을 수신하는 경우 그냥 지워버린다고 답했다. 이용자의 소극적 대응은 수신거부의 효과가 크지 않기 때문인 것으로 조사되었다.

기업의 개인정보 관련 고충 처리 업무는 크게 전화, e-mail, 상담게시판 등의 형태로 이루어지고 있었는데, 응답자의 87.8%가 문제를 제기한 경험이 없는 것으로 나타나 이용자들이 개인정보의 관리로부터 야기되는 문제에 대단히 소극적으로 대응하고 있음을 알 수 있다. 한편, 기업의 개인정보 고충처리 체계에 대한 고객들의 만족도는 매우 낮은 것으로 조사되었다.

2. 기업의 고객 자기정보 통제권 보장 실태

인터넷 사이트에 게재된 약관과 개인정보보호정책을 통해 조사한 결과, 전체 67개 조사대상 기업의 2/3 이상이 개인정보 수집의 구체적인 목적을 명시하고 있지 않은 것으로 나타났다. 개인정보의 구체적인 수집목적을 설명하되, 개별항목과 직결시켜 설명하지는 않는 곳이 25곳(37.3%)으로 가장 많았다. 한편, 아동의 개인정보 수집에 대한 부모 동의권을 명시하지 않고 있는 곳은 총 11개 기업으로 전체의 16.4%였다.

조사 대상 사이트중 95.5%의 사이트에서 개인정보의 보유기간을 제시하고 있으나 그중 45개(전체의 67.5%)가 탈퇴하면 개인정보를 삭제하겠다는 식의 일반적 수준으로 보유기간을 제시하고 있었다. 비회원 거래자의 개인정보 보존 연한을 제시하고 있는 곳은 단 한 곳도 없었다.

약관 및 개인정보보호정책의 변경 시 안내하는 방법은 홈페이지 게시가 59.37%로 가장 많았다. 약관 및 정책의 변경에 대한 고지 방식에 대한 안내는 비교적 잘 나와 있는 반면, 약관 및 정책 변경시 동의를 구하는 방식에 대한 안내를 하지 않는 곳이 14.9%로 상대적으로 미흡했다. 약관 및 정책의 변경시 동의 방식을 안내한 85.1%는 모두 소극적 동의 방식을 채택하고 있었다.

개인정보 보호를 위한 기술적 대책을 비교적 구체적으로 제시하고 있는 곳은 총 49개로 73.1%였다. 기술적 대책을 전혀 제시하지 않거나, 제시하더라도 추상적 기술에 그친 곳이 26.8%였다. 쿠키 거부방안을 제시하고, 쿠키가 개인식별정보와 통합되어 사용되지 않음을 밝히고 있는 곳이 34곳(50.7%)으로 가장 많았고, 설명과 거부방안만을 제시한 곳이 19곳(28.4%)으로 나타났다.

조사 대상 기업 대부분이(95.5%) 개인정보 관리 책임자를 지정하고 있었으나 임원 또는 부서장급에 못 미치는 개인정보관리 책임자를 지정하고 있는 곳이 9곳(13.4%)이었다. 개인정보 관리 책임자의 성명, 직위, 전화, e-mail 등을

모두 고지하는 곳이 51개(76.1%)로 가장 많았고, 대체로 연락처 고지의 의무는 다하고 있었으나 실제 연락이 어렵거나 불가능한 경우도 일부 있었다.

조사대상 중 인터넷 실명확인제를 실시하는 곳이 46개로 68.7%였으며 실시하지 않는 곳이 31.3%였다. 실명확인은 대부분 외부 기관의 데이터베이스를 사용하는 것으로 나타났다. 각 사이트에서 회원가입 시 필수적으로 수집하고 있는 연락처 정보는 대체로 2~3개 가량인 것으로 나타났는데, 이러한 연락처 정보들을 왜 수집해야 하는지 목적을 제시하지 않고 있는 곳이 56.7%나 되었다. 또한 거의 모든 사이트(92.5%)에서 회원가입시 주민등록번호 입력을 요구하고 있었다.

광고성 메일 등의 수신에 대한 별도의 동의 절차를 마련하고 우편물의 종류에 따라 개별적 동의를 받고 있는 곳은 전체의 26.9%였다. 별도의 동의절차를 마련하고 있으되 모든 우편물에 대해 하나의 동의를 받고 있는 곳이 43.3%로 가장 많았다.

이용자의 개인정보가 제3자와 공유될 수 있다는 사실을 명시하고 최소한 현재 공유 대상의 기업 명칭을 고지하는 곳은 12개로 전체의 17.9%에 불과했다. 공유대상과 목적을 모두 추상적으로 표현한 곳이 34.3%, 현재 개인정보가 공유되고 있는지 없는지 명확히 알 수 없는 곳이 47.8%였다. 개인정보 공유에 대한 동의 절차를 명확히 안내하지 않고 있는 곳이 41.8%였고, 공유 대상 기업 각각에 대해 따로 동의절차를 마련하는 곳은 전혀 없었다. 영업의 양수 양도 시에 어떠한 방식으로 안내할 것인지 명시하지 않은 곳이 무려 85.1%이었으며, 양수양도 시에 동의를 받을 것을 명시하지 않은 곳도 83.6%였다.

3. 개인정보 보호를 위한 관리적·기술적 대책 현황

이어 프라이버시 보호를 위한 기업 내부 시스템을 관리적·기술적 차원으로 살펴보았다. 이를 위해 웹사이트 및 문헌 조사에 더해, 조사 대상 기관들 중

10곳을 선정하여 개인정보관리책임자와 면담을 실시했다. 조사 결과 몇 가지 문제점이 발견되었다.

우선, 개인정보보호를 위한 내부 체계에 있어 가장 중요한 것은 개인정보관리책임자가 지위와 업무에 있어 독립성을 가질 수 있도록 하는 것이다. 이를 위해서는 개인정보관리책임자의 임기 보장과 해고 금지 등이 규정될 필요가 있으며, 회사 전체를 대상으로 계획을 수립하고 이행 여부를 감독할 수 있는 실질적 권한을 부여해야 한다. 또한, 개인정보관리책임자가 신사업 개발, 마케팅 등 개인정보의 활용에 초점을 맞추는 업무를 겸직하지 않도록 할 필요가 있다. 그러나, 현재 개인정보관리책임자가 이사 이상의 직위를 가진 곳은 조사 대상 금융기관의 경우 단 한 곳에 그쳤으며, 인터넷 기업의 경우에도 5곳에 불과했다. 또한 마케팅 부서 관련 직원이 개인정보관리책임자로 지정되어 있는 경우가 많았다.

개인정보 관리 실태에 대한 감사도 정기적으로 이루어져야 한다. 그런데, 소규모 기업들의 경우 자체 감사가 진행되지 않고 있었다. 반면 대규모 기업들의 경우 개인정보관리책임자가 직접 감사를 수행하는 경우, 감사실의 일반 감사에 포함되어 수행하는 경우, 감사실과 개인정보관리책임자가 협력하여 수행하는 경우 등 다양한 방식으로 수행되고 있었다. 한편, 국가의 감독 기능과 기업의 자체 감사를 연계시킬 필요가 있다. 국가의 감독 기구가 주요 기업들에 대해 실태 조사를 하는 것도 필요하겠지만, 모든 기업을 실제로 감독하는 것이 어려운 만큼 개인정보관리책임자의 감사 활동을 감독하고, 감사 결과를 보고받는 체계를 고려해야 한다.

고객 불만·고충이 발생하는 건수는 기업의 규모와 업종에 따라 다양했다. 포털/커뮤니티 사이트의 경우 하루 100건 정도의 민원이 접수되고, 그 중에서도 주민등록번호 도용과 관련된 민원이 월 100건에 달했다. 반면, 쇼핑몰의 경우 관련 민원을 통틀어도 하루 2건 정도에 불과했다. 이는 쇼핑몰들의 경우 회원 가입을 하지 않아도 서비스를 이용하는데 지장이 없도록 되어 있기 때문이다. 회원 가입은 꼭 필요한 곳에 국한해야 함을 확인할 수 있었다.

또한, 개인정보의 유출 가능성을 최소화하기 위해서는 업무에 따라 데이터베이스에 대한 적절히 설정하여 불필요한 접근을 최소화하는 것이 중요하다. 이를 위한 기술적 조치로서 금융기관들은 단말기에 고유번호를 부여하고 있으며, 관리자카드를 사용하여 개인 인증을 하고 있었다. 한편, 쇼핑몰과 포털 사이트 등 여타 기업들은 ID와 패스워드를 통해 개인 식별을 하고 있으며, IP 주소를 통해 단말기를 식별하고 있다.

쇼핑몰, 포털 사이트 등의 전자결재시스템은 대부분 신용카드, 핸드폰 결재, ARS 전화 결재, 계좌이체 등으로 이루어져 있었으나, 몇몇 기업이 채택하고 있는 '초고속통신 결재시스템'의 경우 아이디와 비밀번호, 주민등록번호만 입력하면 되도록 되어 있어 다소 위험한 결재방식으로 판단되었다. 현재 한국통신의 메가패스 결재시스템을 4개 포털 사이트가 채택하고 있었으며, 하나로통신의 하나포스 결재시스템을 3개 포털 사이트가 이용하고 있었다.

현금자동지급기(CD)와 현금자동입출금기(ATM) 등 오프라인 자동화기기는 원칙적으로 기기에는 정보가 내장되지 않도록 되어 있어 소비자가 주의를 기울이기만 한다면 안전한 시스템으로 알려져 있었으나, 편의점, 백화점, 극장 등 금융기관 외부에 설치된 자동화기기의 숫자가 급증하면서 사실상 커피자판기와 다를 바 없을 정도로 관리가 소홀해졌다. 자동화기기와 금융기관 사이의 회선을 도청하거나 자동화기기 내부에 데이터 리더기를 장착함으로써 정보가 유출되는 사건들이 보도되었다. 때문에 금융감독원은 자동화기기와 금융기관 사이의 정보 송·수신을 암호화하여 수신하도록 하고, 자동화기기를 공급·관리하는 VAN 사업자들의 경우 고객 정보를 수집하지 못하도록 조치를 취했으나, 감독을 위한 법제는 아직 마련되지 않은 상태이다.

한편, 개인정보관리책임자들은 기업들의 자율적인 개인정보 보호 노력이 부진한 원인으로 마케팅 효과의 부족을 들었다. 사실 평소에 개인정보 보호를 위해 열심히 노력하던 기업이라도 아주 사소한 곳에서 정보가 유출되는 경우가 많다. 문제는 개인정보가 유출되었을 경우에는 언론에서 크게 떠들지만, 개인정보 보호를 잘하고 있다고 해서 주목받지는 못한다는 사실이다. 따라서 최

소한의 조건만 충족시키려 할 뿐, 다른 기업들보다 더 많은 투자를 하려 하지는 않는다는 것이다. 이와 관련해서 인증 제도의 운영방식을 개선할 필요가 있다. 단순히 인증 마크를 해당 기업 웹사이트에 게시하는 방식으로는 별로 효과가 없으므로, 인증 기관 스스로 인증마크의 위상을 제고하고, 인증받은 기업들을 적극적으로 홍보하려고 노력해야 한다.

4. 국내외 개인정보 보호 법제에 대한 검토

개인정보 보호를 위해 기업들의 자발적 노력이 중요하다 해도, 자기정보통제권은 기본권이므로 최종적으로는 법률에 의해 보호받게 된다. 국내에도 프라이버시 보호를 위한 여러 가지 법률이 제정되어 있으나, 분야별 법률 체계를 택하고 있어 개인정보 보호의 사각 지대가 많으며, 정보 보호를 목적으로 제정된 몇몇 법률을 제외하면 OECD 가이드라인에서 제안하고 있는 수준의 보호 원칙을 담지 못하고 있다. 또한 온라인 상의 개인정보 보호 문제만을 다루는 경우가 많다. 그러므로 유럽 선진국들과 마찬가지로 온라인과 오프라인, 공공 영역과 민간 영역의 구분 없이, 누구나 지켜야 할 개인정보 보호 원칙을 천명하는 일반법을 제정하는 것이 필요하다. 다만 일반법의 경직성을 탈피하기 위해서 필요한 부분에서는 분야별 입법을 통해 해당 분야에 맞는 세부적 보호 방식을 규정해야 할 것이다.

한편, 현재 개인정보 보호를 담당하는 핵심 부처로는 행정자치부와 정보통신부 산하의 개인정보분쟁조정위원회, 재정경제부 산하의 금융감독원이 있다. 그런데, 이 기관들의 상급 부처들은 각각 행정 효율성, 혹은 해당 산업의 발전을 주 목적으로 하는 부서인 탓에 개인정보 보호가 위축될 가능성이 많으며, 실제로도 그런 모습들이 나타난 바 있다. 때문에 인사권과 예산권이 독립된 프라이버시 전담 감독기구의 설립 필요성이 지적되었다.

다음으로 현행 정보통신망이용촉진및정보보호등에관한법률을 검토했다. 이

법은 법률의 목적 자체가 정보통신망 이용촉진과 정보통신망 보호, 개인정보 보호라는 세 가지 서로 다른 목적을 하나의 법률을 통해 실현하려 하고 있다는 점에서 근본적인 문제가 있다. 또한, 정보수집에 대한 이용자의 동의권 보장에 있어 한계가 있으며, 특히 제3자 제공에 대한 포괄적 동의 방식이 인정될 소지가 있었다. 그 외에 개인정보 취득 경위에 대한 설명 의무가 명시되어 있지 않은 점도 정보 주체의 권리를 제약하는 요인이었다. 이를 해결하기 위해 프라이버시 영향평가제와 명시적·선별적 동의 방식의 도입, 취득경위의 공개 규정 도입 등이 필요했다.

세 번째로, 최근 제안된 위치정보의이용및보호등에관한법률(안)을 검토했다. 이 법안 역시 위치정보의 보호와 활용이라는 상충될 수 있는 목표를 하나의 법률에서 규율하고 있다. 또한 위치정보는 이동통신기기에 의해서 파악되는데, 기기의 소유자와 이용자가 서로 다를 경우에 발생할 문제를 충분히 검토하지 못하고 있다는 문제점이 발견되었다. 또한 서비스 유형에 따라 요구되는 위치정보의 정확도가 달라질 수 있는데, 이를 정보통신부 장관이 고시에 의해 일방적으로 결정할 수 있게 하고 있었다. 또한, 긴급 구조를 명목으로 하는 공공기관의 위치정보 수집 권한이 남용될 가능성과 위치정보 수집 차단을 위한 옵션을 기기에 제공하지 않고 있다는 점도 문제로 지적되었다.

다음으로 검토된 신용정보의이용및보호에관한법률은 상당 부분을 금융감독위원장의 재량에 맡기고 있었으며 정보주체의 고지받을 권리와 동의권을 규정하지 않고 있었다. 또한, 신용정보 제3자 제공에 동의하지 않을 경우에도 금융기관의 서비스를 이용할 수 있도록 제3자 제공 절차와 서비스 이용 계약을 분리할 필요성이 지적되었다.

5. 정책 개선 방향 및 구체적 보호 지침

앞에서 진행된 조사 연구의 결과, 본 연구는 자기정보통제권의 확립을 위해

기존 OECD 가이드라인의 8원칙을 보완하는 원칙들이 필요함을 지적했다. 본 연구에서 제출된 원칙은 다음과 같다. 첫째, 개별 정보주체와 정보 수집자 사이의 불균형 상태를 해소하기 위해 정보주체들이 집단적으로 권리를 행사할 수 있도록 해야 한다. 이는 감독 기구의 구성, 정보주체의 단체 결성으로 표현될 수 있다. 둘째, 개인정보의 수집은 가급적 분산되어 이루어져야 한다. 수집된 정보의 공유를 최소화하고, 국가가 담당하는 개인정보 관련 사무들은 가급적 지방자치단체 사무로 이관해야 한다. 셋째, 프라이버시를 침해하지 않거나 덜 침해하면서 감시 목적을 달성할 수 있는 다른 방법이 있는 한 감시 행위를 회피할 선택의 여지가 주어져야 한다. 이를 위해, 새로운 감시 장비의 도입, 새로운 개인정보 데이터베이스의 구축, 기존 데이터베이스의 연동 등의 경우에, 감시 행위의 불가피성을 미리 점검할 수 있는 프라이버시 영향평가제도를 도입해야 한다. 또한, 정보 주체의 법적 대응 능력을 보완하기 위해 대안적 분쟁조정제도와 집단소송제도의 도입을 검토해야 한다.

또, 구체적 정책방향으로 개인정보보호 일반법의 제정과 독립적 감독기구의 설치, 주민등록번호 수집 관행의 시정, 개인정보 공유에 관한 포괄적 동의 방식 시정, 개인정보보호정책 및 약관의 개선 등을 제안했다.

우선, 주민등록번호의 경우 평생불변 전국민 고유식별번호이므로, 유출된 피해자의 권리 회복이 불가능하다. 그럼에도 공공기관은 물론, 민간에서도 폭넓게 수집되고 있어 유출 및 오·남용의 가능성이 매우 높으며, 신용카드의 개설 등 물질적 피해로 연결되는 경우도 많다. 때문에, 주민등록번호의 재부여를 가능하게 하고 민간 수집을 최소화하는 등의 제도적 개선이 요구된다.

또한, 정보수집자들이 구체적 사항을 정보주체들에게 알리지 않은 채 제3자와의 개인정보 공유에 동의할 것을 강제하는 포괄적 동의 방식도 개선되어야 한다. 이를 개선하기 위해 약관에 대한 동의 절차와 개인정보 공유에 대한 동의 절차를 분리하여 제시하고 동의 여부의 선택 또한 공유 대상 기업 각각에 대해 따로따로 이루어져야 한다.

약관과 개인정보보호정책의 경우 서로 비슷비슷한 내용에 매우 길고 어려운

표현으로 이루어져 있어 이용자들의 이해 정도가 매우 낮다. 물론, 쉽게 전달되는 것과 정확히 전달되는 것은 다소 상충되는 일이다. 이를 해결하기 위해서는 개인정보 보호정책을 2단계로 분리해서 제시해야 한다. 1단계에서는 ▲ 개인정보의 보존 연한 ▲ 제3자 공유 ▲ 이용 요금 ▲ 개인정보관리책임자 등 해당 사이트에 고유한 내용들만으로 정책을 제시하여 이용자들이 한 눈에 정보를 파악할 수 있게 하고, 2단계에서는 전체 정책과 약관을 제시하여 정확한 정보를 전달받을 수 있도록 하는 것이 바람직하다.

이어 본 연구는 개인정보 보호를 위한 일반 원칙을 수집, 목적 제시, 이용 및 제3자 제공, 보유 및 파기, 개인 참가권 보장, 정확성·안전성 유지, 공개, 책임, 데이터베이스의 분산, 개인정보 영향평가제도, 개인정보 감사 제도, 분쟁조정제도, 집단소송제도, 관리책임자 지정, 이용자 단체 구성, 감독기구 설치, 교육 등으로 나누어 제시했다. 또한, 정보통신서비스제공자, 금융기관, 신용정보기관 등 각 업종별로 지켜져야 할 특수한 원칙들에 대해서도 별도로 제안하고 있다.

Ⅰ. 서론

1. 연구의 목적과 의의

지난 몇 년간 우리 사회는 엄청난 속도로 정보화 시대로 진입하고 있다. 2002년 들어 인터넷 사용자가 이미 2천5백만에 달하며, 11월에는 초고속인터넷 가입자 1천만 시대에 진입했다는 발표가 있었다. 휴대폰의 경우 3천만 가입자를 기록하고 있는데, 그 중 1천5백만이 무선인터넷을 이용하고 있다. 또한 가정용 PC만도 1천5백만 대가 보급된 상태이다. 이러한 물적 기반은 다양한 영역의 정보화를 가속화하고 있다. 포털 사이트, 커뮤니티 사이트의 운영은 물론 전자상거래와 전자금융이 날로 확대되고 있다. 2002년에는 인터넷뱅킹 가입자가 1천7백만명을 넘고, 전체 주식거래 중 사이버 매매가 70%를 넘었으며, 전자정부포털사이트, 국가종합전자조달시스템, 국가재정정보시스템, HTS (Home Tax Service), 교육종합행정정보시스템과 같은 전자정부 기반이 완성되었고, 사이버 교육이 크게 확대되는 등 커다란 발전을 이룩하였다.[1)]

그러나 정보화 사회의 진전은 해결하기 힘든 몇 가지 문제를 동반하고 있는데, 그 가운데 중요한 하나는 개인 프라이버시에 대한 체계적인 위협이다.[2)] 모든 것이 온라인화 되어 전자적 흔적을 남기게 되는 정보화 사회에서 개인에 대한 감시와 추적은 언제 어디서나 가능해진다. 특히, 국가의 행정정보 전산화와 전자상거래의 발전의 전제조건이자 핵심적 요소가 되는 것은 개인정보의 대량 축적 및 활용이다. 국가의 개인정보 집적은 국가기관의 감시와 사회 통

---

1) 한국정보보호진흥원, 『2002 개인정보보호백서』, 서울:한국정보보호진흥원, 2003, p. 20.

2) 김주환은 프라이버시 개념이 처음부터 미디어와 밀접한 관련을 맺고 등장·발전했음을 지적한다. 처음 프라이버시라는 개념이 등장하게 된 계기도 19세기 후반 포토 저널리즘의 횡행 탓이었으며, 이후 TV, 라디오 등 전자매체와 녹음기술, 도청장치 등 각종 커뮤니케이션 수단의 발달이 권리로서의 프라이버시 개념을 촉진시켜왔다는 것이다. 김주환, 『디지털 시대의 프라이버시 권리』, 김주환 외, 『디지털시대와 인간존엄성』, 서울 : 나남출판, 2001, pp. 15-16.

제를 용이하게 만든다. 기든스는 모든 국가가 성립하기 위해서는 기본적으로 정보의 집중에 근거한 감시 체제의 구축과 이를 바탕으로 한 인간 행위의 통제가 필요함을 강조했다.[3] 물론 이런 감시 체제가 일정 정도 인간의 존엄성을 확장시키는 데 기여해 왔음을 기든스도 지적하고 있으나, 그 정도가 지나치면 언제든지 개인의 기본권을 억압하는 체제로 전환되었음이 역사를 통해 계속 확인되어 왔다. 이런 문제는 각종 개인정보들이 집적된 국가 기간전산망의 통합을 주요 목표로 하고 있는 전자정부 추진 과정에서 다시 나타나고 있다.[4]

그런데, 최근 많은 학자들은 민간 영역에서 구축되는 개인정보 데이터베이스가 프라이버시에 가져오는 위협이 더욱 크다고 본다.[5] 예컨대 한상희는 다음과 같이 언급하고 있다.

> "빅 브러더는 죽었다"라는 말이 나올 정도로 국가적 감시라는 것이 현대 정보화 사회에서 차지하는 비중은 상대적으로 축소되고 있다. 즉, 자본주의적 생산양식에서 기업이 소비를 창출하고 그로부터 이윤을 추구하기 위한 전략의 하나로 나타나는 소비자 감시(consumer surveillance)의 문제는 국가감시의 문제가 비교도 되지 않을 만큼 엄청난 속도로 그 진행을 가속화하고 있다. 오히려 국가감시는 이러한 기업 감시의 한 부분으로, 또는 그것에 보조하여 그 기업들을 위하여 이루어지는 양상까지도 보인다.[6]

---

3) 안쏘니 기든스, 진덕규 역,『민족국가와 폭력』, 서울 : 삼지원, 1991, pp. 56-65.

4) 그 대표적인 사례로 전자주민카드의 도입 시도를 들 수 있다. 이에 관해서는 홍석만・이준구,『역감시 권리로서의 프라이버시권에 대한 재구성』, 민주사회를 위한 변호사모임 편,『역감시의 권리로서 프라이버시권에 대한 재구성』, 서울: 민주사회를 위한 변호사모임, 1999, 윤현식,『개인정보의 국가등록제도와 프라이버시권과의 관계에 관한 연구 - 감시와 통제의 기제로서 주민등록법을 중심으로』, 건국대학교 석사논문, 2002를 참고할 것.

5) 대표적 논의로는 다음과 같은 것들이 있다. 릭 휘태커, 노명현・이명균 역,『개인의 죽음』, 서울 : 생각의 나무, 2001, Margaret Jane Radin, *Contested Commodities,* Cambridge, Mass. : Harvard Univ. Press, 1996, Margaret Jane Radin, "Property Evolving in Cyberspace," *Journal of Law and Communications,* 15, 1996.

6) 한상희,『국가감시와 민주주의 - 공공영역의 창출을 위한 헌법해석』, 프라이버시보호네트워크 제2차 공동토론회 <<개인정보의 국가 등록/관리제도의 문제점>> 자료집, 2001, p.18.

사실, 최근 데이터베이스 마케팅이 각광받는다는 사실에서 확인할 수 있듯이 디지털 경제에서 개인정보는 모든 영업활동의 기반이자 기초 자료로 활용된다. 이는 한 편으로 소비자 내지 고객 중심 마케팅으로의 전환을 가능하게 하지만,[7] 다른 한 편으로는 정보에 대한 관리 소홀 문제나 개인정보의 오·남용 문제를 야기한다. 최근 농협 현금카드 복제로 야기된 대형 금융사고와 같은 재산권 상의 피해를 가져올 뿐만 아니라, 사용 여하에 따라서는 인간성 자체에 대한 위협으로 다가가기도 한다.[8]

따라서, 프라이버시 보호, 특히 민간 영역에서의 개인정보 보호는 정보화 시대로 접어들고 있는 최근 몇 년간 모든 선진 사회에서 중요한 정책 과제로 떠오르고 있다. 나아가 국가간의 장벽이 무너진 정보 사회에서 프라이버시 권리에 관한 문제는 세계적으로 표준화된 권리를 만들어나가는 문제로까지 확대되고 있다.[9]

이처럼 정보화 시대의 도래에 따라 더욱 중요해지고 있는 민간 영역에서의 프라이버시 보호 문제를 논의하는 것이 본 연구의 목표이다. 전자상거래의 확대에 따라 쇼핑몰, 포털사이트 등 각종 웹 사이트의 개인정보 보호 실태를 조사하고 바람직한 대안을 제시하고자 했다. 특히, 최근 더욱 중요해지고 있는 금융기관들의 개인정보 보호 문제, 그리고 온라인 지불시스템과 관련된 개인정보 보호 문제를 면밀히 검토했다. 또한 단순히 개인정보의 수집 및 관리 문제에만 연구를 국한하는 것은 많은 한계가 있으므로, 물리적 차원과 네트워크 차원의 양 측면에서 보안 시스템의 안전 문제를 함께 조사했다. 또한, 프론트

---

7) 박광진, 『디지털 시대의 개인정보 활용과 오용 대책』, 김주환 외, 앞의 책, p. 48.

8) 기업의 개인정보 활용은 때로는 소비자들의 인간 존엄성 자체에 위협을 가한다. 작게는 스팸메일이나 텔레마케팅, 제3자와의 정보 공유 등으로 인한 각종 불안감 및 정신적 스트레스를 일으키고, 크게는 소비자들의 구매 실적에 따라 등급을 매기는 현대판 카스트 제도의 출현이나 정보의 활용을 통한 소비자 심리 조작 등의 문제로까지 이어질 수 있다. 이와 관련된 여러 현상을 심슨 가핀켈, 한국데이터베이스진흥센터 역, 『데이터베이스 제국』, 서울 : 한빛미디어, 2001, pp. 256-280.에서 확인할 수 있다.

9) 이와 관련하여 백의선 외, 『국가간 개인정보 유통에 관한 정책 연구』, 한국정보보호센터 정책연구, 2000, 이지윤, 『인터넷 개인정보보호 정책 분석 - 유럽연합(EU)과 미국의 정책비교』, 이화여자대학교 석사논문, 2002 등을 참고할 수 있다.

오피스 차원 못지 않게, 기관의 내부 업무처리 과정인 백 오피스 시스템을 잘 구축하여 운영함으로써 내부 업무 처리 과정에서 프라이버시 침해를 방지하는 것이 중요하므로, 내부 시스템 운영 실태도 조사했다.

이러한 연구에 기반하여 본 연구는 개인정보보호 실태조사 과정에서 확인된 각 영역의 문제점들에 대한 바람직한 법적·제도적 해결책을 모색해 보았다.

2. 선행연구 및 관련연구 분석

정보화 사회의 도래로 인해 프라이버시의 보호의 중요성이 높아지고 있다. 이에 따라, 프라이버시 문제를 다룬 많은 연구가 쏟아지고 있다. 그러나 대부분의 연구가 프라이버시 보호와 관련된 일반적 이론을 다루는 연구이거나, 혹은 국가 영역에서의 프라이버시 문제를 다루는 데 집중되어 왔다. 반면에 민간 영역의 프라이버시 문제를 다루는 연구는 상대적으로 빈약한 편이다.

민간 영역의 프라이버시 문제를 다루는 기존의 연구들은 크게 두 가지 유형으로 분류할 수 있다. 하나는 법적·제도적 측면의 분석을 중심으로 하는 연구이며, 다른 하나는 실제 기관들의 운영 실태를 조사하는 연구이다. 먼저, 법적·제도적 측면을 분석하는 연구들을 보면, 이 연구들은 주로 법학자들에 이루어지고 있으며 사실상 프라이버시 연구의 대부분을 차지하고 있다. 이는 다시 둘로 나누어볼 수 있다. 한편으로는 주로 OECD에서 제시하는 프라이버시 보호 8원칙에 입각하여 현재의 법제를 평가하고 부족한 측면들을 지적하는 규범적 연구들이 있으며, 다른 한편으로는 프라이버시 보호를 위한 다양한 규제 방법론의 적합성을 둘러싼 실증적 연구들이 있다.

규범적 연구[10]의 경우, 프라이버시에 대한 기본 개념조차 없었던 우리 사회

10) 이에 속하는 연구로는 이덕구,『민간이 보유하는 개인정보의 보호』, 인천대학교 평화통일연구소,『통일문제와 국제관계』제8호, 1997, 정재훈,『민간부문에서의 정보프라이버시 보호』, 한국정보법학회 제7회 세미나, 1997, 방석호,『전자상거래에서의 프라이버시와 소비자 보호』, 한국정보법학회 국내학술세미나, 1998, 노순규,『정보관련 법제화와 정보보호』, 한국정보통신진흥협회,『정보화사회』123호, 1998, 김연수,『개인정보보호』, 서울 : 사이버출판

에 프라이버시 권리와 관련된 주요 원칙들을 소개하고 이를 기준으로 우리 사회의 주요 법제를 점검하고 있다는 점에서 큰 학문적, 실천적 기여를 해왔다. 특히, 우리 사회에 프라이버시 보호와 관련된 기본법 혹은 기본 원칙이 아직 제정되어 있지 않음으로 인해 다양한 문제가 발생했음[11]을 고려할 때, 이러한 연구는 분명 의미 있는 연구로 평가될 수 있다. 그러나 이런 연구들이 갖는 몇 가지 한계를 지적할 필요가 있다. 우선, 많은 경우 이 연구들은 현실에 대한 분석을 전제로 하는 연구가 아니므로, 실제로 웹 사이트에서 벌어지는 구체적 프라이버시 침해 양상들에 대한 적절한 해결책을 제시하지 못하고 있다는 문제가 있다. 다음으로, OECD 가이드라인을 위시한 서구의 기준을 그대로 옮겨오는 경우가 많다는 것도 문제로 지적될 수 있다. 서구 사회와 우리 사회

사, 2001, 이인호,『한국의 개인정보보호법제의 문제점과 정비방안』,『각국 개인정보보호 법제도의 비교법적 접근』, 한국정보보호진흥원 2003년 제2회 개인정보보호 심포지움, 2003 등이 있다.

11) 한국의 정보통신운동 단체들은 지난 해 말 프라이버시 일반법 혹은 일반원칙의 제정을 요구하면서 다음과 같은 이유를 들었다. "현재 우리 사회의 프라이버시 보호 법제는 공공기관의개인정보보호에관한법률, 통신비밀보호법, 정보통신망이용촉진및정보호호등에관한법률, 신용정보의이용및보호에관한법률처럼 보호가 필요한 분야별로 개별적인 입법을 하거나 주민등록법, 전자정부구현을위한행정업무등의전자화촉진에관한법률, 전자상거래등에서의소비자보호에관한법률, 금융실명제및비밀보장에관한법률 등 기존 법률에 일부 조항을 신설하는 형태를 취하고 있다. 이러한 법률 체계는 몇 가지 문제점을 안고 있다. 먼저, 누락되는 영역이 너무 많다. 예컨대 프라이버시 침해 정도가 심각한 의료 정보에 대해 보호 입법이 보건의료기본법 제13조의 "모든 국민은 보건의료와 관련하여 자신의 신체·건강 및 사생활의 비밀을 침해받지 아니한다"라는 단 한 줄에 불과해, 병원 및 의사 개개인의 직업 윤리에 의존하고 있는 상황이다. 또한 호텔 및 여행업, 학원, 항공사 등의 개인정보 보호는 정보통신망이용촉진및정보보호등에관한법률에서 편법으로 규제하고 있는 상황이며, 비디오방과 도서대여점 등 각종 대여업이나 백화점 등의 유통업은 규제할 법률 자체가 존재하지 않는다. 특히 최근 중대한 사회 문제로 떠오르고 있는 사업장에서의 프라이버시 침해를 규제할 수 있는 근거가 존재하지 않는다. 둘째, 정보 보호를 목적으로 제정된 몇몇 법률을 제외하면 보호 조항 자체가 부실하다. OECD가 제정한 <개인데이타의 국제유통과 프라이버시 보호에 관한 가이드라인>의 목적 명확화의 원칙, 관리적 보호조치의 원칙, 기술적 보호조치의 원칙, 개인 참가의 원칙, 수집 제한의 원칙을 거의 대부분의 법제에서 찾아볼 수 없다. 셋째, 대부분의 프라이버시 보호 법제가 최근 전자화된 개인정보의 보호만을 다루고 있어, 오프라인 상의 프라이버시 침해까지 포함하는 적절한 대응이 이루어지지 못하고 있다." 광주인권운동센터 외,『정보사회 기본권 보장을 위한 33대 공약 - "국민의 권리는 정보사회에서도 지켜져야 한다"』기자회견 자료집(2002.11.14), p.15.

의 사회문화적 전통이 동일하지 않으므로, 서구의 기준에서 본 프라이버시 문제의 해결책이 그대로 우리의 프라이버시 문제 해결에도 적합하다고 보기는 어렵다. 마지막으로, 정보화 사회가 상당한 수준으로 발전했기 때문에, 과거의 프라이버시 기준을 그대로 적용해서는 곤란하다.

개인정보보호의 법제적 연구에 있어 한 걸음 앞선 연구로는 이은우의 연구[12]를 들 수 있다. 그는 전자 감시 기술의 발전으로 인해 기존의 프라이버시 개념으로 해결하기 어려운 여러 문제[13]가 등장한다고 지적하면서 혼자 있을 권리나 자기정보통제권이 아닌 반감시권이라는 개념을 채택하고 있다. 그가 이 개념을 학문적으로 엄밀하게 정립하여 제출한 것은 아니지만, 시대적 변화나 우리 사회에서의 특성 등을 고려하여 프라이버시 문제를 다룸으로써 논의를 한 걸음 진전시켰다고 볼 수 있다.

한편, 개인정보에 관한 법제적 연구경향에서 나타난 실증적 연구[14]에 관해 보면, 국가 규제 vs 시장 자율 규제의 문제, 개별 법제를 통한 보호 vs 일반법을 통한 보호 등이 주요 쟁점으로 논의되고 있다. 이 연구들은 실제 사례나 통계 등을 통해 증명을 해야 하므로, 현실적합성이 높고 정책적인 함의를 많이 제공해준다. 그러나 이 연구들의 사례가 실제 기관에서 발생하는 구체적 사례들에 대한 분석으로 발전하기는 여전히 한계가 있으며, 대부분의 연구는

---

12) 이은우, 『정보화에 따른 프라이버시권 침해법령 조사 연구』, 국가인권위원회 2002년도 인권상황 실태조사 연구용역사업보고서, 2002.

13) 그는 기존의 프라이버시권들과 구별하여 반감시권을 주장하는 이유를 다음과 같이 지적하고 있다. ① 민주주의에 대한 중대한 위협이다. ② 보호 대상이 개인으로 국한되어서는 안 된다. 식별가능성 여부를 불문해야 하며 단체도 포함되어야 한다. ③ 고지 혹은 동의라는 계약적 사고를 넘어서야 한다. ④ 감시 계획의 수립 단계부터 참여·통제할 권리를 보장받아야 한다. ⑤ 민간의 감시활동에 대해서도 통제할 수 있어야 한다. 이은우, 위의 책, pp. 16-20.

14) 이에 속하는 연구로는, 정찬모, 『개인정보보호에 관한 국제적 입법동향 및 우리의 대응』, 서울 : 정보통신정책연구원, 1997, 정영화 외, 『개인정보보호 감독기구 도입을 위한 법제도 개선방안연구』, 서울 : 한국정보보호센터, 2000, 정영화, 『정보사회의 프라이버시 보호를 위한 정책과제 - 개인정보보호법률(Privacy Act)의 실현을 중심으로』, 프라이버시보호네트워크 1차 토론회 자료집, 2001, 신종철, 『프라이버시 보호를 위한 규제에 대한 연구』, 성균관대학교 석사논문, 2001, 박광진, 앞의 책 등을 들 수 있다.

총론 차원에서의 보호 방안 연구에 머무르고 있다.

개인정보보호에 관한 연구에 있어 두 번째의 주된 경향은 현실을 객관적으로 분석하는 것이다. 주로 실태조사의 형태로 이루어지는 이 경향도 다시 두 가지로 구분해볼 수 있다. 우선, 개별 기관들의 정책과 제도적·기술적 시스템 혹은 개인들의 의식 등을 분석하는 연구[15]이다. 이러한 연구들은 학계에서는 그다지 많이 이루어지지 않았으며, 주로 정부출연연구소나 비영리기구들이 조사하여 발표한 것들이 대부분을 차지하고 있다. 이 연구들은 법제 연구들이 다루기 어려운 정보보호 시스템의 현실적 문제점들을 다루고 개선방안을 마련한다는 점에서 의의가 있으나, 대부분 조사 대상으로 삼고 있는 문제를 해결하는 데 관심이 국한되어 있는 탓에 그 해결 방안과 프라이버시 권리의 일반 원칙들이 연계되지 않는 문제를 낳는다. 이 문제는 특히 보안기술과 관련된 문제에서 심각하다. 단순히 프라이버시 원칙들과 연계되지 않을 뿐 아니라, 종종 프라이버시 원칙에 위배되는 대안들이 제시되곤 한다. 예컨대, 홍창수 등은 암호기술을 다룬 한 연구에서 "당신이 나를 감시하는 것을 해결하는 방법은 그 감시를 막는 것이 아니라 내가 당신을 감시하도록 허용하는 것"[16]이라는 로렌스 레식의 논지를 빌어, 다음과 같은 이야기를 하고 있다.

> 사이버 공간은 『자유, 공개, 익명』이라는 모토를 버리고 『규제와 통제, 보호, 인증』이라는 새로운 모토를 선택했다. (중략) 몰래 수집된 개인정보(전자서명 데이터)는 명백한 프라이버시 침해지만, 사용자가 자기를 감시하도록 허용한 상태에서의 개인정보(전자서명 데이터)의 수집과 보관은 프라이버시 침해라 볼 수 없다는 관점에서 많은 것을 우리에게 시사한다.[17]

---

15) 이 분야의 연구로 다음과 같은 연구들이 있다. 서근우, 『신용정보관리제도의 현황과 과제』, 서울 : 한국금융연구원, 1996, 기술과 법 연구소, 『전문가 집단의 개인정보보호 마인드에 관한 설문조사 결과보고서』, 서울 : 한국정보보호진흥원, 2001, 홍인수, 『개인정보보호 및 스팸메일에 대한 이용자 의식 조사』, 서울 : 한국소비자보호원, 2001.

16) Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York : BASIC BOOKS, p. 153.

17) 홍창수 외, 『PKI에 잠재된 개인정보의 모호성』, 한국정보보호진흥원, 『개인정보연구』 2002

이는 실제로 국가정책에서 반복되는 경우가 많은데, 암호기술을 집적하여 관리하는 것이 분산 관리하는 것보다 보안에 투자하는 비용이 적게 든다는 이유로 개인정보를 대규모로 집적하는 것이 프라이버시 보호에 도움이 된다는 식의 정책이 나오기도 한다.[18]

현실 분석의 연구경향에서 나타나는 또 다른 부류의 연구는, 본조사가 목표로 하는 것과 같이 실제 개인정보 수집자들의 수집 현황에 대한 실태를 조사한 것들이다.[19] 이 분야에 속하는 연구는, 많은 경우 단순히 정부 부처나 각 기관들에 의해 수행되는 조사 작업들이다. 따라서 대부분 현재의 개인정보 보호 법률의 준수 여부를 중심으로 조사되고 있을 뿐이다. 그러나, 지난 2002년 말 한국소비자단체협의회의 연구[20]는 상대적으로 진전된 방식으로 연구가 진행되었다. 협의회는 ▲ 개인정보 보호에 대한 이용자들의 의식과 태도 ▲ 인터넷 사이트들의 개인정보 보호 관련 실태 ▲ 개인정보 관련 분쟁에 대한 분석 등을 입체적으로 분석하면서 소비자 보호의 관점에서 현재 개인정보 보호 체계의 문제점을 지적하고 개선 방안을 제시하고 있다. 그러나, 개인정보 보호를 자기정보통제권이라는 기본권에 대한 문제로 인식하지 않고 소비자 보호의 문제로만 국한해서 보고 있었다. 또한 소비자단체협의회 및 회원 단체들의 홈페이지에서 설문조사를 실시해 설문조사의 표본이 매우 적으며 성비 불균형이 발생하는 등 표본의 대표성에 다소 문제가 있는 것으로 보였다.

넌 제1호, p. 30.

18) 교육인적자원부 자료, 『교육행정정보시스템 설명자료 - 교무/학사 등 5개 업무영역 중심으로』, 2003, pp. 27-32.

19) 이 분야에 속하는 연구로는 Cyberlaw Institute of Korea, 『국내 인터넷 사이트의 개인정보 보호에 관한 실태조사』, 1999. 8. 16., 함께하는 시민행동 보도자료, 『국내 대표적 인터넷 사이트 개인정보보호실태조사 결과』, 2000. 4. 6., 박영우 외, 『2001년 주요 민간부문 정보보호 실태조사』, 서울 : 한국정보보호진흥원, 2001, 함께하는 시민행동 보도자료, 『50여개 인터넷 사이트 개인정보보호규정 수용도 조사결과』, 2001.11.16. 한국소비자단체협의회, 『개인정보 침해관련 실태조사 및 제도개선방안 연구』, 재정경제부 용역사업, 2002. 등이 있다. 이 외에 연구 작업은 아니지만, 정보통신부가 매년 실시해온 개인정보보호실태 정기 조사 등 각 부처에서 수행하는 조사들이 있다.

20) 한국소비자단체협의회, 『개인정보 침해관련 실태조사 및 제도개선방안 연구』, 재정경제부 용역사업, 2002.

선행 연구들에서 나타난 문제들을 극복하기 위해 본 연구는 실태에 대한 분석과 법제 분석을 동시에 진행하여 양 쪽 연구의 장점을 살리도록 한다. 또한, 양 측면의 분석이 충돌하는 갈등양상을 해소하고 접점을 찾기 위해 권력과 시장의 개념을 중심으로 하는 사회과학에서의 프라이버시 논의를 전개하려고 한다.

3. 연구의 방법과 대상

가. 연구의 대상

본 연구는 금융기관 및 인터넷의 개인정보 공유 현황을 조사하여 프라이버시 침해 여부와 가능성을 조사한 후 바람직한 대안을 제시하는 것을 목표로 하고 있다. 따라서, 본 연구는 주요 금융 기관과 정보통신서비스 제공자들을 조사 대상으로 한다.

금융기관으로는 은행, 보험사, 카드사, 증권사 40개사를 조사했다. 은행의 경우 서울에 본점을 두고 있는 11개 은행을 선정했으며, 신용카드사는 현재 허가를 받은 9개 카드사를 선정했다. 보험사와 증권사의 경우 금융감독원에서 발표한 자산 기준 상위 10개사를 선택했다. (2003년 1/4분기 기준)

정보통신서비스제공자로는 일반 시민들이 특히 자주 이용하는 언론사, 포털/커뮤니티 사이트, 쇼핑몰을 각 10개씩 선정했다. 언론사의 경우 3개 공중파 방송사 외에 주요 종합일간지 6개사와 경제지 1개사를 선정했다. 포털/커뮤니티 사이트의 경우 일반 이용자들이 많이 찾는 사이트 10곳을 선정했으며, 쇼핑몰의 경우 공정위 발표 30대 기업군의 계열사들 중 10곳을 선정했다. 선정된 기관은 <표 1>과 같다.

<표 1> 조사대상 사이트

구분	회사명	사이트명	구분	회사명	사이트명
증권사 (10)	LG투자증권	http://www.iflg.com	쇼핑몰 (10)	삼성몰	http://www.samsungmall.co.kr
	삼성증권	http://www.samsungfn.com		LG이숍	http://www.lgeshop.com
	현대투자신탁증권	http://www.yescyber.co.kr		롯데닷컴	http://www.lotte.com
	현대증권	http://www.elibero.co.kr		Hmall(현대)	http://www.hmall.com
	대우증권	http://www.bestez.com		신세계닷컴	http://www.shinsegae.com
	동양종합금융증권	http://www.tyib.co.kr		OK 캐시백	http://www.okcashbag.com
	대신증권	http://www.daishin.co.kr		CJ몰	http://www.cjmall.com
	한국투자증권	http://www.hantutams.com		CS클럽(한솔)	http://www.csclub.com
	대한투자신탁증권	http://www.daetoo.com		옥션	http://www.auction.co.kr/
	굿모닝신한증권	http://www.gmsh.co.kr		인터파크	http://www.interpark.com
보험사 (10)	삼성화재해상보험	http://www.samsungfire.com	포털/커뮤니티 (10)	다음	http://www.daum.net
	현대해상화재보험	http://www.hi.co.kr		프리챌	http://www.freechal.net
	LG화재	http://www.lginsure.com		네이버	http://www.naver.com
	동부화재해상보험	http://www.idongbu.com		네띠앙	http://www.netian.com
	대한생명	http://www.korealife.com		네이트	http://www.nate.com
	삼성생명	http://www.samsunglife.com		인티즌	http://www.intizen.com
	흥국생명보험	http://www.hungkuk.co.kr		드림위즈	http://www.dreamwiz.com
	교보생명	http://www.kyobo.co.kr		엠파스	http://www.empas.com
	SK생명	http://www.sklife.co.kr		세이클럽	http://www.sayclub.com
	알리안츠생명	http://www.allianzfirstlife.co.kr		하나포스	http://www.hanafos.com
은행 (11)	농협	http://www.nonghyup.com	언론사 (10)	조선일보	http://www.chosun.com
	신한은행	http://www.shinhan.com		동아일보	http://www.donga.com
	외환은행	http://www.keb.co.kr		중앙일보	http://www.joins.com
	우리은행	http://www.wooribank.com		한겨레신문	http://www.hani.co.kr
	하나은행	http://www.hanabank.com		한국일보	http://www.hankooki.com
	한미은행	http://www.goodbank.com		경향신문	http://www.khan.co.kr
	국민은행	http://www.kbstar.com		매일경제	http://www.mk.co.kr
	조흥은행	http://www.chb.co.kr		MBC	http://www.imbc.com
	씨티은행	http://www.citibank.co.kr		KBS	http://www.kbs.co.kr
	기업은행	http://www.kiupbank.co.kr		SBS	http://www.sbs.co.kr
	제일은행	http://www.kfb.co.kr	카드사 (9)	BC카드	http://www.bccard.com
카드사	국민카드	http://www.kookmincard.co.kr		현대카드	http://www.hyundaicard.com
	삼성카드	http://www.samsungcard.co.kr		롯데카드	http://www.lottecard.co.kr
	LG카드	http://www.lgcard.com		우리카드	http://www.wooricard.com
	외환카드	http://www.yescard.co.kr		신한카드	http://www.shinhancard.com

나. 연구의 방법

연구의 방법은 크게 네 가지로 구분된다. 먼저, 일반 시민들을 대상으로 개인정보 보호에 대한 인식과 태도, 그리고 기업들의 개인정보 보호 노력에 대한 체감 정도를 살펴보았다.

두번째로, 조사대상 기업들의 개인정보보호정책과 약관, 그리고 회원가입절차를 살펴보았다. 이를 통해 조사대상 기업들이 이용자의 자기정보통제권을 어느 정도 보호하고 있는지를 확인해보았다.

이 검토는 다시 다음과 같이 세분화 될 수 있다. 첫째, 해당 기관들의 가입 및 거래개설 약관을 조사함으로써, 가입자들에게 보장되어야 할 각종 프라이버시 권리가 제대로 보장되고 있는지를 확인했다. 구체적 내용으로는 ▲ 수집 범위의 명확성 ▲ 수집 및 이용 목적의 구체성 ▲ 보유 기간의 구체성 ▲ 열람·수정·삭제 권한 보장 여부 ▲ 쿠키 운용 여부 ▲ 기술적 대책 및 관리적 대책의 제시 여부 ▲ 아동의 개인정보 보호 정책의 적절성 ▲ 비회원 거래자의 개인정보 보호 정책의 적절성 ▲ 약관 및 개인정보보호정책 변경시 고지 의무 준수 ▲ 의견 수렴 및 불만 처리 방법 소개 여부 ▲ 이용자의 손해 처리를 위한 보험 가입 여부 등이 조사되었다.

둘째, 회원 가입 양식을 조사함으로써, 불필요한 정보 수집이나 과도한 정보 수집 여부를 확인했다. 구체적 내용으로는 ▲ 불필요한 주민등록번호 수집 여부 ▲ 과도한 연락처 수집 여부 ▲ 광고 메일 및 우편물 수신 선택권 제공 여부 등을 조사했다.

셋째, 특별히 제3자 정보 공유와 관련하여 투명성 및 이용자의 선택권 보장 정도를 조사한다. 구체적 내용으로는 ▲ 개인정보 제공 및 활용 동의서의 분리 여부 ▲ 개인정보 공유 대상 및 공유 대상 정보의 범위/공유 목적의 구체적 명시 여부 ▲ 개인정보 공유 대상 변경 시 고지 방식 ▲ 개인정보 공유 대상별 분리 선택[21] 가능 여부 등을 조사할 것이다.

세 번째로, 현재 금융기관과 쇼핑몰들이 채택하고 있는 보안 시스템의 현황

을 살펴보았다. 개별 기업들의 시스템을 살펴보는 것은 여건상 불가능했으며, 주로 금융감독원의 정책 및 발표 자료들을 중심으로 검토했다. 더불어, 인증 시스템과 관련된 실태 조사를 진행했다.

마지막으로, 개인정보 보호와 관련된 주요 법제를 조사·평가하여 프라이버시 보호의 적절성을 평가했다. 법령의 경우 ▲ 정보통신망이용촉진및정보보호 등에관한법률 ▲신용정보의이용및보호에관한법률 ▲ 위치정보의이용및보호에 관한법률(안) ▲ 금융실명제및비밀보장에관한법률 등을 검토했다. 또한 현재 개인정보 보호를 담당하는 기구들의 감독 시스템을 평가했다. 이는 해외 법제 및 기구들과의 비교법적 연구를 진행했다.

이러한 조사 결과를 종합하여, 본 연구는 프라이버시 보호를 위한 가이드라인을 제시했다. 가이드라인은 우선, 개인정보 보호를 위한 일반 원칙을 제시하고, 이어 ▲ 정보통신서비스제공자 ▲ 금융기관 ▲ 신용평가기관의 세 분야에 별도로 규정되어야 할 개인정보 보호 원칙들을 제시했다.

---

21) 이인호는 서비스 제공자가 고지한 내용 중 이용 목적이나 제3자 제공과 관련하여 일부에 대해서만 동의하는 선별적 동의권이 부여되어야 한다고 주장한다. 이인호, 앞의 책, pp. 131-132.

Ⅱ. 정보사회와 개인정보 보호

1. 정보사회에서 개인정보 보호의 중요성

정보사회는 한 마디로 정보가 사회의 핵심적 전략 자원이 되는 사회이다.[22] 한 사회의 발전은 그 사회의 정보 획득 및 처리 능력에 의존하게 된다. 그런데, 이렇게 획득·처리되는 정보 중에는 개인에 대한 정보도 포함되어 있다. 때문에, 감시 사회라는 부정적 전망과 연결되기도 한다.

가. 감시의 정의와 유형

일반적으로 감시라는 용어는 상당히 부정적인 인상을 불러일으킨다. 그러나, 이론적 의미에서 감시란, "어떤 특정한 의도를 지니고 대중을 관찰·감독하는 것"[23]이다. 고영삼은 <표 2>에서 보는 것과 같이 감시를 네 영역으로 구분하고 있다.

감시는 긍정적 의도를 가지고 공개적으로 추진되는 경우도 많으며, 자신의 이익을 위해 감시 대상 스스로가 선택하는 행위인 경우도 많다. 그렇다면 모든 감시를 부정적으로 볼 필요는 없다. 오히려 사회 발전을 위해 정상적으로 요청되는 행위일 경우가 많다.

---

22) 후기산업사회론의 개척자인 다니엘 벨은 정보 사회를 "지식이 사회의 핵심적 전략 자원이 되는 사회"로 규정한 바 있다. 그러나, 지식과 정보는 서로 다른 개념이다. 정보가 '데이터에 의미 내용이 부여되어 가공된 형태'라면, 지식은 '타인에게 전달된 정보가 전달받은 사람에게 습득되어 인지 구조에 통합되고 의미가 부여된 것'이다. 이처럼 정보와 지식을 구분해서 본다면, 현재 사회를 "지식"이 핵심적 전략 자원이 되는 사회로 규정하기에는 다소 무리가 있다는 지적이 있다. 박인우, 『지식 정보 사회와 우리 교육의 방향』, 함께하는 시민행동 엮음, 『인터넷 한국의 10가지 쟁점』, 서울 : 역사넷, 2002, pp. 236-237.

23) David Lyon & Elia Zureik, "Surveillance, Privacy and the New Technology," *Computers, Surveillance, and Privacy*, Minneapolis: Univ. of Minnesota Press, p. 3.

<표 2> 의도와 방식에 따른 감시의 분류

구분		감시의 의도 및 영향	
		악의적 감시	선의에 의한 감시
감시의 방식	은밀	**일반적 개념의 감시** 뒷조사, 음해, 개인정보 침해 등	**사적 배려, 보살핌**
	공개	**부정적 정책에 의한 감시** 전체주의 사회에서의 공개적 검열, 나치의 유대인 색출 등	**사회에 부정적인 요소에 대한 감시** 업무 감사, 사회복지정책, 정보공개 요구, 신용정보 조사

출처 : 고영삼, 전자감시사회와 프라이버시, 서울 : 한울아카데미, 1998, p. 21을 통해 재구성

한편 감시 행위를 감시의 주체와 대상으로 나누어 생각해볼 필요가 있다. 감시 행위는 기본적으로 권력 현상이므로, 국가와 기업 등 권력 자원을 가진 집단을 하나의 주체로, 그리고 통치 및 기업 활동의 대상으로서 일반 시민(이자 소비자)을 다른 하나의 주체로 놓고 구분해보면 <표 3>과 같이 구분할 수 있다.

<표 3> 주체와 대상을 기준으로 분류한 감시 행위

		감시 주체	
		국가 및 기업	시민사회
감시 대상	국가 및 기업	국가 기구간 감시(3권 분립 등) 경쟁 기업간 상호 감시	시민사회의 행정 감시, 기업 감시, 역감시*
	시민사회	행정·정책 수행을 위한 감시 범죄에 대한 감시 반대자 탄압을 위한 감시	불법에 대한 감시·고발 스토킹, 사적 도청 등

* 역감시 : 감시 대상이 감시주체의 감시 행위의 타당성을 거꾸로 감시하는 것

나. 정보사회에서 감시의 문제

앞에서 살펴본 바와 같이, 모든 사회 구성원들은 감시의 주체로든 대상으로든 그리고 긍정적 의미의 감시든 부정적 의미의 감시든 일상적으로 감시 행위에 참여한다.

<표 3>의 분류에서 볼 때, 정보사회에서 문제가 되는 것은 국가 및 기업이 시민사회에 대해 감시하는 것과 시민사회 상호간에 이루어지는 감시이다. 시민사회 상호간에 이루어지는 감시 중 문제가 되는 것은 스토킹이나 초상권 침해, 사적 도청이나 사생활 침해 등이 있다. 최근 개인적으로 혹은 심부름 센터 등을 통해 가족·연인·동료 등의 사적 생활을 도청하는 경우가 증가하고 있으며, 카메라 폰을 이용하여 유명인의 나체 사진을 몰래 촬영하여 인터넷을 통해 유포하는 경우도 많다. 타인의 아이디와 비밀번호를 알아내어 이메일을 몰래 읽거나, 아예 사이버 공간에서 그 사람 행세를 하는 경우도 있으며, 심한 경우 타인 명의로 신용카드를 발급받아 사용하는 경우도 빈번하게 발생한다. 사회적 문제가 되고 있는 스팸 메일의 경우도 상당수가 개인들의 이메일 아이디를 몰래 사용하였다는 점에서 시민 상호간에 발생하는 감시 행위의 결과이다.

시민사회 상호간의 감시에서 문제가 되는 것이 명백히 부정적 의도를 갖고 이루어지는 반면, 국가나 기업이 시민사회를 감시하는 경우는 다소 모호하다. 명백히 부정적 의도를 갖고 이루어지는 감시 행위들이 존재하는 것은 사실이나, 더욱 많은 감시 행위가 사회복지 정책의 수행이나 범죄의 예방 그리고 소비자에 대한 서비스 증진 등 긍정적 의도를 가지고 추진되기 때문이다.

문제는 과거와 달리 긍정적 의도를 갖고 추진되는 감시 행위라고 해서 안심하고 받아들일 수 없는 상황이 되었다는 점이다. 우선 축적되는 정보의 양이 엄청나게 증가했다. 여러 국가기구가 정책적으로 수집하는 개인정보를 취합하면, 사실상 모든 국민의 삶을 연대기적으로 재구성하는 것이 가능하다. 나아가 정보가 디지털화되면서 정보의 전달과 통합 및 재구성이 매우 용이해졌다. 따

라서 긍정적 의도로 수집된 정보라 하더라도 이후에 부정적 의도로 활용될 가능성을 무시할 수 없으며, 악의를 가진 사람의 손에 유출될 가능성도 크다. 마지막으로 이 두 요소가 결합됨에 따라 개인에 대한 조작이 가능해진다. 기업이 소비자의 구매 정보를 취합·분석하여 효과적으로 타겟 마케팅을 전개하면 소비자의 선택이란 사실상 무용지물이 된다. 이는 수요와 공급의 일치를 조건으로 하는 자본주의 경제의 정상적 가동을 위협하는 요인이 될 것이다. 나아가 국가 권력이나 특정 정치 세력이 같은 일을 할 경우, 민주주의 자체도 위협받게 된다.

결국 산업사회에서 환경 문제가 그렇듯이, 감시 및 이로 인한 프라이버시 침해라는 문제는 정보사회의 발전에 따른 부산물이면서 정보사회의 지속가능성에 본질적 한계를 가져오는 문제이다.

이러한 경향은 최근 들어 인터넷의 발전으로 개인들 사이의 네트워크가 강화되고 개인정보의 거대한 통합 데이터베이스가 구축됨으로써 더욱 심화되고 있다. 인터넷이라는 공간 속에서 개인들의 참여의 폭이 넓어진 만큼 개인들은 이전보다 훨씬 높은 밀도로 연결된다. 개인들 사이의 상호작용이 훨씬 빈번하게 이루어질 뿐만 아니라 주고받는 정보의 양도 늘어나게 된다. 이런 방식으로 개인들은 개별적으로 존재하고 있는 것이 아니라 인터넷이 만들어 놓은 거미줄 같은 관계의 망 속에서 지금과 여기라는 시간과 공간의 물리적 한계를 넘어 서로 연결되어 있다. 개인들이 거미줄 망과 같은 네트워크로 연결됨에 따라 개인들의 독자성과 프라이버시는 더욱 위험한 상황에 놓이게 되었다. 즉, 지식정보 사회의 지식체계와 네트워크는 개인들 사이의 통합과 참여의 가능성은 높여주었지만 반대로 개인의 고유한 권한인 독립적 주체성의 영역은 극도로 위축시켜 놓는 모순을 가져왔다.[24]

지식정보 사회에서는 중앙집권적인 국가의 힘이 여전히 남아있는 상태에서, 보다 분산화된 통제와 감시가 동시에 진행되고 있다. 개인들이 하나의 거대한 거미줄과 같은 네트워크를 형성하고 있기 때문에 그 네트워크의 중요한 분기

---

24) Manuel Castells, *The Rise of Network Society*, Oxford: Basil Blackwell, 1996.

점마다 개인을 감시하는 체계가 발전하고 있다. 이것은 전통적인 감시의 주체인 빅 브라더와 함께 분산화된 감시의 주체로서의 리틀 브라더가 곳곳에 존재하고 있음을 의미한다.[25] 따라서 개인에 대한 감시는 이전보다 분산되긴 했지만 약화되진 않은 채 오히려 더 널리 실행되어 감시의 보편화가 일어나게 된 것이다. 현대사회에서 개인이 처한 이러한 상황은 흔히 프라이버시의 종말(end of privacy)로 일컬어진다.[26] 따라서 정보사회에서 축적된 지식을 바탕으로 일어나는 개인에 대한 감시와 통제는 현대 사회가 맞이한 위기의 중요한 근원이다. 이러한 위기를 극복할 수 있는 중요한 방안 가운데 하나가 곧 개인정보에 대한 자기통제권을 확립하는 것이다.

2. 자기정보통제권의 개념과 의의

프라이버시 권리의 기원은 1888년에 쿨리 판사가 제기하고 1890년 워렌과 브렌다이스가 이론화한 '혼자 있을 권리'이다. 브랜다이스는 당시 사회의 문명발전으로 인간 생활이 매우 복잡하게 되었기 때문에 세계에서 도피할 수 있는 어떤 것이 필요하다고 주장하며 프라이버시 권리를 확립했다.[27] 이후 20세기 중반까지 프라이버시 권리는 (특히 언론에 대한 대항권의 성격을 지니며) 신

25) 김동노, 『지식정보사회의 감시체계와 개인의 프라이버시』, 『계간 사상』, 2003년 봄호, p. 153.

26) 이에 관해서는 Richard Spinello, "The End of Privacy", *America*, No. 176, reprinted in Robert Long, ed., *Rights to Privacy*, New York: H.W. Wilson Co., 1997을 볼 것.

27) 김주환, 『디지털 시대의 프라이버시 권리』, 김주환 외, 『디지털 시대와 인간 존엄성』, 서울 : 나남출판, 2001, p. 16. 이론적으로는 이들의 논의가 기원이 되고 있으나, 실제로 프라이버시에 대한 요구는 훨씬 일찍부터 존재해왔다. 세계 최초의 프라이버시 입법은 1361년 영국에서 제정된 '집안의 내부를 훔쳐보는 것을 금지하는 법률'로 거슬러 올라간다. 또, 1765년 영국의 Camben 경은 Entick vs. Carrington 사건에 대한 판결에서 "사적 문서는 개인이 보유할 수 있는 가장 소중한 재산"이라며 개인의 문서를 압수하기 위해 무단 가택 침입을 한 당국의 위법성을 지적했다. 스웨덴의 1776년 공공문서공개법에서는 정부의 모든 보유 문서가 입법목적을 위해서만 사용해야 한다고 규정되었으며, 프랑스에서도 이미 1885년에 프라이버시 침해를 불법행위로 법률에서 다루고 있었다고 한다. 정영화 외, 앞의 책, pp. 59-60.

체 및 사적 공간에 대한 소극적 방어의 권리로 존재했다.

그러나 1960년대에 들어 메인프레임 컴퓨터가 실용화되면서 국가 기관을 중심으로 정보 처리 능력이 크게 확대된다. 이는 감시 사회의 도래라는 어두운 전망에 대한 두려움을 확산시켰다. 이와 함께 다른 한편으로는 혼자 있을 권리라는 기존의 프라이버시 권리가 더욱 복잡해진 현대 사회에서는 적절하지 못하다는 문제가 제기된다.

그 결과, 자기정보통제권에 대한 문제의식이 등장한다. 즉, '자신에 관한 정보를 언제, 어떻게, 어느 정도 타인에게 유통시킬 것인지를 스스로 결정할 수 있어야 한다'는 문제의식이다.[28] 이는 다시 세 가지로 구분된다. 타인이 가진 자기 정보를 열람할 수 있는 자기정보접근권, 잘못된 자기 정보를 바로잡을 수 있는 자기정보정정청구권, 그리고 정보처리로부터 벗어날 수 있는 자기정보삭제청구권이 그것이다.[29]

그러나 이것만으로도 개인정보 보호의 의미를 충분히 설명하기 어렵다는 점이 지적되기도 한다. 앞에서도 살펴보았듯이, 개인에 대한 감시는 이미 정상적·공적 행위이며, 그로 인해 침해받는 권익 역시 개인의 권익이라기보다는 이미 사회적 피해로 나타나게 된다. 즉, '공공재로서의 프라이버시'라는 역설적 개념이 등장한다는 것이다. 이런 점에서 자기정보통제권을 전통적인 프라이버시 개념에서 분리해 공적 권리로 전환시킬 필요성을 강조하는 입장이 나타난다. 김종철은 다음과 같이 주장한다.

> 프라이버시의 족쇄로부터 해방된 새로운 개인정보통제권은 자신의 정보가 어떻게 수집, 처리, 관리, 이용되는지에 대한 감독권을 의미한다. 이 권리는 적극적 프라이버시권의 개념 하에 보호되던 정보에의 접근권과 정보수정, 삭제권을 그 내용으로 포섭할 뿐만 아니라 이 정보가 원래의 목적달성을 위해서만 사용되고 있는지에 대한 감독권까지 포함하는 것이다.[30]

---

28) 신종철, 『프라이버시 보호의 사회적 과제』, 함께하는 시민행동 엮음, 앞의 책, p. 120.
29) 권영성, 『헌법학원론』, 서울 : 법문사, 2000, p. 428.
30) 김종철, 『헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론』, 법무부, 『인터넷 법률』 제4호(2001년 1월) p. 36.

3. OECD 가이드라인의 개인정보보호 원칙 검토

프라이버시의 보호의 국제적 기준으로 받아들여지는 원칙은 OECD가 1980년에 제시한 「개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인」(이하 OECD 가이드라인)이다. 이 법률에서는 개인정보의 취급과 관련하여 8가지 원칙을 제시하고 있는데, 이는 그 전후로 제정된 세계 각국의 프라이버시 보호 법률의 주요 내용으로 자리잡고 있다. 그 원칙들은 다음과 같다.

▲ 수집제한의 원칙 : 모든 개인정보는 적법하고, 공정한 수단에 의해 수집되어야 하며, 정보주체에게 알리거나 동의를 얻은 후 수집되어야 한다.

▲ 정보내용정확성의 원칙 : 개인정보는 그 이용목적에 부합하는 것이어야 하고, 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태로 유지하여야 한다.

▲ 목적 명확화의 원칙 : 개인정보를 수집할 때는 목적이 명확해야 하고, 이를 이용할 경우에도 애초의 목적과 모순되지 않아야 한다.

▲ 이용제한의 원칙 : 개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화된 목적 이외의 용도로 공개되거나 이용되어서는 안 된다.

▲ 안정성 확보의 원칙 : 개인정보의 분실, 불법적인 접근, 파괴, 사용, 수정, 공개위험에 대비하여 합리적인 안전보호 장치를 마련해야 한다.

▲ 공개의 원칙 : 개인정보에 관한 개발, 운용 및 정책에 관해서는 일반적인 공개정책을 취하여야 한다. 개인정보의 존재, 성질 및 주요 이용목적과 함께 정보관리자의 신원, 주소를 쉽게 알 수 있는 방법이 마련되어야 한다.

▲ 개인 참가의 원칙 : 정보주체인 개인은 자신과 관련된 정보의 존재확인, 열람요구, 이의제기 및 정정・삭제・보완 청구권을 가진다.

▲ 책임의 원칙 : 개인정보 관리자는 위에서 제시한 원칙들이 지켜지도록 필요한 제반조치를 위해야 한다.[31]

---

31) 조양호, 『OECD의 개인정보 보호 8가지 원칙』, 함께하는 시민행동 부설 인터넷 시민학교 굿시티즌 온라인 강좌 『프라이버시 - 빅브라더를 막아라』

즉, 개인정보는 당사자의 동의 하에 수집되고, 그 이후의 활용도 수집 당시 동의받은 사항에 충실해야 하며, 이를 위협할 수 있는 모든 요소들을 제거하기 위해 노력해야 한다는 것이다.

위에서 살펴볼 수 있듯이, OECD 가이드라인은 개인정보의 수집 및 이용이 기본적으로 개인의 동의 하에서 이루어져야 한다는 계약론적 사상에 기반하여 제정되고 있다. 다른 원칙들은 개인의 동의를 실질적으로 보장하기 위해 요구되는 원칙들을 나열하고 있다.

그런데 이러한 계약론적 사상은 프라이버시 혹은 개인정보의 문제에 내재한 권력 현상을 고려하지 않는다는 근본적 문제가 있다. 계약이란 계약의 양 당사자가 자유롭고 평등한 상태에서 체결할 때 정당성을 인정받을 수 있다. 이러한 논리적 정당성과는 달리 현실에서는 국가나 기업이 개별 정보주체에 비해 압도적인 정치적·경제적 힘을 행사할 수 있는 권력 불균형 상태가 존재한다. 따라서 개인의 동의라는 것은 사실상 순수한 의미에서의 동의라기보다는 강요된 동의일 가능성이 크다. 국가가 법률이나 정책을 통해 부당한 개인정보 수집을 강행하거나 기업이 서비스 제공의 대가로 부당한 개인정보 수집을 요구하더라도 법률을 위반하거나 서비스를 포기하지 않고서는 사실상 이를 거부하거나 이의를 제기할 방법이 없는 것이 현실이다.

또한 많은 경우 정보 수집자와 정보주체 사이에는 정보 불균형 상태가 존재한다. 개인정보와 관련된 많은 사안이 기술적 요소를 포함하고 있는데, 이에 대해서 개별 정보주체가 정확한 정보를 갖기는 사실상 어렵다. 마찬가지로 수집된 정보를 정보 수집자가 실제로 어떻게 취급·사용하고 있는지를 확인하는 것도 개별 정보주체에게는 거의 불가능한 일이다.

4. 정보통신기술의 발전과 개인정보 보호 원칙의 현대화 방안

결국, OECD 가이드라인의 근본적 문제는 '계약'이라는 이름 하에 자기정보

(http://www.goodcitizen.or.kr/lecture/list.asp?b_number=195&b_code=code2)

통제권을 실현할 책임을 개별 정보주체에게 떠맡기고 있다는 점이다. 그렇기 때문에 앞에서 살펴본 김종철의 논의는 자기정보통제권을 공적 권리로 해석할 것을 주장하면서, 정보수집자에 대한 역감시권 즉 정보수집자의 정보처리 행위에 대한 감독권을 주장하고 있다.

이는 유럽의 개인정보 보호 전통과도 일맥상통한다. 전통적으로 유럽은 개인정보 보호를 국가가 보호할 기본권의 문제로 간주한다. 이에 따라 국가 및 민간의 정보수집자들로부터 독립적인 감독 기구가 정보 수집자들을 일상적으로 감독하도록 하고 있다.[32] 즉, 개별 정보주체들로부터 개인정보 수집자들에 대한 감독권을 위임받은 별도의 국가 기구를 운영하는 것이다.

그러나 역감시권을 국가 기구에 의해 실현되는 권리로 이해하는 것은 바람직하지 않다. 역감시권 역시 근본적으로 개인에게 부여되는 권리이며, 다만 개별 정보주체에게 맡겨졌을 때 발생하는 권력 불균등 및 정보 불균형 현상을 보완하기 위해 감독권을 집단적으로 행사하는 것으로 이해하는 것이 옳은 방향이다. 마치 공권력의 행사에 대해 개인이 저항권을 가질 수 있는 것처럼, 개인정보에 대한 국가의 공권력이 가진 무제한의 권력에 대해 개인이 가질 수 있는 유일한 저항권의 권리가 정보의 자기통제권과 역감시권이다. 이후 논의에서는 이같은 거대 권력 대 개인의 불균형 상태가 현실적으로 어떻게 드러나는지를 검토하고, 이를 보완하기 위한 제도적 방안들을 모색해볼 것이다.

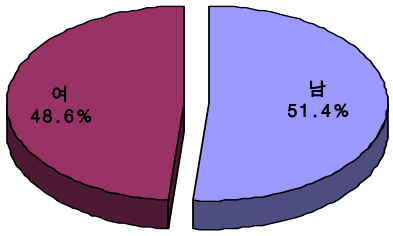
32) 이인호, 앞의 글, p. 141.

Ⅲ. 개인정보 보호에 관한 이용자들의 의식과 태도

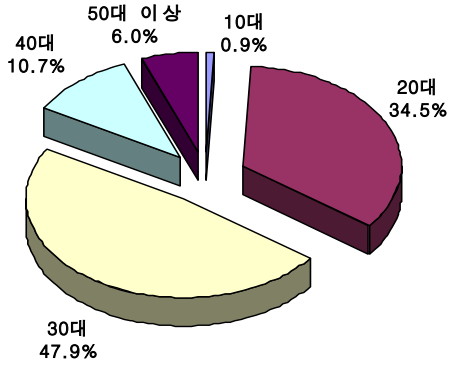
개인정보 보호에 관한 이용자들의 의식과 태도를 조사하기 위하여, 전문 인터넷 설문조사 기관인 (주)폴에버에 의뢰하여 인터넷 이용자 1,042명을 대상으로 설문을 실시하였다. 조사 내용은 ① 인터넷 사용자들의 개인정보보호에 대한 인식 및 태도 ② 인터넷 사이트의 개인정보 수집 및 이용실태 ③ 인터넷 사이트의 개인정보 관련 고객상담 실태 등이었다. 조사에 대한 기본적인 사항은 다음과 같다.

○ 모집단 : 대한민국 거주 인터넷 이용자
○ 표본크기 : 1,042명
○ 표본추출 : 표본추출
○ 자료수집방법 : 구조화된 설문지를 이용한 인터넷 패널 조사

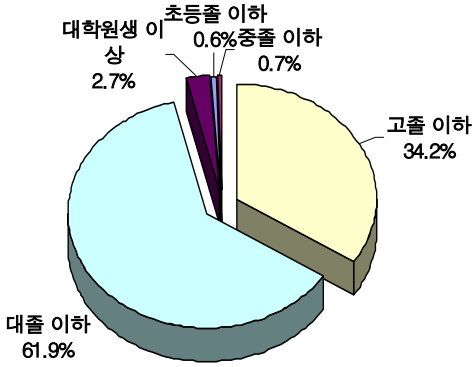
이 설문조사에 응답한 응답자들의 기본적인 인구학적 특성들은 다음과 같다. 연령별로 봤을 때 10대가 적은 이유는 리서치 업체의 조사방식 때문이다. 사전에 패널회원으로 가입한 사람들에 대해 설문을 실시했는데 상대적으로 10대의 회원가입률이 낮았다.



[그림 1] 성별에 따른 응답자의 구성비율



[그림 2] 연령에 따른 응답자의 구성 비율



[그림 3] 학력에 따른 응답자의 구성비율

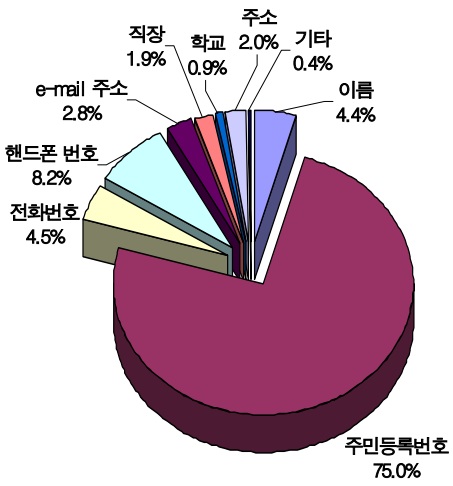
인터넷 이용자를 대상으로 하는 설문조사는 크게 나누어 “자기정보 통제권을 제약하는 정보수집관행에 대한 태도”, “약관 및 개인정보보호 정책에 대한 인지도”, “개인정보의 제3자 제공 및 공유에 대한 인지도”, “개인정보 고충처리에 대한 만족도” 조사로 구성된다.

1. 자기정보통제권을 제약하는 정보 처리 관행

가. 이용자들이 민감하게 취급하는 개인정보에 대한 수집 여부

「정보통신망이용촉진및정보보호등에관한법률」 및 정보통신부의 「개인정보보호지침」에서는 정보통신서비스제공자가 사상, 신념, 과거의 병력 등 개인의 권리, 이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하지 못하도록 규정하고 있다. 그러나 이러한 규정은 수집이 제한되어야 하는 정보의 범위를 최소한도로 규정한 것일 뿐, 실제 서비스 이용자들이 생각하는 민감한 개인 정보의 범위는 더 넓다고 봐야 할 것이다.

실제로 사이트들에서 요구하고 있는 개인정보에 대하여 조사한 결과 이용자들이 인터넷 사이트 회원 가입 시 가장 입력을 꺼려하는 정보로는 주민등록번호가 75.0%로 가장 높게 나타났다. 다음으로 핸드폰번호 8.2%, 전화번호 4.5%, 이름 4.4%, e-mail 주소 2.8% 등의 순이었다.



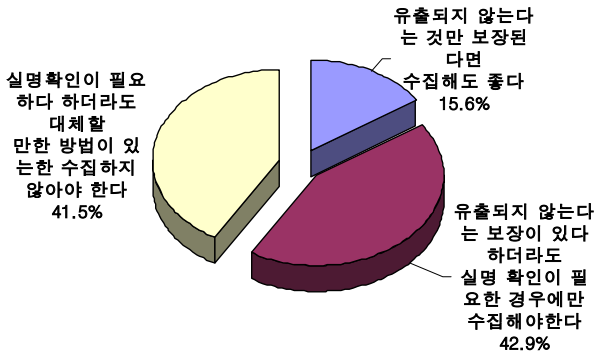
[그림 4] 이용자들이 민감하게 취급하는 개인정보

이용자의 75%가 주민등록번호를 입력하는 것을 꺼리는 것에 반해, 모든 상업적 사이트 심지어 개인 홈페이지에서조차 주민등록번호를 요구하는 것은 우리나라에서 주민등록번호가 본인을 확인 할 수 있는 거의 유일한 코드로 인식되고 있기 때문이다. 그러나 조사에서 나타난 바와 같이 주민등록번호는 이용자들이 아주 민감하게 생각하는 개인정보이며, 범죄에 악용되었을 경우 매우 심각한 피해를 줄 수 있다는 점에서 주민등록번호의 수집이 제한되는 것이 바람직할 것이다.

다음 장에서 다시 논의될 예정이지만, 실제로는 실명확인이 거의 필요 없는 경우에도 주민등록번호의 수집이 이루어지고 있는 경우가 많다. 또한 실명확인이 필요한 경우에도 주민등록번호를 대체할 수 있는 대안적 방안의 모색이 필요한 실정이다. 주민등록 번호를 기반으로 하는 통합 데이타베이스 구축이 점차 널리 퍼지게 됨에 따라 한 개인의 주민등록번호를 취득하는 경우 개인정보가 송두리째 유출되거나 악용될 수 있는 가능성이 커지기 때문에 그러하다.

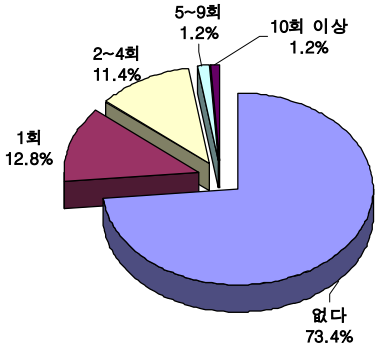
나. 주민등록번호 수집으로 인한 자기정보통제권 침해 여부

주민등록번호 수집에 대한 설문에서, 응답자중 회원 가입 시 주민등록번호를 요구하는 것에 대해, 유출되지 않는다는 보장이 있다 하더라도 실명확인이 필요한 경우에만 수집해야 한다고 대답한 사람이 42.9%로 가장 많았다. 그리고 실명확인이 필요하다 하더라도 대체할 만한 방법이 있는 한 수집하지 않아야 한다(41.5%)는 응답도 높게 나타났다. 유출되지 않는다는 것만 보장된다면 수집해도 좋다는 응답은 15.6%에 그쳐 상당히 낮은 지지도를 얻은 것으로 나타났다. 실명확인이 반드시 필요한 경우에도 주민등록번호 확인 이외의 다른 실명확인 방식이 있다면, 이용자들은 그 방식을 선호할 것임을 알 수 있다.



[그림 5] 회원가입시 주민등록번호 요구에 대한 태도

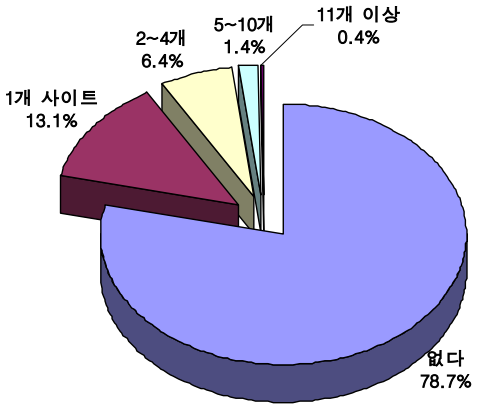
실제 인터넷 사이트에 회원 가입 시 주민등록번호가 도용되어 회원가입이 실패한 경험에 대해 질문한 결과, 1회(12.8%)라고 답한 사람이 가장 많았으며, 2~4회라고 답한 응답자가 11.4%, 5~9회 1.2%였고 10회 이상도 1.2%로 나타났다. 따라서 주민등록번호 도용으로 인한 회원 가입 실패 경험이 있는 경우는 모두 26.6%로 네 명 중 한 명꼴로 주민등록번호가 도용된 경험이 있는 것으로 나타났다. 이는 주민등록번호로 인한 자기정보통제권 침해 문제가 결코 그냥 넘어갈 수 없는 수준에 이르렀다는 것을 보여준다.



[그림 6] 주민등록번호 도용으로 인한 회원가입 실패 경험

다. 자유로운 회원 탈퇴의 제약 여부

온라인에서 회원가입 시 주민등록번호를 입력하는 것과는 별개로 회원 탈퇴 시 신분증 사본이나 주민등록등본을 제출할 것을 요구하는 사이트가 있었냐는 질문에 없다고 대답한 응답자가 78.7%였고, 1개사가 요구한 경우가 13.1%, 2~4개의 경우가 6.4%, 5~10개사의 경우가 1.4%, 11개사 이상의 경우가 0.4%로 나타났다. 결과적으로 회원 탈퇴 시 신분증 사본이나 주민등록등본 제출을 요구한 사이트는 전체적으로 22.3%에 이르렀다. 「정보통신망이용촉진및정보보호등에관한법률」 제30조 6항[33]은 회원 가입 절차보다 회원 탈퇴 절차를 어렵게 하는 것을 금지하고 있다. 그런 절차가 정보주체의 자유로운 동의 철회를 어렵게 하기 때문이다. 기본적으로 회원 탈퇴가 온라인 상에서 이루어질 수 있도록, 탈퇴 메뉴를 온라인으로 제시해야 할 것이다.



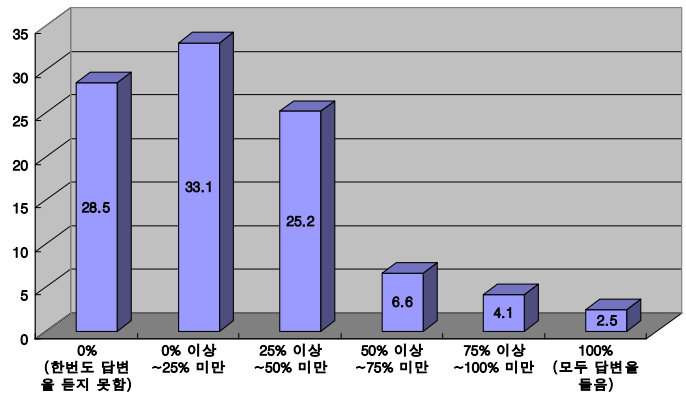
[그림 7] 회원탈퇴 시 신분증 사본, 주민등록등본을 요구한 사이트

33) 제30조 (이용자의 권리 등) ⑥정보통신서비스제공자등은 이용자로부터 제1항 및 제2항의 규정에 의한 동의의 철회, 개인정보의 열람 또는 정정의 요구를 받은 경우에는 제22조 및 제23조의 규정에 의하여 개인정보를 수집하는 방법보다 쉽게 할 수 있도록 필요한 조치를 취하여야 한다.

라. 자기정보 유통 경로에 대한 고객의 알 권리 보장 여부

이용자가 서비스를 이용하기 위해 제공한 개인정보는 정보주체가 동의한 범위 안에서 서비스 제공자가 보관, 이용할 수 있으나 궁극적으로 개인정보에 대한 소유권은 정보를 제공한 주체에게 있다. 따라서 정보주체는 자기 정보가 어떻게 이용되고 있는지 언제나 확인할 수 있어야 하며, 제휴사 등 제3자에게 제공되는 경우 그 유통경로를 확인 할 수 있는 권리가 있다.

개인정보의 유통경로에 대한 고객의 알권리 보장 실태를 알기 위해 텔레마케팅 전화가 걸려올 경우 개인정보 취득 경위를 알려주는지 여부를 조사하였다. 텔레마케팅 전화를 받았을 때 개인정보 취득 경위에 대해 질문을 한 경험이 있다고 대답한 응답자는 242명(23.2%)이었다. 이 중, 질문에 대해 한 번도 답변을 듣지 못한 경우가 28.5%로 나타났으며, 0~25%미만이 33.1%, 25~50%미만이 25.2% 등으로 나타나, 개인정보 취득경위에 대한 응답 비율이 50%미만인 경우가 86.8%에 달했다. 반면 개인정보 취득경위에 대한 응답을 50%이상 받은 경우는 13.2%에 불과했다.



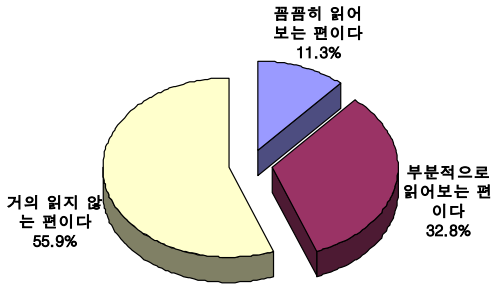
[그림 8] 개인정보 취득경위에 대한 회신여부

2. 약관·개인정보보호정책에 대한 인지도

가. 개인정보보호정책·약관에 대한 이용자들의 관심도 조사

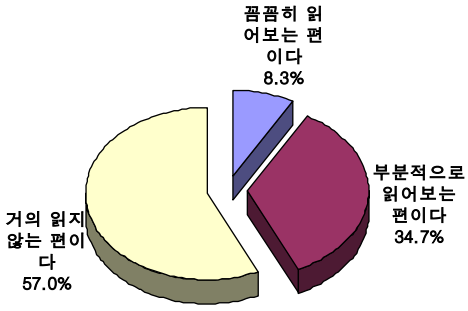
정통부의 개인정보지침에서는 서비스 제공자가 개인정보보호정책을 홈페이지 첫 화면에 링크 등을 통하여 이용자가 쉽게 볼 수 있도록 할 것을 의무화하고 있다. 다음 장에서 다루고 있는 기업의 고객 자기정보권 보장 실태 조사에 따르면 대부분의 기업들이 기본적인 정책 고지의 의무는 준수하고 있는 것으로 나타났다. 반면, 서비스 이용자의 입장에서 보면, 개인정보보호정책 및 회원가입 시 동의하게 되는 약관은 일종의 계약서로 반드시 읽어야 할 의무가 있다고 할 수 있다. 그러나 서비스 이용자들의 약관 및 개인정보보호정책에 대한 이용자들의 관심도 조사는 많은 문제점을 보여주고 있다.

회원가입 시 약관 확인 여부에 대한 질문에 대해 전체 응답자 1,042명 중 인터넷 서비스를 이용하기 위해 회원가입을 할 때 이용약관을 "꼼꼼히 읽어보는 편이다"라고 응답한 비율은 8.3%에 불과했다. "부분적으로 읽어보는 편"이라고 답한 응답자가 34.7%, "거의 읽지 않는 편이다"가 무려 57.0%로 나타났다.



[그림 9] 회원가입 시 약관을 읽는 정도

이러한 현상은 개인정보보호정책에도 마찬가지였는데, “거의 읽지 않는다”는 대답을 한 응답자가 55.9%였고, “꼼꼼히 읽어보는 편이다”라고 응답한 비율은 11.3%에 불과했다



[그림 10] 회원가입 시 개인정보 보호정책을 읽는 정도

<표 4> 인터넷 사용정도와 약관 관찰정도의 상관성[1]

		포털 사이트 가입 수			전체
		0-2개	3-5개	6개 이상	
이용약관 관찰정도	꼼꼼히 읽음	48 (9.4%)	26 (8.3%)	5 (5.0%)	79 (8.5%)
	부분적으로 읽음	155 (30.3%)	122 (39.0%)	37 (36.6%)	314 (33.9%)
	거의 읽지 않음	309 (60.4%)	165 (52.7%)	59 (58.4%)	533 (57.6%)

1) χ^2 = 8.534 (p = .074)

한 가지 흥미로운 사실은 인터넷의 이용정도와 약관을 읽는 정도 사이에 상관성은 거의 없는 것으로 나타났다는 사실이다. 인터넷 사용정도를 포털 사이트의 가입수로 측정한 후, 사이트 회원가입 수와 이용약관을 읽는 관계를 조

사해 보았는데, 이 둘 사이에는 거의 관계가 없는 것으로 나타났다. 다음의 표에서 확인되듯이, 통계적으로 유의미하지는 않지만($p>.05$), 여러 사이트에 가입한 이용자일수록 오히려 약관을 읽는 정도가 약한 것으로 나타났다. 다음에 논의되겠지만, 이러한 경향은 거의 모든 사이트의 약관이 비슷하게 구성되어 있기 때문인 것으로 해석된다.

나. 개인정보보호정책·약관에 대한 이용자들의 만족도 조사

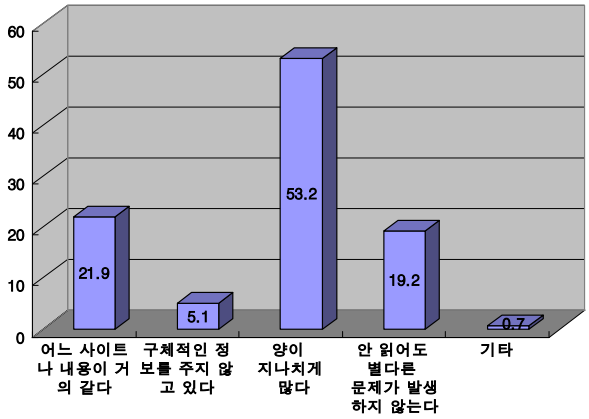
이용 약관 및 개인정보보호 정책은 서비스 제공자와 이용자간의 기본적인 계약 내용이며, 자기 정보 통제권 확보를 위한 가장 기본적인 소통 수단이 되는 것이기 때문에 이용자들이 이를 거의 읽지 않는 다는 것은 문제가 있다. 그래서 그 이유를 분석하기 위해 '이용약관 및 개인정보보호 정책을 거의 읽지 않는 편이다'라고 응답한 이들을 대상으로 읽지 않는 이유를 물었다.

이용약관을 거의 읽지 않는다고 답한 594명에게 질문한 결과, 양이 지나치게 많다(53.2%)는 응답이 가장 많았으며, 어느 사이트나 내용이 거의 같다(21.9%), 안 읽어도 별다른 문제가 발생하지 않는다(19.2%), 구체적인 정보를 주지 않고 있다(5.1%), 그리고 기타(0.7%)의 순으로 나타났다. 개인정보보호정책의 경우에도, 양이 지나치게 많다(53.2%)는 응답이 가장 많았으며 어느 사이트나 내용이 거의 같다(21.9%), 안 읽어도 별다른 문제가 발생하지 않는다(19.2%), 구체적인 정보를 주지 않고 있다(5.1%), 그리고 기타(0.7%)의 순으로 나타나 동일한 패턴을 보여주었다.

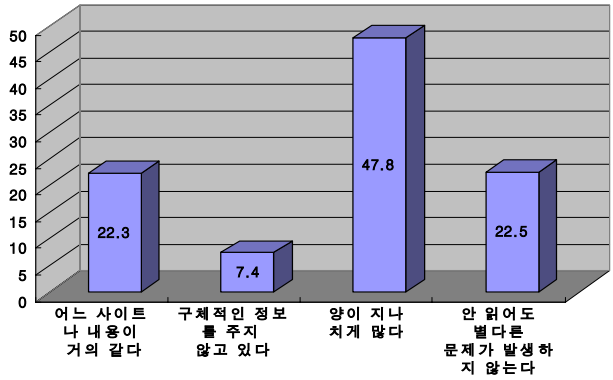
이러한 결과는 대다수의 이용자들이 약관 및 개인정보보호정책에 대한 중요성을 제대로 인식하지 못하고 있다는 점을 보여주고 있다. 그러나 보다 중요한 것은 서비스 제공자들이 약관이나 개인정보보호 정책을 형식적으로 게시하는데 머무르고 있을 뿐 이용자 입장에서 충실하게 고지하지 못하고 있다는 점이다. 약관이나 정책이 지나치게 복잡하고 양이 많아 이용자들이 읽지 않는다면, 각 사이트들은 약관이나 개인정보보호 정책을 보여줄 때 이용자들이 보다

쉽게 접근할 수 있도록 하는 방안을 찾아야 할 것이다.

그중 한 가지 방식은, 이용자들이 주로 관심을 가지는 부분과, 의무·권리 관계상 중요한 내용(특히 이용자에 불리한 내용) 등을 따로 떼어내서 이용자들이 쉽게 볼 수 있도록 하는 것이다. 현재 일부 사이트의 개인정보보호 정책에서는 이러한 방법을 사용하고 있으나 대다수의 사이트에서는 모든 내용이 동일하게 표시되거나 혹은 단지 글자 모양을 조금 진하게 하는 것 정도에 그치고 있다.

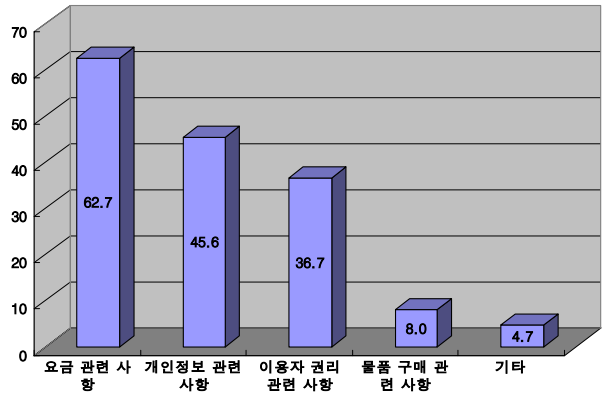


[그림 11] 이용약관을 읽지 않는 이유



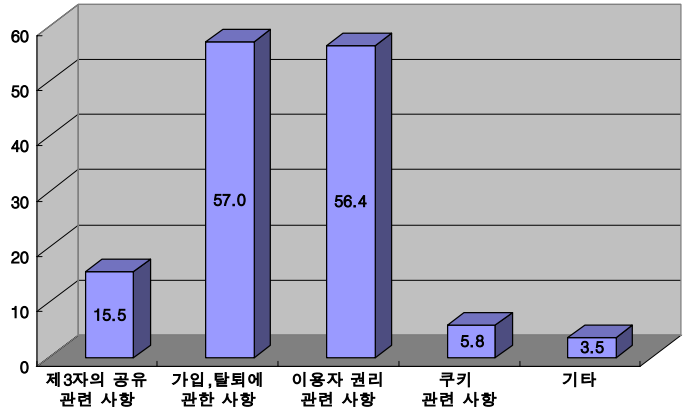
[그림 12] 개인정보보호정책을 읽지 않는 이유

이용자들이 중요하게 생각하는 부분을 알아보기 위해 이용약관을 “부분적으로 읽는 편이다”라고 응답한 362명을 대상으로 이용약관에서 주로 읽는 내용을 물었다. 복수응답을 허용한 이 질문에 대해 가장 많은 응답자가 요금관련 사항(62.7%)을 읽는다고 답했으며, 개인정보 관련 사항(45.6%), 이용자권리 관련 사항(36.7%), 물품구매 관련 사항(8.0%), 기타(4.7%)의 순서로 나타났다.



[그림 13] 이용약관에서 주로 읽는 부분

한편 개인정보보호정책에서 이용자들이 주로 관심을 가지고 읽는 내용은 가입, 탈퇴에 관한 사항(57.0%), 이용자 권리 관련 사항(56.4%), 제3자의 공유 관련 사항(15.5%), 쿠키 관련 사항(5.8%), 기타(3.5%) 순으로 나타났다. 결국 이 조사가 보여주는 것은 개인정보 주체들이 개인정보 공유의 위험성이나 쿠키에 의한 정보유출의 위험성보다는 이용자의 권리나 회원가입 및 탈퇴와 같은 절차상의 현실적인 문제에 더 큰 관심을 가지고 있다는 사실이다. 실제로 개인정보 유출이나 공유에 따른 위험은 비가시적이고 자주 일어나지 않을 것으로 가정하는 반면 권리나 절차의 문제는 가시적이고 직접적인 영향을 가지고 있기 때문에 그러한 것으로 이해된다.



[그림 14] 개인정보보호 정책에서 주로 읽는 부분

3. 기업의 고객 개인정보 제3자 제공에 대한 인지도

가. 개인정보 공유의 인지도와 정보공유에 대한 이용자의 태도

약관 및 개인정보보호 정책에서는 이용자로부터 수집한 개인정보의 제3자 제공에 대한 설명을 해야 한다. 개인정보의 공유 여부를 아는 것은 개인정보에 대한 자기정보통제권의 관점에서 매우 중요한 것이고, 특히 각종 스팸 메일과 텔레마케팅 전화, 광고 문자 메시지에 시달리는 현실을 고려하면 더욱더 그러하다.

그러나 실제 약관이나 개인정보보호 정책을 살펴보면, 이에 대한 설명이 매우 추상적이어서 이용자가 충분히 이해 할 수 없는 경우가 많다. 이에 대해서는 다음 장에서 다시 다루기로 한다. 다른 한편으로는 약관이나 정책에 개인정보 공유에 대한 설명이 있어도 실제 이용자들은 잘 알고 있지 못한 경우가 있는데, 이는 앞서 살펴 본 바와 같이 이용자들이 약관이나 개인정보보호 정

책을 잘 읽지 않기 때문인 것으로 보인다.

<표 5>는 현재 개인정보 공유에 대한 서비스 제공자의 고지 및 이용자의 이해 실태가 얼마나 심각한 상황인지 나타내주고 있다. 자신이 주로 이용하는 쇼핑몰, 포털, 언론사 등에서 자신의 개인정보가 공유되는 업체의 수를 안내 받았는지 여부를 묻는 질문에 모든 사이트에서 80% 이상이 안내 받지 못했다고 답했으며, '자신의 개인정보가 공유되는 업체가 몇 개인지 아는가'라는 질문에 대해서는 90% 안팎이 모르고 있다고 답했다. 이는 대부분의 사람들이 자신의 정보가 누구와 공유되고 있으며 누구에 의해 사용되고 있는지를 전혀 알지 못하고 있다는 뜻이다.

<표 5> 기업의 개인정보 공유에 대한 인지도

구 분		쇼핑몰 가입자	포털사이트가입자	언론사사이트가입자
개인정보 공유업체 수 안내 여부	받았음	17.2%	14.7%	10.7%
	못 받았음	82.8%	85.3%	89.3%
개인정보 공유업체 수 인지여부	알고 있음	10.4%	10.2%	8.0%
	모르고 있음	89.6%	89.8%	92.0%

또 이번 조사에서는 개인정보의 공유 인지여부와 인터넷의 이용정도는 무관한 것으로 밝혀졌다. 인터넷 사용빈도가 높을수록 개인정보에 대한 공유에 대한 안내를 받았을 가능성이 클 것으로 가정할 수 있으나, 조사에서는 이 둘 사이에는 관계가 없는 것으로 나타났다. 인터넷의 사용정도를 쇼핑몰에서의 구매경험과 포털 사이트에 가입한 수로 측정한 후 이를 개인정보 공유안내에 대한 인지여부와 연결시켜 보았다. <표 6>에서 나타났듯이, 인터넷 쇼핑몰에서 구매경험이나 포털 사이트의 가입 수와 무관하게 거의 대부분의 인터넷 이용자들은 일관되게 개인정보 공유여부를 안내받지 못한 것으로 응답했다.

<표 6> 인터넷 이용정도와 정보공유 인지여부 사이의 상관성

구 분		개인정보 공유 안내 받았다	개인정보 공유 안내 받지 못했다
쇼핑몰 구매경험[1]	없음	68 (21.3%)	251 (78.7%)
	1-10회	91 (15.7%)	487 (84.3%)
	11회 이상	20 (13.8%)	125 (86.2%)
전 체		179 (17.2%)	863 (82.8%)
포털 사이트 가입 수[2]	0-2개	75 (14.6%)	437 (85.4%)
	3-5개	45 (14.4%)	268 (85.6%)
	6개 이상	19 (18.8%)	82 (81.2%)
전 체		139 (15.0%)	787 (85.0%)

1) χ^2 = 5.844 (p = .054) 2) χ^2 = 1.295 (p = .523)

그러나 이러한 문제가 나타나는 이유를 인터넷 사이트의 부실한 규정마련에 기인하는 것으로 보기는 힘들다. 다음 장에서 본격적으로 논의하겠지만, 물론 인터넷 사이트 가운데는 필요한 규정을 제대로 마련해두지 못한 경우들도 있다. 그러나 보다 심각한 문제는 이용자들의 태도에서 찾을 수 있다. 이용자들은 대부분 개인정보 공유의 위험성에 대해 안일한 태도를 보여주고 있다. <표 7>에서 확인되듯이, 인터넷 사이트에서 정보수집의 목적을 어느 정도 구체적으로 명시했는지 여부에 상관없이 대부분의 이용자들은 개인정보 공유에 대한 안내를 받지 못했다는 태도를 보여주고 있다. 이러한 경향은 쇼핑몰 사이트, 포털 사이트, 그리고 신용카드 사이트에 공통적으로 나타나 사이트의 종류에 상관없이 이용자들이 개인정보 공유에 대해 무관심한 것으로 나타났다. 따라서 개인정보 공유를 포함한 개인정보 관리에 대한 규정을 보다 명확히 하여 각 사이트들이 이를 준수하도록 하는 제도적 차원의 노력도 중요하지만, 인터넷 이용자들에게 개인정보 관리의 중요성을 적극 교육, 안내하는 노력도 동시에 병행될 필요가 있다.

<표 7> 사이트의 정보수집목적 명시정도와 개인의 정보공유 인지여부 사이의 상관성

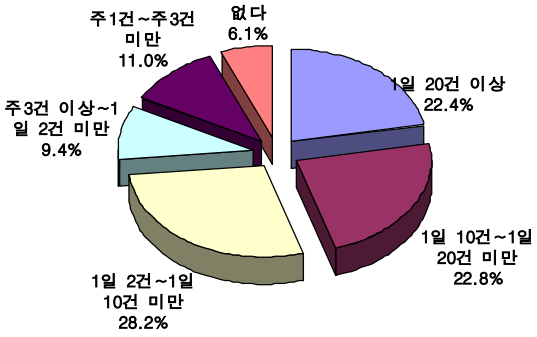
구 분		쇼핑몰 사이트[1]		포털 사이트[2]		신용카드 사이트[3]	
		안내받음	못 받음	안내받음	못받음	안내받음	못 받음
사이트의 정보수집목적 구체적 명시정도	구체적 명시	108 (17.3%)	517 (82.7%)	75 (15.2%)	417 (84.8%)	131 (13.4%)	848 (86.6%)
	개별항목 비명시	43 (17.9%)	197 (82.1%)	15 (13.2%)	99 (86.8%)	5 (12.2%)	36 (87.8%)
	추상적으로 명시	28 (15.8%)	149 (84.2%)	63 (14.4%)	373 (85.6%)	4 (18.2%)	18 (81.8%)
전체		179 (17.2%)	863 (82.8%)	153 (14.7%)	889 (85.3%)	140 (13.4%)	902 (86.8%)

1) χ^2 = .326 (p = .849) 2) χ^2 = .354 (p = .838) 3) χ^2 = .483 (p = .786)

나. 개인정보 공유와 스팸 메일

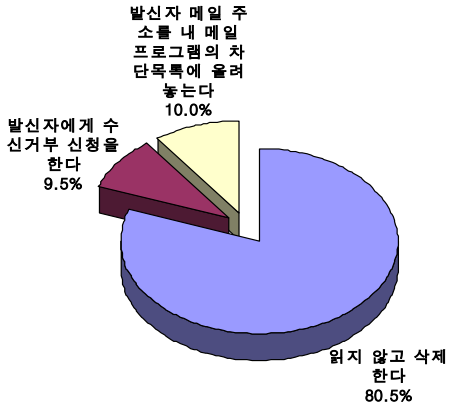
인터넷에서 나타나는 개인정보 공유에 따른 중요한 문제 가운데 하나는 최근 들어 사회문제가 되고 있는 스팸 메일의 범람이다. 물론 스팸 메일의 범람이 전적으로 개인정보의 공유에 기인하는 것으로 돌릴 수는 없지만 기업들 사이에 일어나는 개인정보의 공유가 상당한 정도로 기여하고 있는 것은 사실이다. 상업성 메일은 물론이며 심지어 성인 사이트의 광고가 연령에 관계없이 무차별적으로 배포되고 있는 현실에 비추어 보면 스팸 메일은 심각한 문제를 야기하고 있다. 이번 조사에서 실제로 개인들이 어느 정도로 스팸 메일을 수신하는지 알아보았는데, 현실적으로 느끼는 체감지수와 그리 다르지 않을 정도로 많은 스팸 메일이 뿌려지고 있음을 알 수 있었다. 하루에 10회 이상 스팸 메일을 수신하는 경우가 전체의 45.2%에 이르고 있으며, 하루 1회 이상 수신하는 경우는 73.4%에 이르고 있다. 이에 대한 적절한 대책이 시급히 요청되는 상황인데, 최근 정부가 '수신자 동의 없는 메일발송'을 금지하는 옵트 인

(opt-in) 정책을 채택하기로 한 것은 바람직한 정책수립으로 여겨진다.



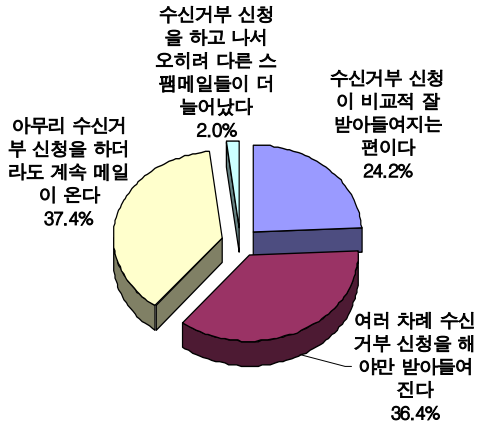
[그림 15] 스팸 메일 수신정도

스팸 메일이 이렇게 대량으로 살포되고 있음에 비해 이용자들의 대응은 상당히 소극적인 것으로 나타났다. 80.5%에 이르는 응답자들이 스팸 메일을 수신하는 경우 그냥 지워버리는 소극적 대응을 보여주고 있고, 발신자에게 수신거부를 신청하는 경우(9.5%)와 발신자 주소를 메일차단 프로그램에 올려놓는 경우(10%)는 상대적으로 소수에 지나지 않았다.



[그림 16] 스팸 메일에 대한 이용자의 대응

이용자들이 스팸 메일에 대해 이렇게 소극적으로 대응하는 이유는 여러 가지가 있겠지만, 수신거부의 효과가 그리 크지 않다는 것에서도 찾을 수 있다. 실제로 조사를 한 결과를 보면, 수신거부를 한 경우 잘 받아들여진 경우는 24.2%에 불과하고 여러 차례의 노력이 필요했던 경우가 36.4%, 그리고 아무리 수신거부를 해도 효과가 없었거나 오히려 수신거부 이후 스팸 메일이 더 늘어난 경우가 39.4%를 차지했다. 이러한 경향을 미루어 볼 때, 스팸 메일에 대한 옵트 인 정책과 함께 수신 거부된 메일에 대한 적절한 정책적 규제도 필요한 것으로 생각된다.



[그림 17] 스팸 메일의 수신거부에 관한 효과성

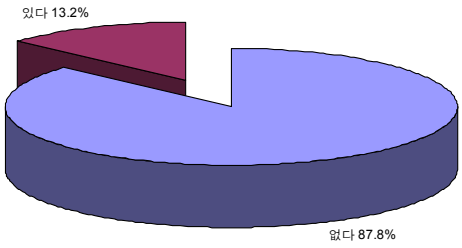
4. 개인정보 고충처리에 대한 만족도

「정보통신망이용촉진및정보보호등에관한법률」 및 「개인정보보호지침」에서는 서비스 제공자들이 개인정보관리책임자를 두도록 명시하고 있는데, 이는 개인정보와 관련한 일체의 책임 주체를 설정하고 동시에 이용자의 불만을 처리하기 위한 목적이 있다. 기업들이 채택하고 있는 개인정보 고충 처리 방식

에 대한 이용자들의 인식을 살펴보기 위하여 고객들의 이용 정도와 만족도를 조사하였다.

가. 기업의 개인정보 고충처리 체계에 대한 고객들의 이용 정도

기업의 개인정보 관련 고충 처리 업무는 크게 전화, e-mail, 상담게시판 등의 형태로 이루어지고 있었다. 인터넷 이용자들에게 개인정보 관련 불만이나 질문을 제기한 적이 있는가 물었을 때, e-mail를 통해 제기한 경험이 있는 경우가 14.7%로 가장 많았고, 게시판에 글을 올린 경우가 13.4%, 전화를 통해 제기한 경험이 있는 경우가 11.6%로 나타났다. 전체적으로 볼 때, 응답자의 87.8%가 문제를 제기한 경험이 없는 것으로 나타나 이용자들이 개인정보의 관리로부터 야기되는 문제에 대단히 소극적으로 대응하고 있음을 알 수 있다.



[그림 18] 개인정보 관리에 대한 불만제기 여부

이러한 상황 속에서 심각한 문제가 발견되고 있는데, 회원가입 시 주민등록번호 도용으로 가입에 어려움을 겪었던 응답자들도 대체로 문제를 제기하지 않은 채 그냥 지나치고 있다는 사실이다. 주민등록번호 도용경험 여부와 개인

정보관리에 대한 문제제기 여부의 상관성을 검토한 결과, 주민등록번호를 도용당한 경험이 있는 응답자들이 그렇지 않는 사람에 비해 보다 적극적으로 문제를 제기하고 있지만 그 차이의 정도는 그리 크지 않으며 대부분의 경우(80% 정도)에 전혀 문제를 제기하지 않고 있는 것으로 나타났다. 이것은 심각한 사회문제를 야기할 수 있는 주민등록번호의 유출 및 도용에 대해 인터넷 사용자들이 상당히 무관심하다는 것을 입증해 주는 자료인데, 이에 대한 문제제기와 이용자의 태도를 전환할 수 있는 정책적 홍보가 시급히 요청된다.

<표 8> 주민등록번호 도용경험과 문제제기 여부의 상관성

		전화를 통한 문제제기[1]		이메일을 통한 문제제기[2]	
		했음	안했음	했음	안했음
주민등록번호 도용의 경험	있음	51 (18.4%)	226 (81.6%)	69 (24.9%)	208 (75.1%)
	없음	70 (9.2%)	695 (90.8%)	84 (11.0%)	681 (89.0%)
전체		121 (11.6%)	921 (88.4%)	153 (14.7%)	889 (85.3%)

1) χ^2 = 16.994 (p = .000) 2) χ^2 = 31.498 (p = .000)

나. 기업의 개인정보 고충처리 체계에 대한 고객들의 만족도

개인정보 관련 불만이나 질문을 e-mail를 통해 제기한 경험이 있는 153명을 대상으로 개인정보 관리 책임자의 응답 비율을 물었을 때, 한 번도 응답을 받지 못한 경우는 11.6%, 응답비율이 0~25%미만인 경우는 30.1%, 25~50%미만인 경우가 11.8%, 50~75%미만이 19.6%, 75~100%미만이 7.8%, 그리고 100%(모두 전화를 받음)가 19.6%로 나타났다.

게시판을 통해 문제를 제기한 경험이 있는 140명을 대상으로 개인정보 관리 책임자의 응답을 받은 비율을 물었을 때는, 한 번도 응답을 받지 못한 경우가 15.0%, 응답비율이 0~25%미만인 경우는 29.3%, 25~50%미만이 11.4%, 50~

75%미만이 22.1%, 75~100%미만이 11.4%, 그리고 100%(모두 응답을 받음)가 10.7%로 나타났다. 문제를 제기하는 세 가지 방식 - 즉, 이메일, 전화, 게시판 - 가운데 상대적으로 가장 응답률이 높은 것은 게시판으로 나타났다. 이것은 기업들이 전화나 이메일과 같은 개별적인 문제제기에는 별로 신경을 쓰지 않지만 문제제기의 공론화가 가능한 게시판에 의한 문제제기에는 상대적으로 더 민감하게 반응하고 있음을 보여주는 것이다.

전화를 통해 문제를 제기한 경험이 있는 121명에게 질문한 결과는 한 번도 응답을 받지 못한 경우가 30.6%, 응답비율이 0~25%미만인 경우는 34.7%, 25~50%미만이 12.4%, 50~75%미만이 11.6%, 75~100%미만이 3.3%, 그리고 100%(모두 전화를 받음)가 7.4%로 나타났다. 이 수치는 이용자의 민원에 대한 응답률이 전화를 사용하는 경우 가장 저조했음을 보여준다.

<표 9> 개인정보 관리의 문제제기에 대한 응답률

응 답 률	e-mail	게시판	전화
0%	11.6%	15.0%	30.6%
0~25%미만	30.1%	29.3%	34.7%
25~50%미만	11.8%	11.4%	12.4%
50~75%미만	19.6%	22.1%	11.6%
75~100%미만	7.8%	11.4%	3.3%
100%	19.6%	10.7%	7.4%

문제를 제기하는 방식에 따라 조금 차이는 있었지만, 전반적으로 개인정보 관리 책임자들이 개인정보의 주체들이 제기하는 문제에 대해 무관심함을 알 수 있다. 앞에서 보았듯이, 개인정보 관리에 문제가 있을 때 정보 주체가 문제를 제기하는 비율도 높지 않았고 정보관리 책임자도 제기된 문제에 대해 무관심한 형태를 보여주어 양자 모두에게 문제가 있음이 확인되었다. 따라서 개인정보 주체의 보다 적극적인 문제제기와 정보관리 책임자의 보다 성의 있고 책

임 있는 태도가 요망된다.

개인정보 관련 불만이나 질문을 했을 때 답변이 얼마나 유용한 것이었나를 알기 위해 각각의 방식을 이용해 문제를 제기한 경험이 있는 이들을 대상으로 다시 기업이 회신한 내용에 대한 만족도를 질문하였다.

e-mail를 통해 제기한 경험이 있는 이용자중 16. 3%가 "전혀 도움이 되지 않았다"고 답했고, "별로 도움이 되지 않았다"고 답한 경우가 32.0%였다. "그저 그렇다"는 14.4%, "약간 도움이 됨"이 30.1%, "매우 도움이 됨"은 7.2%로 나타났다. 결과적으로 도움이 되지 않는 편(전혀 도움이 되지 않음+별로 도움이 되지 않음)이 48.3%로 도움이 되었다(약간 도움이 됨+매우 도움이 됨)고 답한 37.3%에 비해 더 많았다.

게시판을 이용한 경우에도 도움이 되지 않는 편이 52.8%인 반면, 도움이 되는 편은 32.2%로 나타나 역시 전체적으로는 도움이 되지 않는다는 응답이 훨씬 높게 나타났다.

전화를 이용하여 불만이나 질문을 한 적이 있는 이용자들의 경우도 마찬가지로 도움이 되지 않는 편이라고 응답한 경우가 65.3%로 도움이 되었다고 대답한 응답자 22.3%에 비해 압도적으로 많았다.

<표 10> 문제제기에 대한 응답의 효과

만 족 도	e-mail	게시판	전화
전혀 도움이 되지 않음	16.3%	20.7%	30.6%
별로 도움이 되지 않음	32.0%	32.1%	34.7%
그저 그렇다	14.4%	15.0%	12.4%
약간 도움이 됨	30.1%	27.9%	18.2%
매우 도움이 됨	7.2%	4.3%	4.1%

이러한 현상은 각 기업이 정보관리 책임부서를 선정하는 것에서도 나타나

는데, 상당수의 기업들이 정보관리 책임을 위한 독립부서를 두지 않고 있는 형편이다. 가령, 국민은행은 E개발팀, 우리카드는 상품개발팀, LG투자증권은 인터넷 개발팀, 인터파크는 종합연구소, 삼성몰은 기획팀 등이 개인정보관리 책임을 맡고 있어 개인정보 보호업무가 독자적으로 이루어지고 있는지 의심스러운 현실이다. 설문의 결과는 이러한 현실의 일면을 보여준다고 할 수 있다. 기업에 개인정보관리책임자를 두고 관련 업무를 하도록 되어 있지만 현실적으로 다분히 형식적인 관리에 그치고 있음을 알 수 있다.

Ⅳ. 기업의 고객 자기정보 통제권 보장 실태

「정보통신망이용촉진및정보보호등에관한법률 시행령」 제3조에서는 정보통신부 장관이 이용자의 「개인정보보호를 위한 지침」을 고시하고, 정보통신사업자 및 법에서 규정한 기타 사업자에게 이를 준수할 것을 권장할 수 있도록 하고 있다. 이에 따라 이 장에서는 이러한 규칙이 각 기업에 의해 어느 정도 지켜지는지를 검토해 보려고 한다.

이 검토에 있어 특히 관심을 두는 것은 각 기업의 인터넷 사이트에 나와 있는 개인정보보호 정책 및 회원가입시 동의를 구하는 약관을 통해 기업이 고객의 자기정보통제권을 어느 정도 보장하는가이다. 덧붙여 개인정보의 제3자 공유에 대한 자기정보 통제권도 조사의 대상으로 삼는다. 조사대상 기업은 총 70개였으나, 한국투자증권, 대신증권, 동양종합금융증권 등 3개사는 개인정보보호정책을 아예 게시하지 않는 등 사실상 조사가 불가능해, 67개만이 실제로 조사되었다.

조사 항목은 ① 약관 및 개인정보보호정책에 나타난 자기정보통제권 보장 실태에 관한 10개 주제 14개 항목 ② 회원가입 양식에 관한 3개 주제 7개 항목 ③ 제3자 공유실태에 관한 2개 주제 4개 항목으로 총 15개 주제 25개 항목으로 이루어져 있다.

조사대상 기업 중 한 곳을 제외하고 모두 개인정보보호정책을 온라인상에 게시하고 있었으나 각 기업이 제시하고 있는 개인정보보호 정책의 내용에 있어서는 큰 차이가 있었다. 개인정보보호 실태를 검토하는 순서는 먼저 약관 및 개인정보보호 정책에서 나타난 정보의 자기통제권을 살펴보고 이어서 회원가입 양식에 나타난 개인정보보호의 통제권을 살펴보기로 한다.

1. 약관 및 개인정보보호정책으로 본 자기정보통제권 보장 실태

기업의 약관 및 개인정보보호정책에 있어 정보주체의 통제권이 얼마나 보장되고 있는가를 보기 위해 “목적 명확화의 원칙”, “수집제한의 원칙”, “이용제한의 원칙”, “공개의 원칙”, “개인 참가의 원칙”, “책임의 원칙”이 제대로 지켜지고 있는가에 초점에 맞추어 검토해보기로 한다.

가. 목적 명확화의 원칙

목적 명확화의 원칙은 개인정보를 수집할 때는 목적이 명확해야 하고, 이를 이용할 경우에도 애초의 목적과 모순되지 않아야 한다는 것이다. 기본적으로 모든 사이트에서 회원 가입 등을 통해 개인정보를 수집하는 목적은 해당 사이트의 서비스를 원활하게 제공하기 위함이다. 그러나 “서비스 제공”이라는 추상적인 목적의 제시는 이용자 입장에서는 언제든지 회사의 자의적인 판단에 의해서 “서비스”가 규정되고 자신들의 개인정보가 이용될 수 있다는 의미로 받아들여 질 수밖에 없다. 따라서 수집하는 정보의 항목별로 구체적인 목적을 제시하는 것이 바람직하다.

1) 수집 정보의 구체적 항목과 수집목적의 명시 여부

전체 67개 조사 대상 중 구체적인 수집목적을 설명하되, 개별항목과 직결시켜 설명하지는 않는 곳이 25곳(37.3%)으로 가장 많았다.

예를 들면, “저희 ○○은행은 다음과 같은 목적을 위하여 개인정보를 수집하고 있습니다. △ 서비스 제공을 위한 계약의 성립 (본인식별 및 본인의사확인 등) △ 서비스의 이행 (금융거래, 인증서비스 관련 각종 공지 등) △ 기타 금융정보 제공 등. 개인정보의 수집범위는 고객님의 성명, 실명번호, 주소,

전화번호, e-mail 주소 등 상기 목적을 이행하기 위하여 필요한 항목으로 제한합니다"와 같은 경우이다.

반면에 "보다 나은 서비스를 제공하기 위하여"와 같이 추상적인 형태의 목적만을 제시하고 있는 곳이 22곳(32.8%)이었고, 개별 항목별로 수집정보의 구체적 항목과 수집목적을 설명하고 있는 곳은 19곳(28.4%)이었다. 아예 수집목적을 제시하지 않는 곳은 개인정보보호정책이 없는 1개사였다. 전체적으로 볼 때, 조사대상 기업의 2/3 이상이 개인정보 수집의 구체적인 목적을 명시하고 있지 않은 것으로 나타났다.

기업 분류별로는 쇼핑몰과 카드사가 비교적 수집목적을 명확하게 제시하는 편이었고, 언론사, 은행, 증권사는 개별항목별로 구체적인 수집 목적을 제시하는 곳이 한곳도 없었다.

<표 11> 수집하는 정보의 구체적 항목과 수집목적의 명시 여부

구 분	①	②	③	④	계
보험사	4	2	3	1	10
쇼핑몰	7	2	1		10
언론사		6	4		10
은 행		4	7		11
증권사		4	3		7
카드사	6	2	1		9
포 털	2	5	3		10
계	19 (28.4%)	25 (37.3%)	22 (32.8%)	1 (0.1%)	67

① 개별 항목별로 구체적인 수집 목적을 설명하고 있다.

② 구체적인 수집목적을 설명하되, 개별 항목과 직결시켜 설명하지는 않고 있다.

③ 추상적인 형태의 수집목적만을 제시하고 있다.

④ 제시하지 않고 있다.

나. 수집 제한의 원칙

개인정보를 수집할 때에는 반드시 필요한 범위 내에서 수집해야 하며 정보주체의 동의를 받아야 한다. 또한, 사상, 신념, 병력 등의 민감한 개인정보는 수집 자체가 제한되어야 한다. 개인정보 수집제한의 원칙을 적용함에 있어 중요한 논의의 대상이 되는 것은 14세 미만 아동에 대한 개인정보 수집의 경우이다. 정보통신부의 개인정보보호지침에 따르면, 아동의 개인정보 수집에 대한 부모 동의권을 명시하고 있다. 이것은 14세 미만의 아동의 경우 개인정보의 중요성에 대한 인식이 충분하지 않고, 정보에 대한 판단력이 부족한 상태에서 아동이 입력한 개인정보로 인해 불이익을 당할 우려가 있기 때문이다.

1) 아동 개인정보 수집시 부모 동의권 보장 여부

조사 결과 아동의 개인정보 수집에 대한 부모 동의권을 명시하지 않고 있는 곳은 총 11개 기업으로 전체의 16.4%였다. 부모의 동의권을 명시하거나, 아동의 개인정보를 수집하지 않음을 밝힌 곳은 각각 32개와 10개로 전체의 62.7%였으며, 기타가 4개로 6.0%였다.

<표 12> 아동의 개인정보 수집시 부모의 동의권 보장 여부

구 분	명시함	명시안함	수집하지 않음	기 타	계
보험사	7	1	1	1	10
쇼핑몰	3	1	6		10
언론사	9	1			10
은 행	2	6		3	11
증권사	4	3			7
카드사	4	1	4		9
포 탈	10				10
계	32 (47.8%)	11 (16.4%)	10 (14.9%)	4 (6.0%)	67

그런데, 몇몇 기업의 아동의 개인정보보호 방침에서는 해당 기업들이 원래 그 항목의 제정 목적을 잘못 이해하고 있다는 사실을 알 수 있었다. 부모의 동의권을 명시하지 않은 사이트 중 두 곳에서는 해당 웹 사이트에 아동이 유의해야 할 정보가 없으므로 부모의 동의가 필요없다고 밝히고 있으며, 기타로 분류된 은행 사이트에서는 아동의 정보를 게시하거나 제공하지 않음을 밝히고 있다. 다른 은행의 경우에는 권리를 부여하는 경우(환율 클럽 가입)에만 개인정보를 수집한다고 밝히고 있다. 아동의 개인정보 수집에 대한 부모의 동의권을 명시하는 것은 권리 행사 능력이 부족하다고 판단되는 나이인 아동의 개인정보를 특별히 보호하고자 하는 취지로 이해되어야 하기 때문에 위 사이트들과 같이 특정한 경우를 설정하여 부모의 동의를 받는 것은 이 정책의 취지에 적절하지 못하다고 할 수 있다.

다. 이용 제한의 원칙

이용 제한의 원칙은, 개인정보가 정보주체의 동의나 법률의 규정에 의하지 않고서는 명확한 목적 이외의 용도로 공개되거나 이용되어서는 안 됨을 의미한다. 일반적으로 인터넷 사이트에서의 개인정보 수집 목적은 “서비스를 제공”하기 위한 것이므로, 그 목적이 달성된 시점, 즉 회원이 탈퇴 혹은 동의 철회를 한 시점에는 해당 개인정보가 파기되어야한다. 그러나 많은 사이트에서 개인정보의 수집 목적을 모호하게 제시하고 있는 현실을 감안하면, 개인정보의 보유 및 이용기간이 명확하게 제시되지 않을 경우, 회원이 탈퇴 혹은 동의를 철회한 이후에도 회사의 자의적인 판단에 의해 개인정보가 계속해서 보유될 가능성을 배제할 수 없다. 따라서 개인정보의 보유 및 이용기간을 명시하는 것은 이용 제한의 원칙을 실현하는 구체적인 방법이 된다. 또한 약관 및 개인정보보호정책의 변경을 안내하고 변경된 약관과 정책에 대해 새로이 동의를 구하는 방식 역시 개인이 동의한 범위 안에서 개인정보가 이용되어야 한다는 원칙을 준수하고 있는지 확인할 수 있는 척도가 될 수 있다.

따라서 이용제한의 원칙이 지켜지는가를 검토하기 위해서는 “개인정보 보유연한에 대한 명시여부”와 “비회원 거래자의 개인정보 보유연한에 대한 명시여부”, “약관 및 개인정보보호 정책 변경시 안내 및 동의여부”를 살펴볼 필요가 있다.

1) 개인정보 보유 연한에 대한 명시 여부

「정보통신망이용촉진및정보보호등에관한법률」 제22조 및 동법 시행령 10조에서는 개인정보보유 기간 및 이용기간에 대해 이용자에게 고지하거나 정보통신서비스이용약관에 명시하여야 한다고 밝히고 있다.「개인정보보호지침」 제7조에서도 개인정보 보유·이용기간 및 법적 근거 등 보유이유를 서면 또는 홈페이지 등을 통하여 이용자에게 공개하도록 하고 있다. 이를 위반하였을 시에는 1천만원 이하의 과태료에 처할 수 있다.

조사 결과 67개 사이트중 95.5%의 사이트에서 개인정보의 보유기간을 제시하고 있으나 그 중 45개(전체의 67.5%)가 탈퇴하면 개인정보를 삭제하겠다는 식의 일반적 수준으로 보유기간을 제시하고 있었다. 각각의 항목별로 구체적인 보존 연한을 명시하고, 그 근거들을 구체적으로 제시한 곳은 보험사, 쇼핑몰, 카드사, 포털에서 14개 사이트가 있다. 이 기업들은 법적 분쟁이 일어날 소지가 많은 곳으로 소송 등에 대비해 탈퇴 후에도 수년간 보관해야 할 정보가 많이 있기 때문인 것으로 보인다. 구체적 설명이 없는 보험사 한곳과 은행 한곳은 개인정보보호정책이나 약관이 아예 없는 경우이다.

<구체적 보존 연한 명시의 예>*

○ 귀하의 개인정보는 다음과 같이 개인정보의 수집목적 또는 제공받은 목적이 달성되면 파기됩니다. 단, 상법 등 법령의 규정에 의하여 보존할 필요성이 있는 경우에는 예외로 합니다.
- 회원가입정보의 경우, 회원가입을 탈회하거나 회원에서 제명된 때
- 대금지급정보의 경우, 대금의결제 또는 채권소멸시효기간이 만료된 때
- 배송정보의 경우, 물품 또는 서비스가 인도되거나 제공된 때

○ 위 개인정보 수집목적 달성시 즉시 파기 원칙에도 불구하고 다음과 같이 거래 관련 권리의무 관계의 확인 등을 이유로 일정기간 보유하여야 할 필요가 있을 경우에는 미리 보유기간 및 이용기간을 명시하고 귀하의 동의를 받습니다

- 소송이나 분쟁에 있어 근거자료로 보존할 필요성이 있는 경우
  : 소송과 분쟁이 종료되는 시점까지
- 청약 및 승락에 관한 기록 : 3년
- 대금결제에 관한 문서 : 3년
- 청약의 철회등에 관한 문서 : 3년
- 기타 개별적으로 이용자의 동의를 받은 경우 : 동의를 득한 기간까지

* BC카드 개인정보보호정책 中 (http://www.bccard.co.kr)

<표 13> 개인정보의 보유기간 제시 여부

구 분	①	②	③	④	계
보험사	1	5	1	3	10
쇼핑몰		4	1	5	10
언론사		7	3		10
은 행	1	10			11
증권사		7			7
카드사		4		5	9
포 털	1	8		1	10
계	3 (4.5%)	45 (67.2%)	5 (7.5%)	14 (20.9%)	67

① 구체적 설명이 없다.

② 탈퇴하면 삭제한다 식의 일반적 수준으로만 제시되고 있다.

③ 각각의 항목별로 구체적인 보존 연한을 명시하고 있다.

④ 각각의 항목별로 구체적인 보존 연한을 명시하고 있고, 그 근거도 구체적으로 제시한다.

2) 비회원 거래자의 개인정보 보유 연한에 대한 명시 여부

사이트의 성격에 따라 비회원에게 개인정보를 요구하여 상거래가 일어나는 경우가 있는데 쇼핑몰 사이트가 대표적이다. 이런 경우 회원들의 개인정보 보유 연한 제시와는 별도로 비회원 거래자의 개인정보 보유 연한에 대한 제시가 필요하다. 총 67개 사이트 중 비회원 거래가 일어나는 곳은 쇼핑몰 9개, 포털

4개 사이트가 있었다. 이 중 비회원 거래자의 개인정보 보존 연한을 제시하고 있는 곳은 단 한 곳도 없었다. 결국, 비회원의 개인정보는 아무런 보호의 규칙도 설정되어 있지 못한 상태이다.

3) 약관 및 개인정보보호 정책 변경시 안내 및 동의 방식

약관 및 개인정보보호정책이 최초 이용자가 동의한 내용에서 변경될 경우에는 서비스 제공자는 이에 대해 이용자들에게 고지하고 변경된 사항에 대해 동의를 구해야하는 책임이 있다. 특히 약관의 변경 내용이 이용자에게 불리한 경우에는 보다 적극적인 방식으로 동의를 구하는 것이 바람직하다.

조사결과 약관 및 개인정보보호정책의 변경시 안내하는 방법은 홈페이지 게시가 59.7%로 가장 많았고, 홈페이지 게시와 더불어 e-mail, 우편, 영업장 게시 등의 기타 방법을 병행하는 곳이 38.8%였다. 그러나 약관이나 정책의 변경에 대한 개인정보 주체의 동의는 필수적으로 요청되는 만큼 보다 적극적인 방식으로 변경내용을 공지하도록 할 필요가 있다.

<표 14> 약관 및 개인정보보호정책 변경시 안내 방식

구 분	홈페이지 안내	기타방식 병행	안내없음	계
보험사	8	1	1	10
쇼핑몰	9	1		10
언론사	2	8		10
은 행	3	8		11
증권사	1	6		7
카드사	7	2		9
포 탈	10			10
계	40 (59.7%)	26 (38.8%)	1 (1.5%)	67

약관 및 정책의 변경에 대한 고지 방식에 대한 안내는 비교적 잘 나와 있는 반면, 약관 및 정책 변경시 동의를 구하는 방식에 대한 안내를 하지 않는 곳

이 14.9%로 상대적으로 미흡함을 알 수 있다. 약관 및 정책의 변경시 동의 방식을 안내한 85.1%는 모두 일정기간 안내 후 회원이 탈퇴하지 않을 경우 약관에 동의한 것으로 간주한다는 소극적 동의 방식을 채택하고 있었다. 약관 및 정책의 일부 변경에 대하여 모든 이용자들의 적극적인 동의를 받는다는 것이 현실적으로 불가능하다고 하더라도, 변경 내용이 이용자에게 불리하고 중대한 내용일 경우 적극적인 동의를 받는 것이 보다 바람직할 것으로 보인다.

<표 15> 약관 및 개인정보보호정책 변경시 동의 방식

구 분	안내 없음	미탈퇴시 동의한 것으로 간주	계
보험사	2	8	10
쇼핑몰	1	9	10
언론사	1	9	10
은 행	1	10	11
증권사	3	4	7
카드사		9	9
포 털	2	8	10
계	10 (14.9%)	57 (85.1%)	67

라. 공개의 원칙

「개인정보보호지침」 제7조에서는 인터넷 홈페이지 접속파일(쿠키)의 운영에 관한 사항 및 개인정보보호를 위한 기술적·관리적 대책에 관한 사항을 개인정보보호정책에 포함시키고 공개하여야 한다고 규정하고 있다.

서비스 제공자들은 개인정보에 관한 개발, 운용 및 정책에 관해서는 일반적으로 공개정책을 취하여야 한다. 각 사이트 별로 개인정보보호정책을 첫 화면에 링크하여 게시하는 것도 이러한 이유 때문이다. 기업의 개인정보 취급에 관한 사항을 공개하는 것 중 최근 들어 더욱 중요하게 인식되고 있는 것이 쿠키 운용과 기술적 대책에 관한 사항들이다. 개인정보가 각종 마케팅에 이용되면서, 개인정보를 해킹하는 사례가 빈번히 일어나고 있으므로 서비스 제공자

들은 이용자들이 자신들의 정보가 얼마나 안전하게 보관되는지 알 수 있도록 충분히 공개해야할 책임이 있다.

1) 기술적 대책의 구체적 제시 여부

개인정보 보호를 위한 기술적 대책을 비교적 구체적으로 제시하고 있는 곳은 총 49개로 73.1%였다. 그러나 기술적 대책을 전혀 제시하지 않거나(9개), 제시하더라도 "보안을 위해 최선을 다 하겠다"는 식의 추상적 기술에 그친 곳(9개)이 26.8%였다. 해당 시스템의 구체적인 사양까지 밝히는 것은 오히려 해킹의 근거가 될 수도 있다는 점에서 반드시 바람직하다고 볼 수는 없지만, 최소한 이용자들이 자신의 정보가 어떠한 방식으로 보호되고 있는지 정도는 알 수 있어야 하는 것이 공개의 원칙에 부합한다고 할 수 있다.

<표 16> 기술적 대책의 구체적 제시 여부

구 분	①	②	③	계
보험사	1		9	10
쇼핑몰			10	10
언론사	1	3	6	10
은 행	5	1	5	11
증권사	1	1	5	7
카드사	1		8	10
포 탈		4	6	10
계	9 (13.4%)	9 (13.4%)	49 (73.1%)	67

① 정책이 없다.

② 추상적인 내용이 제시되고 있다.

③ 어떠한 방식을 사용하는지 정도의 비교적 구체적인 내용이 제시되어 있다.

④ 해당 시스템마다 회사, 기종, 모델명 등 매우 자세하게 설명하고 있다.

2) 쿠키 운용에 관한 정책 명시 여부

이용자가 사용한 컴퓨터에 남아있는 쿠키를 통해 특별히 해킹을 하지 않아도 이용자의 아이디, 비밀번호 등 기본적인 정보를 알아낼 수 있다는 점에서 쿠키 운용에 관한 충분한 설명은 이용자에게 매우 중요한 정보가 된다.

쿠키 거부방안을 제시하고, 쿠키가 개인 식별정보와 통합되어 사용되지 않음을 밝히고 있는 곳이 34곳(50.7%)으로 가장 많았고, 설명과 거부방안만을 제시한 곳이 19곳(28.4%)으로 나타났다. 그런 점에서 전체적으로 쿠키에 대해 비교적 상세한 설명을 하는 것으로 볼 수 있다. 그러나 쿠키 운용에 관한 정책이 전혀 없는 곳(6개)과 설명이 있어도 추상적인 기술에 그친 곳(5개)도 16.5%를 차지했고, 쿠키에 대해 상세한 설명을 한 곳은 포털사이트 한 기업에 불과했다.

<표 17> 쿠키 운용에 관한 정책 명시 여부

구 분	①	②	③	④	④⑤	⑥	계
보험사	1			1	6	2	10
쇼핑몰	1	1		3	5		10
언론사		2		4	4		10
은 행	2			6	3		11
증권사	1			1	5		7
카드사					9		9
포 털	1	2	1	4	2		10
계	6 (9.0%)	5 (7.5%)	1 (1.5%)	19 (28.4%)	34 (50.7%)	2 (3.0%)	67

① 정책이 없다.

② 정책이 존재하지만, 추상적 설명에 그치고 있다.

③ 쿠키에 담기는 정보의 내용을 상세히 소개하고 있다.

④ 쿠키에 담기는 정보의 내용을 소개할 뿐 아니라, 쿠키 거부 방안을 제시하고 있다.

⑤ 개인식별정보와 통합하여 사용되지 않음을 밝히고 있다.

⑥ 기타 (Session 방식 - 쿠키 저장 없음)

조사 항목에는 포함되어 있지 않았지만, 쿠키에 대한 정책에 쿠키가 어떠한 식으로 악용될 수 있는지에 대해 언급하고 이용자의 경각심을 일깨우는 곳은 한 곳도 없었다. 또한 쿠키 거부 방안을 제시하고 있는 곳에서도, 쿠키를 거부할 경우 서비스를 정상적으로 이용하지 못할 수 있다는 경고만을 제시함으로써, 당연히 쿠키를 받아들여야만 하는 것으로 인식하게 하는 측면이 있었다.

마. 개인 참가의 원칙

개인정보의 주체는 자신과 관련된 정보에 대한 존재확인, 열람요구, 이의제기 및 정정·삭제·보완 청구권을 가진다. 이는 비록 동의에 의해 기업에 개인정보를 제공했다 할지라도 그 정보의 주인은 자기 자신이라는 의미이다. 「개인정보보호지침」 제20조와 제21조에서는 이용자의 권리로서 동의 철회권과, 개인정보의 열람 및 정정 요구권을 명시하고 있다.

1) 열람, 정정, 삭제권에 대한 명시 여부

조사 대상 67개 사이트 중 개인정보보호 정책이 없는 보험사 1개사를 제외하고 모든 사이트가 개인정보의 열람, 정정, 삭제권을 보장하고 있는 만큼 이 원칙은 충실히 지켜지고 있는 것으로 평가된다.

바. 책임의 원칙

개인정보관리의 책임에 관한 원칙이 지켜지는가는 “개인정보 관리 책임자의 지정여부”와 “개인정보 관리책임자를 접촉하기 위해 필요한 정보의 공개여부”로 나누어 검토해 볼 수 있다.

1) 개인정보 관리책임자 지정 여부

「정보통신망이용및개인정보보호등에관한법률」 제27조와 「개인정보보호지침」 제15조에서는 정보통신서비스제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 불만을 처리하기 위하여 개인정보관리책임자를 지정하여야 한다고 규정하고 있다. 또한 지침 제15조에서는 개인정보관리책임자는 서비스제공자 등의 임원 또는 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장의 지위에 있는 자 또는 개인정보 취급 부서의 장이어야 한다고 규정하고 있다. 개인정보관리책임자를 지정하지 아니한 자에 대해서는 「정보통신망법」제67조 제8호에 의거 500만원 이하의 과태료에 처할 수 있다.

조사 대상 67개 기업 중 3곳을 제외한 64개(95.5%) 기업이 개인정보 관리책임자를 지정하고 있었다. 그러나 지침에서 규정하고 있는 임원 또는 부서장급에 못 미치는 개인정보관리 책임자를 지정하고 있는 곳이 9개(13.4%) 사이트나 됐다.

<표 18> 개인정보 관리 책임자 지정 여부

구 분	지정한다	지정하지 않는다	계
보험사	9	1	10
쇼핑몰	10		10
언론사	10		10
은 행	10	1	11
증권사	6	1	7
카드사	9		9
포 탈	10		10
계	64 (95.5%)	3 (4.5%)	67

2) 개인정보 관리 책임자의 정보공개 여부

「정보통신망이용및개인정보보호등에관한법률」 제22조와 「개인정보보호지침」 제6조에서는 서비스 제공자는 개인정보관리책임자를 지정하고 성명, 소속 부서, 지위, 전화번호, 전자우편주소, 기타 연락처를 이용자에게 미리 고지하여야 한다고 규정하고 있다.

조사 대상 중 개인정보 관리 책임자의 정보 중 성명, 직위, 전화, e-mail 등을 모두 고지하는 곳이 51개(76.1%)로 가장 많았다. 또 금융기관 1개사를 제외하고는 개인정보관리책임자를 정하고 있는 모든 사이트에서 연락할 수 있는 전화, e-mail 등의 연락처 정보를 고지하고 있었다.

그러나 많은 경우에 개인정보 관리 책임자의 연락 전화번호로 공개된 전화번호가 고객센터의 전화번호이거나 대표 전화번호였기 때문에 개인정보관리책임자와 직접 통화하는 것이 어려운 경우가 많았다. 또한 고객센터에 개인정보관리책임자와의 통화를 요구했을 때 책임자가 누구인지 모르는 경우도 다수였다. 심지어 모 증권사의 경우 개인정보보호정책에 게시된 책임자와 통화를 요구하자, "단지 명목상 올려놓은 것일 뿐"이라는 답변을 하기도 했다. 고객센터로 통화가 되는 경우, 전화번호 안내나 직접 통화는 불가능하고 메모를 전달해 전화를 주겠다는 답변을 듣는 경우가 많았는데, 그 중 다수가 결국 연락이 되지 않았다. 그리고 모 은행의 경우에는 정책에 안내되어 있는 전화번호가 전혀 엉뚱한 곳인 경우도 있었다. 정책 및 약관에 대한 확인이 불가능하여 조사 대상 목록에서는 빠졌으나 모 보험사의 경우 개인정보관리책임자가 바쁘다며 통화를 끊어버리는 사례도 있었다. 관리책임자가 바뀌었음에도 이전 관리책임자가 그대로 게시되어 있는 경우도 있었다.

3) 보험 가입 여부

「전자상거래등에서의소비자보호에관한법률」 제24조에서는 공정거래위원회가

전자상거래 또는 통신판매에서의 소비자 보호를 위하여 관련 사업자에게 소비자피해보상보험계약등을 체결하도록 권장할 수 있도록 하고 있다.[34] 개인정보의 보호에 대한 책임을 높이는 방안으로 서비스 제공자가 이용자의 개인정보 유출에 따른 피해에 대한 손해배상보험에 가입하는 것은 한 가지 좋은 예가 될 수 있다. 보험사 중 2개, 쇼핑몰 중 3개, 은행 중 2개, 증권사 중 1개 사이트가 보험에 가입되어 있다고 밝혔으며, 나머지는 가입되어 있지 않거나 확인 불가능한 경우였다.

2. 회원가입 양식을 통해 살펴본 자기정보통제권 보장 여부

회원제로 운영되는 대부분의 사이트들은 회원가입 시 이용자의 개인정보를 수집하게 된다. 서비스를 이용하기 위해서는 이용자가 어쩔 수 없이 입력해야 하는 개인정보들이 과연 적절한 것인지 각 사이트별 회원가입양식을 통해 조사하였다. 이 조사를 위해서는 앞에서와 마찬가지로 “목적명확화의 원칙”, “수집제한의 원칙”, 그리고 “이용제한의 원칙”을 검토해 보았다.

가. 목적 명확화의 원칙

정보수집 목적의 명확화를 검토하기 위해서는 “실명 확인의 적절성 여부”와 “개인 연락처 정보수집의 적절성 여부”를 조사할 필요가 있다.

---

34) 「전자상거래등에서의소비자보호에관한법률」 제24조 (소비자피해보상보험계약등)
①공정거래위원회는 전자상거래 또는 통신판매에서의 소비자 보호를 위하여 관련 사업자에게 다음 각호의 1에 해당하는 계약(이하 "소비자피해보상보험계약등"이라 한다)을 체결하도록 권장할 수 있다. 다만, 제8조제4항의 규정에 의한 전자결제수단의 발행자는 소비자피해보상보험계약등을 체결하여야 한다.
1. 보험업법에 의한 보험계약
2. 소비자피해보상금의 지급을 확보하기 위한 금융기관과의 채무지급보증계약

1) 인터넷 실명확인의 적절성 여부

조사대상 중 인터넷 실명확인제를 실시하는 곳이 46개로 68.7%였으며 실시하지 않는 곳이 31.3%였다. 실명확인제를 실시하는 곳 중 보험사 한 곳만이 주민등록번호 알고리즘 검사 방식을 택하고 있었고, 나머지 45개 사이트에서는 한국신용평가 혹은 정보통신산업협회 등 외부 기관의 데이터베이스를 사용하여 실명확인을 하고 있는 것으로 나타났다. 주민등록 번호와 실명을 통한 인터넷 실명확인제를 실시하지 않는 곳 중 은행, 카드사 등은 오프라인 상에서 실명확인을 통해 아이디를 등록하는 방식이거나, 소유카드 정보를 이용한 실명확인 방식을 택하고 있었다. 제공하는 서비스에 약간의 차이는 있을 수 있겠으나, 사이트 유형별로 봤을 때 실시하는 곳과 실시하지 않는 곳이 모두 존재하기 때문에 과연 실명확인이 반드시 필요한 절차인지는 의문이다. 결국, 실명확인의 목적성이 불분명한 가운데 주민등록번호 등 실명확인을 위한 정보가 과다수집 및 축적되고 있는 것을 알 수 있다.

<표 19> 인터넷 실명 확인제 실시 여부

구 분	실시한다	실시하지 않는다	계
보험사	8	2	10
쇼핑몰	8	2	10
언론사	9	1	10
은 행	4	7	11
증권사		7	7
카드사	7	2	9
포 털	10		10
계	46 (68.7%)	21 (31.3%)	67

<표 20> 실명확인 방식

구 분	외부기관 DB이용	알고리즘 확인	계
보험사	7	1	8
쇼핑몰	8		8
언론사	9		9
은 행	4		4
증권사			
카드사	7		7
포 털	10		10
계	45 (97.8%)	1 (2.2%)	46

2) 개인 연락처 정보 수집의 적절성 여부

각 사이트에서 회원가입 시 필수적으로 수집하고 있는 연락처 정보는 대체로 2~3개가량으로 주소, e-mail, 전화를 필수적으로 수집하는 경우가 많았고, 휴대폰은 선택사항인 경우가 많았다. 그러나 문제는 이러한 연락처 정보들을 왜 수집해야 하는지 그 목적이 불분명하다는 것이다. 연락처 정보 각각의 수집의 목적을 제시하지 않고 있는 곳이 56.7%로 가장 많았고, 회원가입 양식에서 연락처의 수집 목적을 구체적으로 밝힌 곳은 6개(9.0%)에 불과했다. 개인정보보호정책이나 약관에서 수집목적을 제시한 것으로 대신하는 곳이 26.9%였다.

<표 21> 연락처 정보 중 필수적으로 수집하고 있는 정보

구 분	주소		e-mail		전화		휴대폰	
	수집함	수집안함	수집함	수집안함	수집함	수집안함	수집함	수집안함
보험사	8	2	10		9	1	4	6
쇼핑몰	10		10		9(1)		2(1)	7
언론사	10		10		8(2)		1(2)	7
은 행	6	5	5	6	5	6	1	10
증권사	6	1	5	2	5(1)	1	1(1)	5
카드사	9		8	1	7(2)		2(2)	5
포 털	8	2	7	3	5(2)	3	2(2)	6
계	57	10	55	12	48(8)	11	13(8)	46

* 괄호 안의 숫자는 전화, 휴대폰 중에 하나를 선택할 수 있는 곳

<표 22> 연락처 정보 수집시 목적 제시 여부

구 분	①	②	③	④	계
보험사	5	3	2		10
쇼핑몰	3	7			10
언론사	9		1		10
은 행	6			5	11
증권사	7				7
카드사	3	6			9
포 탈	5	2	3		10
계	38 (56.7%)	18 (26.9%)	6 (9.0%)	5 (7.5%)	67

① 제시하고 있지 않다.

② 개인정보보호정책(약관)에서 포괄적으로 제시하고 있다.

③ 실제 수집단계에서 구체적 목적을 제시하고 있다.

④ 수집하지 않는다.

나. 수집 제한의 원칙

개인정보 수집제한의 원칙에 있어서는 가장 큰 논란거리가 되고 있는 것은 주민등록번호의 수집문제이다.

1) 주민등록번호 수집 및 관리의 적절성 여부

우리나라의 주민등록번호는 거의 모든 개인정보의 기본이 되는 개인 식별번호로, 개인의 자기정보통제권을 위협하는 가장 큰 요인으로 지적되고 있다. 조사결과 거의 모든 사이트(92.5%)에서 회원가입시 주민등록번호 입력을 요구하고 있었는데, 과연 이것이 적절한 것인지는 의문의 여지가 있다. 주민등록 번호를 수집해야 하는 경우는 반드시 개인의 실명을 확인할 필요가 있는 경우인데, 이 경우에도 주민등록번호가 아닌 다른 방식으로 개인을 식별할 수 있는 방법(예컨대 은행의 계좌번호, 신용카드 등을 통한 확인 방식)이 있다면, 굳이 주민등록번호를 요구할 필요는 없다.

<표 23> 주민등록번호를 수집하는 경우

구 분	회원가입시	필요한 서비스를 이용할 때	수집하지 않는다	계
보험사	10			10
쇼핑몰	10			10
언론사	10			10
은 행	8		3	11
증권사	6		1	7
카드사	9			9
포 털	9	1		10
계	62 (92.5%)	1 (1.5%)	4 (6.0%)	67

또한 해당 은행의 계좌가 없는 이용자가 웹 사이트를 이용하기 위한 준회원으로 가입할 경우 실제 반드시 주민등록번호를 통해 개인을 확인해야 하는 서비스가 없음에도 불구하고 모두 주민등록번호를 수집하는 것은 그것이 일종의 관례화되었기 때문으로 보인다. 예컨대 카드사의 경우 준회원으로 가입함으로써 이용할 수 있는 서비스는 지극히 제한되어 있고, 비회원과 큰 차이점이 없

으며 금융거래를 할 수 있는 권리도 없는 상태이다. 따라서 반드시 개인을 식별해야만 하는 경우, 예컨대 카드 발급 신청과 같은 경우에 국한해서 실명확인을 거치는 방식도 생각할 수 있다. 현재 대부분의 사이트에서는 무조건 회원가입시 주민등록번호를 요구하는 것은 불필요한 정보의 과도한 수집이다. 따라서 주민등록번호의 수집을 제한하고, 대체방안을 적극 모색할 필요가 있다. 앞 장의 검토에서도 나타났듯이, 개인들이 회원정보를 입력할 때 정보유출의 위험성에 대해 가장 민감하게 받아들이는 요소가 주민등록번호라는 점에서 더욱 그러하다.

다. 이용 제한의 원칙

개인정보는 수집된 목적 이외의 용도로 사용되어서는 안 되는데, 최근 들어 크게 문제가 되는 것은 개인정보가 이용제한의 범위를 넘어 유출됨으로써 광고성의 스팸메일이 무차별적으로 범람하고 있는 현상이다.

1) 광고성 메일 등의 수신에 대한 동의 절차 여부

<표 24> 광고성 메일/우편물 수신에 대한 동의 절차 여부

구 분	①	②	③	④	⑤	계
보험사	3	2	4	1		10
쇼핑몰	8	2				10
언론사	4	6				10
은 행	4	1	1		5	11
증권사	2	1		4		7
카드사	5	2		2		9
포 털	3	4	3			10
계	29 (43.3%)	18 (26.9%)	8 (11.9%)	7 (10.4%)	5 (7.5%)	67

① (별도의 동의절차를 마련하고 있으나) 모든 우편물에 대해 하나의 동의를 받고 있다.
② 우편물의 종류에 따라 개별적 동의를 받고 있다.
③ 약관에 대한 동의로 대체된다.
④ 안내가 없다.
⑤ 해당사항 없다.

회원 가입시 기입하게 되는 e-mail등 연락처를 통한 광고를 전송하는 것에 대해 별도의 동의절차를 마련하고 우편물의 종류에 따라 개별적 동의를 받고 있는 곳은 전체의 26.9%였다. 별도의 동의절차를 마련하고 있으나, 모든 우편물에 대해 하나의 동의를 받고 있는 곳이 43.3%로 가장 많았다.

3. 개인정보 제3자 공유의 자기정보 통제권 보장 실태

개인정보의 제3자 공유에 관한 사실은 개인정보보호정책 내용 중 이용자가 가장 관심을 갖게 되는 부분이다. 매일 수십, 수백 통 씩 날아오는 엄청난 양의 스팸 메일에 시달리고 전화나 핸드폰으로 이름까지 정확히 알고는 걸려오는 광고전화를 수시로 받는 사람들에게는 과연 나의 정보가 어떻게 누구와 얼마만큼 공유되는지는 매우 중요한 사실이다.

『정보통신망법』 제24조 및 『개인정보보호지침』 제9조에서는 서비스 제공자 등은 이용자의 개인정보를 제공받은 자는 당해 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이를 이용하거나 제3자에게 제공하여서는 안된다고 규정하고 있다. 이에 대해 위반하였을 시에는 『정보통신망법』 제62조에 의하여 5년이하의 징역 또는 5천만원 이하의 벌금에 처한다.

대부분의 사이트들에서는 위의 법률과 지침에 근거하여 원칙적으로 이용자의 개인정보를 제3자와 공유하지 않음을 밝히고 있으나, 정보 주체의 동의가 있는 경우 혹은 법률에 근거가 있는 경우 제한적으로 제3자와 공유될 수 있음

을 밝히고 있다. 그런데, 많은 경우 과연 제한적 이용이라는 것이 과연 어디까지인지 알 수 없다는 점이 문제이며, 수집 목적으로 제시된 "보다 나은 서비스 제공"을 위한 정보 공유라는 모호한 표현은 무제한적으로 제3자와 정보를 공유할 수 있다는 것과 크게 다르지 않다. 이러한 경우 이용자는 자신의 개인정보가 어떻게 공유되는지 전혀 알 수 없는 반면 서비스 제공자는 법적 고지의 의무를 다하였기 때문에 책임이 없다고 할 수 있는 문제가 생긴다. 그리고 한편으로는 내가 정보공유에 동의한다는 것이 과연 어떤 절차를 거쳐 이루어지는 것인지 알 수 없는 것 또한 문제이다. 약관에 동의하면 그것으로서 나의 개인정보가 공유될 수 있는 것인지, 아니면 추후 별도의 고지를 통해서 선택권이 부여되는 것인지 명확하게 알 수 없는 것이다.

개인정보의 제3자 공유에 대한 개인정보 주체의 자기통제권은 "개인정보 공유대상의 구체적 명시여부", "개인정보 공유에 대한 동의권의 보장정도", 그리고 "영업의 양수양도시 안내 및 동의방식"을 검토함으로써 실태를 파악할 수 있을 것이다.

가. 공유 대상의 구체적 명시 여부

<표 25> 현재 개인정보 공유대상 기업의 구체적 명시 여부

구 분	①	②	③	④	⑤	계
보험사				8	2	10
쇼핑몰		1	3		6	10
언론사	1		2	6	1	10
은 행			2		9	11
증권사				2	5	7
카드사	1		1	2	5	9
포 털	1			5	4	10
계	3 (4.5%)	1 (1.5%)	8 (11.9%)	23 (34.3%)	32 (47.8%)	67

① 공유 대상 기업의 명칭과 제공목적, 제공항목을 구체적으로 명시

② 공유 대상 기업의 명칭과 제공항목만을 구체적으로 명시

③ 공유 대상 기업의 명칭만을 구체적으로 명시
④ 공유 대상과 목적을 모두 추상적으로 표현
⑤ 공유 여부를 명확히 할 수 없음

조사에서, 이용자의 개인정보가 제3자와 공유될 수 있다는 사실을 명시하고 최소한 현재 공유 대상의 기업 명칭을 고지하는 곳은 12개로 전체의 17.9%에 불과했다. 공유대상과 목적을 모두 추상적으로 표현한 곳이 34.3%, 현재 개인정보가 공유되고 있는지 없는지 명확히 알 수 없는 곳이 47.8%였다. 개인정보 공유 현황을 명확히 밝히지 않은 47.8% 중에는 실제 개인정보를 공유하지 않는 경우도 다수 있을 수 있으나, 그런 경우에는 현재 공유되는 기업이 없음을 명확하게 밝히는 것이 바람직하다.

나. 공유에 대한 동의권의 보장정도

「개인정보보호지침」 제9조에서 의미하는 "이용자의 동의"는 서비스 제공자가 이용자에게 반드시 사전에 해당 이용자에게 개별적으로 서면, 전자우편, 전화 등에 의해 필요한 사항을 고지하고 명시적인 동의를 받아야 한다는 것이다. 또한 개별적으로 동의를 받아야 한다는 것은 이용자 개개인의 동의 여부를 확인해야 한다는 것으로 일괄적으로 전체 이용자에게 공유사실을 고지한 후 거부의사가 없는 경우 동의로 간주하는 것은 개별적 동의로 볼 수 없다.[35]

조사 결과 개인정보 공유에 대한 동의 절차를 명확히 안내하지 않고 있는 곳이 41.8%였고, 공유 대상 기업 각각에 대해 따로 동의절차를 마련하는 곳은 전혀 없었다. 다만, 카드사의 경우 제휴카드를 발급하는 경우가 있는데 이 경우에는 제휴사와 공유하는 정보에 대해 개별적으로 동의를 받는다. 이 경우가 개별적이고 명시적인 동의의 전형적인 예라고 할 수 있을 것이다. 그러나 다른 일반적인 경우에 대해서는 개인정보의 제3자 공유 문제가 매우 중요한 것

35) 정보통신부, 『개인정보보호지침 해설서』, 2002.4., pp. 53-54.

임에도 불구하고, 대부분의 사이트에서 매우 추상적으로 기술하고 있기 때문에, 이용자 입장에서는 만족할 만한 정보를 얻을 수 없다는 것이 문제이다. 예를 들어, "원칙적으로 동의 없이 개인정보를 공유하지 않는다. 그러나 동의를 받으면 공유**할 수 있다**"라는 모호한 표현은 비록 법적으로는 문제가 없으나, 한 개인이 약관 동의버튼을 클릭을 하는 순간 그의 정보가 공유될 수 있다는 것인지, 아니면 추후에 동의를 받고 공유할 수 있다는 것인지 판단할 수 없게 만든다. 따라서 서비스 제공자는 현재 개인정보를 공유하는 대상을 명확히 표시하고, 이용자가 각각의 기업에 대해 정보공유를 선별적으로 동의를 할 수 있도록 하는 것이 바람직하다.

<표 26> 현재 공유하는 개인정보에 대한 동의 절차 분리 여부

구 분	①	②	③	④	계
보험사			10		10
쇼핑몰		3	3	4	10
언론사			9	1	10
은 행			1	10	11
증권사			3	4	7
카드사			4	5	9
포 털			6	4	10
계	0 (0.0%)	3 (4.5%)	36 (53.7%)	28 (41.8%)	67

① 공유 대상 기업 각각에 대해 따로 동의 절차를 마련한다.

② 공유 대상 기업에 대한 동의 절차가 따로 마련되어있으나, 전체 공유 대상 기업에 대해 한꺼번에 동의하도록 한다.

③ 약관에 대한 동의로 대체된다.

④ 명확한 안내가 없다.

다. 영업의 양수양도에 따른 안내 및 동의 방식

개인정보 공유와 개인의 정보통제권 확보에 있어 또 하나의 중요한 문제는

한 기업이 영업을 다른 기업에 양도하는 경우에 발생한다. 「정보통신망이용촉진및정보보호등에관한법률 시행령」 제11조에서는 영업의 양수, 양도시에 서비스제공자는 이 사실을 홈페이지에 최소 30일 이상 게시하거나 기타의 방법으로 개별적으로 통지하는 등 이용자에게 충분히 고지하여야 한다고 규정하고 있다.[36] 영업의 양수, 양도가 일어날 경우, 정보 수집/관리의 주체가 바뀐 것으로 이용자가 이전에 동의한 것은 더 이상 유효하지 않다. 따라서 이용자에게 이 사실을 고지하고 새롭게 개인정보 사용에 대한 동의를 받아야만 한다. 그러나 조사 결과 영업의 양수, 양도 시에 어떠한 방식으로 안내할 것인지 명시하지 않은 곳이 무려 85.1%이었으며, 양수, 양도시에 동의를 받을 것을 명시하지 않은 곳도 83.6%였다. 또한 홈페이지를 통한 고지의 경우 정보통신망법과 개인정보보호지침에서는 30일 이상의 고지기간을 명시하고 있으나 일주일 혹은 열흘 간 고지하겠다고 밝히는 곳도 있었다.

<표 27> 영업의 양수 양도시 안내방식

구 분	홈페이지/e-mail	홈페이지/e-mail 기타방식병행	안내없음	계
사	2	1	7	10
쇼핑몰	4		6	10
언론사			10	10
은 행			11	11
증권사			7	7
카드사	3		6	9
포 털			10	10
계	9 (13.4%)	1 (1.5%)	57 (85.1%)	67

36) 제11조 (영업의 양수 등의 통지) ①법 제26조제1항의 규정에 의하여 정보통신서비스제공자와 그로부터 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스제공자등"이라 한다)가 권리·의무를 이전하는 경우 그 사실을 통지하는 방법은 다음 각호와 같다.
1. 인터넷홈페이지에 최소 30일 이상 게시
2. 서면·전자우편 그 밖의 방법으로 이용자에게 통지

또한 영업의 양수양도 시의 동의를 얻는 방식에 대해서는 탈퇴를 하지 않은 사람을 모두 동의한 것으로 간주하는 옵트-아웃 방식의 동의를 받는 곳이 7곳(10.4%), 명시적인 옵트-인 방식의 동의를 받겠다고 명시한 곳은 3곳(4.5%)이었으며, 추상적으로 동의를 받는다고만 서술한 곳이 1곳 있었다.

<표 28> 영업의 양수 양도시 동의 방식

구 분	①	②	③	④	계
보험사	6	4			10
쇼핑몰	6	2	2		10
언론사	10				10
은 행	11				11
증권사	7				7
카드사	6	1	1	1	9
포 털	10				10
계	56 (83.6%)	7 (10.4%)	3 (4.5%)	1 (1.5%)	67

① 안내 절차 없음

② 일정기간 안내 후 탈퇴하지 않은 사람을 모두 동의한 것으로 간주한다.

③ 일정기간 안내 후, 명시적으로 동의한다고 밝힌 사람들을 제외하고 그 외의 사람들의 정보는 폐기한다.

④ 추상적으로 동의를 받겠다고만 나와 있다.

Ⅴ. 개인정보 보호를 위한 관리적·기술적 대책 실태

개인정보 보호를 위한 OECD 가이드라인의 8원칙에는 안전성 확보의 원칙이 포함된다. 개인정보의 수집자는 개인정보의 분실, 불법적인 접근, 파괴, 사용, 수정, 공개위험에 대비하여 합리적인 안전보호 장치를 마련해야 한다는 원칙이다. 이는 다시 관리적 대책과 기술적 대책을 마련하는 것으로 구분된다.

1. 개인정보 보호의 관리적·기술적 대책 개요

가. 금융 정보화 개요

국내 은행권은 1970년부터 본격적으로 전산화가 시작되었다. 은행내부 업무의 전산화(내부 네트워크화)가 진전되고 IT기술의 발전에 따라 보다 넓은 네트워크가 가능하게 되었다. 이러한 배경속에서 1986년 금융결제원이 설립되었다. 금융결제원 역할은 개별 은행 간의 안정적인 네트워크를 구축하는 것이었다. 많은 은행들이 참가하면서부터 은행과 은행사이의 전산망이 설치되었다.[37] 전자화된 네트워킹은 특정 점포에서만 거래가 일어나는 기존의 상식을 바꾸었다. IT기술의 발전은 2003년 현재, 언제 어디서나 금융서비스를 이용할 수 있는 촘촘하고 광범위한 네트워크를 실현하고 있다.

금융정보화추진위원회[38]는 금융정보화 과정을 크게 4단계[39]로 구분하고 있

37) 금융결제원, 『금융결제원 연차보고서』, 2003. 6, p. 9.

38) 금융전산망추진위원회는 1988년 금융전산망 기본계획을 심의하기 시작하며 1996년 6월까지 존속하였고 이후 정보화촉진기본법에 의한 정보화추진위원회의 분과로 1996년 7월부터 현재에 금융정보화추진분과위원회가 존속하고 있다.

39) 금융정보화의 단계를 나누는 것은 정립된 견해이기보다 계획을 설명하기 위한 구분이다. 한국은행 금융결제부, 『전자금융의 발달과 은행산업의 미래』, 1996.을 보면 단계를 아래와 같이 구분하고 있다. (1) 1단계 : 자행 On-Line화 및 업무자동화, (2) 2단계 : 금융네트워크 구축, (3) 3단계 : 화폐의 전자화 및 은행의 무점포화, (4) 4단계 : 금융 EDI.

다. 제 1단계는 금융기관 내부의 온라인망을 구축, 제 2단계는 이를 다른 금융기관의 전산망과 연결하는 금융서비스를 제공, 제 3단계는 금융기관과 고객간에 물리적인 접촉없이도 금융서비스를 제공하고 제공받을 수 있는 새로운 시스템을 구축·운영, 제 4단계로는 특정고객의 특수한 금융수요를 정확히 파악하여 상품의 특성 및 금리 등에서 다른 고객과 차별화된 금융서비스, 금융 EDI(Electronic Data Interchange, 전자문서교환)[40], 고객관계관리(CRM : Customer Relationship Management)시스템[41] 등이다. 시기적으로는 1단계가 1970-86년까지, 2단계는 1986-1999년까지, 그리고 3, 4단계는 1999년[42] 이후로 진행되고 있는데, 그 변화의 시간이 점차 단축되고 있음을 알 수 있다.

그러나 2003년에 발표한 금융감독원이 발표한 금융사고 예방대책 모범규준을 살펴보면 1. 보험영업 부문, 2. 자산운용 부문 3. 일반관리 부문, 4. 전산(IT) 부문 등으로 나누고 있는데, 이는 전산(IT)부문에서 일어나는 금융사고가 작은 문제가 아님을 나타내주고 있다. 변화된 환경에서 전산부문에서의 고객정보의 유출과 유용의 문제를 낳고 있는 것이다.

특히, 2단계 금융정보화가 진행된 1999년도 통계자료[43]에 의하면 금융사고의 대체적인 경향은 다음과 같다. 먼저 프로그램 오류나 실수에 의해 피해가 발생한 경우가 18%였는데, 이를 제외한 고의에 의한 금융사고는 ① 시스템 해킹(전자금융의 취약점 이용), 즉 홈뱅킹, 펌뱅킹 등 전자금융업무의 보안 취약성으로 인해 제 3자에 의해 침해당한 경우가 8%, ② 신용카드의 위조, 즉 위조된 신용카드가 이용된 경우가 4%, ③ 영업점 단말기 부정조작, 즉 정상업무처리를 수행할 수 있는 단말기를 담당자 또는 내부직원이 부정 조작한 경

40) 한국은행 금융결제부, 앞의 책. 기업의 거래정보와 은행의 지급결제정보를 모두 전자화 하여 상호 연계시킴으로써 기업과 은행 간은 물론 기업과 기업간의 모든 정보교환을 전자적으로 가능케 하는 것을 말함.

41) 각 시스템에 산재해 있는 고객 정보를 통합하고, 수익관리, 리스크 관리 시스템 등에서 제공하는 각종 고객 평가 정보를 바탕으로 효과적인 고객 관리를 하는 것으로 정보의 재가공을 통한 수익 창출 시스템이다.

42) 1999년 7월 1일 신한은행 인터넷 뱅킹서비스 시작.

43) 곽홍희,『금융정보망 정보보호 현황 및 표준화 동향』, 금융결제원, 1999.4.

우가 50%, ④ 단말기 조작자 기망, 즉 단말기 담당자를 기망하여 부정 조작하도록 한 경우가 10%, ⑤ 전산 프로그램 조작, 즉 고의로 전산 프로그램을 조작하여 악용한 경우가 8%, ⑥ 위조지폐의 세탁, 즉 위조지폐를 자동화기기를 이용하여 세탁·사용한 경우가 2% 등으로 나타났다. 이러한 경향은 시스템 안정성의 필요성을 더욱 확실하게 입증해주는 것이다. 이러한 필요성에도 불구하고 여전히 문제는 계속되고 있다. 2002년에도 고객정보를 유용하여 고객 예금 또는 시재금 등의 횡령, 유용사고가 236건에 1,583억원[44]이 발생하여 전체 금융사고의 62%를 차지하였다. 특히, 1999년 IMF 이후로 금융 종사자들에 의한 내부 범죄가 무척 많이 증대하였다. 물론 정보시스템의 결과로 보다 정확한 금융사고의 규모가 파악 가능했다고 볼 수 있지만 금융서비스의 안정성, 신뢰성에 손상이 있음은 분명하다.

<표 29> 유형별 금융사고 현황[45]

(단위 : 건, 억원)

구 분	1999년		2000년		2001년		2002년		2003년 6월	
	건수	금액	건수	금 액	건 수	금 액	건 수	금 액	건 수	금 액
횡령·유용	150	936	263	2,346	280	1,560	232	1,544	128	450
현금피탈	2	5	10	39	17	73	22	45	9	8
기 타	70	319	93	1,863*	100	645	126	1,927**	71	364
합 계	222	1,260	366	4,248	397	2,278	380	3,516	208	822

* 한빛은행 관악지점 거래처 부당지원(1002억원)

** (주)쌍용 무역금융사기(1,187억원)

물론 금융 서비스에서 중요한 것은 거래의 안전성과 신뢰성이기 때문에 금융기관은 이용자에게 신뢰를 주기 위한 다양한 보안 대책을 갖고 있다. 정부 또한 국가 경쟁력 차원에서 다양한 보안 지침을 생산하고 감독하고 있다.

---

44) 금융감독원, 『2002년도 금융사고 현황과 대책』, 2003.2

45) 금융감독원, 2003.10 함께하는시민행동 정보공개요청 자료.

나. 이용자 접근 시스템

점포를 이용하거나, CD[46]/ATM[47]기기를 이용하지 않고 개인이 독립적으로 네트워크를 통하여 금융서비스를 받을 수 있는 시스템 뿐 아니라 분산된 금융정보를 종합적으로 이용할 수 있는 시스템이 등장하고 있다. 다음과 같은 금융서비스가 그 대표적인 경우에 해당된다.

1) PC뱅킹

90년대의 대표적인 은행서비스 였던 PC뱅킹은 개인 PC, 전용 단말기로 천리안, 하이텔과 같은 telnet서비스를 경유 또는 직접 은행전산망에 접근하여 계좌이용을 할 수 있다. 인터넷 뱅킹이 등장하면서 서서히 퇴조하여 신한은행, 산업은행 등은 PC뱅킹을 중단했고, 점차 인터넷 뱅킹으로 통합하는 추세이다.

2) 인터넷 뱅킹

인터넷 뱅킹[48]은 현재 수출입은행을 제외한 18개 은행과 우체국, 씨티, 도이치, 홍콩상하이은행에서 인터넷뱅킹서비스를 제공하고 있다. 인터넷 뱅킹은 사용자가 인터넷을 통하여 은행서버에 연결하여 금융서비스를 이용하는 것으로 클라이언트(이용자 PC)->인터넷->인터넷뱅킹시스템(서버)<-co-lan[49]<-은행 호스트(은행 단말기)의 연결 구조를 가지고 있다. 2003년 6월말 현재 18개 국내은행, 씨티은행, 홍콩 상하이은행 및 우체국에 등록된 인터넷뱅킹 고객 수는 2,003만명에 이르고 있다.

---

46) Cash Dispenser: 현금 인출기
47) automatedteller machine: 자동 예금 인출, 예입 장치
48) 한국은행, 『2003. 6월말 현재 국내 인터넷뱅킹서비스 이용현황』, 2003. 6.
49) 기업전용회선

3) 모바일뱅킹

2002년말 현재 수출입은행을 제외한 18개 은행 및 우체국에서 휴대전화를 이용한 모바일뱅킹 서비스를 제공하고 있으며 8개의 국내은행이 PDA를 이용한 서비스를 제공하고 있다. 모바일 단말기->무선인터넷포털->은행의 연결구조를 가지고 있다.

2003년 6월중 국내은행과 우체국이 제공하고 있는 모바일뱅킹 서비스 이용실적은 120만건, 조회서비스는 118만건이고, 자금이체서비스는 2만 3천건으로 실질적인 이용 빈도는 아직 크지 않다고 할 수 있다.

4) E-Mail 뱅킹

2002년말 현재 제일, 외환, 신한, 국민은행에서 제공하고 있으며 등록고객수는 169,233명[50], 실이용고객수는 48,563으로 그 규모는 작다. E-Mail 뱅킹업체는 신용카드 결제서비스 제공업체를 통해 은행과 연결하여 개인의 송금을 연결하는 구조를 가지고 있다.

5) 계좌통합관리서비스

계좌통합관리서비스[51]는 다수의 금융기관에 분산되어 있는 은행, 증권, 신용카드 등의 고객 금융계좌정보를 계좌관리통합서비스업체에서 수집하여 계좌조회, 자금이체 등의 금융서비스를 통합 이용할 수 있도록 관리하여 주는 서비스를 말한다. '계좌통합관리서비스는 서비스기관(aggregator)이 제공한 접속수단(PFM[52] S/W 등)을 이용하여 금융계좌 정보보유기관들의 웹사이트를 추적,

50) 금융정보화추진분과위원회 사무국,『2002년도 금융정보화 추진현황』, 2003, p. 203
51) 금융정보화추진분과위원회 사무국, 위의 책, p. 8.
52) Personal Finance Management. 개인금융자산관리

데이터를 수집하는 스크린 스크래핑(screen scraping) 방식[53]과 금융계좌 정보 보유기관의 데이터베이스에 저장된 데이터를 직접 송수신하는 시스템 연동방식이 있다. 국내에서는 2001년 4월 제일은행이 핑거(주)와 제휴하여 스크린 스크래핑방식에 의한 계좌통합관리서비스를 최초로 시작하였다. 2002년말 현재 시중은행 8개, 지방은행 4개, 특수은행 1개 등 13개 은행에서 계좌통합관리서비스를 제공하고 있으며 모두 스크린 스크래핑방식을 채택하고 있다.

다. 이용자 보호를 위한 정책

1) 전자금융거래 표준약관

이용자(개인, 기업)과 은행사이의 거래 안정성이 필요하게 되자 2000년 공정거래위원회는 인터넷뱅킹과 PC뱅킹에서의 이용자 보호를 위하여 전자금융거래 표준약관을 제정하고자 했으나 은행연합회가 해킹사고의 은행측 책임소재 명시를 거부하여 사실상 무산되었다. 그러나 2000년 10월 17일 서울지법 민사합의19부(김종백 부장판사)는 모 증권사가 "PC뱅킹으로 은행거래를 하던 중 비밀번호가 새나가 1억5,000여만원의 예금이 인출됐다"며 S은행을 상대로 낸 당좌계금지급 청구소송에서 원고승소 판결했다. 재판부는 "누구 과실에 의해 비밀번호가 누출됐는지 알 수 없을 경우 그 입증책임은 고객이 아니라 은행에 있다"며, 특히 PC뱅킹제도는 "은행이 비용절감 및 고객 편의 등을 위해 자체적으로 도입한 만큼 안전성 확보 의무는 명백히 은행에 있다"고 밝혔다. 그 후 다시 시도되어 2001년에 재정된 전자금융거래 기본약관[54]은 제23조(손실부담 및 면책)에 "거래지시의 전송과정에서 거래처의 고의 또는 과실에 의하지

53) 현재 스크린 스크래핑서비스는 클라이언트(Client) 방식으로 이용자가 계좌정보를 요구할 때마다 고객의 PC에 저장된 프로그램 등을 가동하여 해당정보를 고객의 PC에 저장하는 방법이 주로 쓰이고 있다. 중계기관에 관련 정보가 저장되는 서버(sever)방식에도 스크래핑서비스방식이 이용될 수 있다.

54) 공정거래위원회 표준약관 00028호

않은 사고가 발생한 경우에는 그러하지 아니하다"라는 조항을 넣어 이용자의 권익을 향상시켰다.

2) 금융기관전자금융업무감독규정[55)]

감독규정에 관한 금융기관전자금융업무감독규정시행세칙이 2001년 3월 30일에 제정되었고, 감독의 대상은 "1. 은행법에 의해 설립된 금융기관, 2. 농업협동조합법에 의한 농업협동조합중앙회의 신용사업부문, 3. 수산업협동조합법에 의한 수산업협동조합중앙회의 신용사업부문, 4. 한국산업은행법에 의한 한국산업은행, 5. 중소기업은행법에 의한 중소기업은행, 6. 한국수출입은행법에 의한 한국수출입은행, 7. 신탁업법에 의한 신탁회사, 8. 주택저당채권유동화회사법에 의한 주택저당채권유동화회사, 9. 상호신용금고법에 의한 상호신용금고, 10. 종합금융회사에관한법률에 의한 종합금융회사, 11. 여신전문금융업법에 의한 여신전문금융회사, 12. 보험업법에 의한 보험사업자, 13. 증권거래법에 의한 증권회사, 14. 증권투자신탁업법에 의한 위탁회사, 15. 증권투자회사법에 의한 자산운용회사, 16. 선물거래법에 의한 선물업자, 17. 신용협동조합법에 의한 신용협동조합 및 그 중앙회, 18. 기타 금융업 또는 금융관련 업무를 영위하는 자로서 감독원장이 정하는 자" 등이다.

감독규정세칙은 전산실 보호대책, 단말기 보호대책, 전산자료 보호대책, 해킹 방지대책, 바이러스 감염 방지대책, 홈페이지 등 공개용 웹 서버 관리대책, IP주소 사용대책, 정보시스템의 성능관리, 직무의 분리, 전산원장 통제, 거래통제, 프로그램 통제, 일괄작업에 대한 통제, 암호프로그램 및 키 관리 통제, 비밀번호 관리, 그리고 금융감독원이 보안성심의, 정보기술부문 실태평가를 할 수 있도록 되어 있다.

---

55) 제정 금융감독위원회 공고 제2000-117호(2000. 12. 29)

라. 국제적인 전자금융 감독의 흐름

1) 국제결제은행(Bank for International Settlement)

국제결제은행(BIS) 산하 은행감독위원회(Basel Committee)는 2001년 5월 전자금융 관련 리스크관리 준칙[56](Risk Management Principles for Electronic Banking)을 발표하였다. 주된 내용은 1. 거래의 안전장치 마련에서 전자금융거래 당사자의 신원을 확인, 직원의 직무 분리, 전자금융거래 기록 및 관련 정보자료의 유지를 언급하고 있으며, 2. 법적 및 평판리스크에 대한 효율적 관리에서 고객의 개인정보가 부당하게 유출되는 것을 방지하고 개인의 프라이버시[57]가 침해되지 않도록 적절한 보호 장치를 언급하고 있다.

1. 은행은 고객의 전자금융정보의 비밀을 유지할 수 있도록 적절한 암호기술, 특정 프로토콜 등 보안통제수단을 사용하여야 함.
2. 은행은 전자금융에 관련된 고객보호기반과 프로토콜을 정기적으로 평가하는 적절한 절차와 통제력을 확립해야 함.
3. 은행은 제3자 서비스제공자가 채택하고 있는 비밀유지 및 프라이버시에 관한 정책이 은행자신의 정책과 부합되는지를 확인해야 함
4. 은행은 전자금융 이용고객에 대해 고객정보의 비밀유지 및 프라이버시에 관한 정보를 제공할 수 있도록 다음 사항을 포함하여 적절한 대책을 강구해야 함.
   - 웹 사이트 등을 통해 고객에게 프라이버시에 관한 은행정책을 전달함. 고객이 동 정책을 완전하게 이해할 수 있도록 이러한 안내문은 분명하고 구체적인 단어를 사용하는 것이 중요함. 법률적인 사항을 장황하게 서술하

---

56) Basel Committee Publications, *Risk Management Principles for Electronic Banking*, May 2001, (http://www.bis.org/publ/bcbs82.pdf). 축약본을 금융감독원 감독총괄국·IT 기술검사국, 『금융감독원 금융기관 전자금융업무 감독규정 해설』 (2001. 10.), p. 154에서 살펴볼 수 있다.

57) 이는 위 준칙의 『Appendix V, Sound Practices to Help Maintain the Privacy of Customer E-Banking Information』에서 제시된다.

는 것은 비록 그 내용이 정확하더라도 대부분의 고객이 읽지 않을 가능성이 있음.

- 패스워드, 개인 식별번호는 물론 기타 은행 및 개인 데이터가 누출되지 않도록 하여야 한다는 점을 고객에게 인식시킴
- 바이러스 예방, 물리적인 접근 통제, 인터넷 접속시의 방화벽 설정 등 퍼스널컴퓨터 보안에 관한 전반적인 정보를 고객에게 제공함

2) 국제증권감독위원회기구(IOSCO)

국제증권감독위원회기구(IOSCO)산하 기술위원회(TechnicalCommittee)는 1998년에 이어 2001년 6월 인터넷의 발전과 이용확대에 따라 '정보기술부문 및 새로운 인터넷업무에 대한 감독상의 대응'을 담은 두 번째 보고서 '인터넷상의 증권거래활동에 대한 보고서Ⅱ[58]'(Report on Security Activity on the InternetⅡ)를 발표하였다. 이 보고서에서는 인터넷업무 발전에 관한 감독 이슈와 감독 대응 범위[59]를 다음과 같이 규정하고 있다.

'(시스템)의 양적 조절관리 능력, 정기적인 스트레스 테스팅(stress testing) 수행, 정보기술관련 업무수행 및 취약점 분석, 서비스중단에 대비한 백업시스템 구축, 시스템 용량문제를 처리하기 위한 절차 개발, 인터넷접속이 어려운 경우 주문처리를 위한 대체수단 공시, 투자자를 위한 콜센터 구축, 시스템의 침입탐지 또는 침입차단시스템 등 구축, 상시 모니터링 및 비상계획 수립, 데이터 무결성(integrity)을 유지하기 위한 시스템 도입, 프로그램 소스코드(source code)의 무결성을 유지하기 위한 통제방안 마련, 정기적으로 전문적인 보안점검 수행, 암호화, 인증, 부인방지기술의 사용, 바이러스에 대한 대책 수립, 정보기술부문에 대한 전문 감사 실시, 금융거래에 대한 자료 기록.유지, 이용자불만을 해소하기 위한 효율적인 절차 수립, 투자자에 대한 교육'

58) http://www.iosco.org/pubdocs/pdf/IOSCOPD120.pdf
59) http://www.iosco.org/pubdocs/pdf/IOSCOPD120.pdf .16-18p

3) 국제보험감독관협의회(IAIS)

국제보험감독관협의회(IAIS)는 2000년 10월 '인터넷상의 보험 업무에 대한 감독원칙'[60](Principles on the Supervision of Insurance Activities on the Internet)을 발표하였다. 보험업무의 인터넷 도입이 야기하는 사기(fraud)나 보안문제 등 부작용에 대해 감독당국이 고려해야할 3개 원칙을 제시하였다. ▲ 인터넷 보험판매에 대한 감독당국의 접근방식은 전달매체의 종류에 상관없이 일정해야 하고 ▲ 감독당국은 보험회사와 보험중개업자가 인터넷 보험판매에 있어서도 투명성의 원칙과 공시사항을 동일하게 준수해야 하고 ▲ 감독당국은 인터넷 보험 업무를 규제함에 있어서 상호 협력해야 한다는 것이다.

마. 은행, 카드, 증권, 보험사, 쇼핑몰의 개인정보보호-보안 인증 현황

대면 거래가 아닌 비대면 거래가 증대함에 따라, 거래 정보의 보안과 개인정보보호가 중요하게 되었다. 법적 제도적 권고 사항들이 만들어졌지만 각 기업들이 어떠한 신뢰도를 갖고 있는가에 대해 정확한 측정을 이용자가 갖기는 힘들다. 그래서 제3의 기관이 신뢰도를 인증하는 방법이 추세가 되고 있다. 기업은 선택에 따라 국제 표준의 보안인증, 제 3기관의 개인정보보호 인증을 받을 수 있다. 예를 들어 ebay.com은 TRUSTe[61] 마크를 부착하고 있다. TRUSTe는 1996년 미국에서 설립되었는데 개인정보보호에 관한 국제적 비영리 인증기구이다. TRUSTe 마크는 웹 싸이트에서 '이용자에 관한 수집된 정보가 무엇인지, 정보가 이용되는 방법, 제3자와 공유되는 정보가 뭔지, 정보이용에 관한 선택권, 개인정보를 위한 보안장치, 개인정보 수정 가능' 등을 보증한다. 국내에서도 정보통신산업협회에서 부여하는 i-safe 마크, ePRIVACY 마크가 있다. i-safe는 네트워크상에서 영리 또는 비영리 목적으로 설치 운영중인

60) http://www.iaisweb.org/content/02pas/02internet.pdf
61) http://www.truste.org

인터넷 사이트를 대상으로 한 개인정보보호, 시스템 보안, 소비자 보호에 대한 평가를 통하여 인터넷 사이트 안전마크를 부여하는 제도이다. ePRIVACY는 인터넷사이트의 개인정보보호 정책 및 관리수준을 종합적이고 객관적으로 평가하여 일정기준을 충족하는 경우 개인정보보호 우수사이트 인증마크(ePRIVACY마크)를 부여하는 제도이다. 또한 정보보호경영시스템에 대한 국제적인 보안 표준인 ISO17799/BS7799인증[62]이 있다.

그러나 제3의 기관에서 인증마크를 부여 받는 것은 기업의 자율이기 때문에 활성화가 되지 못하고 있다. 금융 거래가 이루어지는 은행, 카드, 증권, 보험사, 쇼핑몰에 대한 조사 결과를 보면 더욱 확연해 진다. 특히, 증권사에서는 이러한 시도가 전무한 실정이다. 또한 기존의 금융권은 금융감독원의 감독을 받고 쇼핑몰과 같은 닷컴 기업들은 정보통신부의 감독을 받고 있기 때문에 종합적인 개인정보보호 정책이 부족하다고 볼 수 있다. 전자 상거래가 점차 증가하고 있는 현황을 고려한다면, 전자거래의 안정성을 확보할 수 있는 종합적인 대책이 도입되어야 하며, 특히 기업의 적극적인 도입의지가 필요하다.

기업이 인증을 받기 위해서는 연간 대략 50~100만원 정도의 비용이 소요된다. 그러나, 인증을 받는 만큼의 홍보 효과가 나타나지 않기 때문에 기업 측에서는 인증을 꺼리게 된다. 앞에서 언급한 i-safe 마크나 ePRIVACY 마크 이외에도 몇몇 소비자단체나 시민단체들도 인증 마크를 운영하고 있으나, 난립하고 있는 인증마크들 중 일반 시민들에게 각인된 인증 마크는 없다. 때문에 홍보 효과가 나타나지 않는 것이다. 인증 마크를 운영하는 기관들이 적극적으로 자신들의 인증 마크의 위상을 제고하도록 노력할 필요가 있음을 보여준다.

바. 정보시스템 변화에 따른 자율과 규제

현재 계좌통합서비스는 단순한 인터넷 서비스로 금융감독당국의 인허가 또

62) 영국표준협회의 보안표준규격 BS7799는 국제표준기구(ISO)에 의해 국제규격 ISO17799로 채택, 승인되었다.

는 등록, 신고 등의 절차가 없이도 취급이 가능하다. 즉, 금융회사가 계좌통합서비스를 제공하는 경우에는 여타 전자금융 서비스와 마찬가지로 보안기준, 개인정보보호 대책에 관한 금융감독원의 감독, 검사대상이 되지만, 인터넷 업체가 서비스를 제공하면 감독, 검사 대상이 아니라는 것이다. 따라서 finger, daum.net, 주식회사 피지스 등의 계좌통합서비스를 하고 있는 업체들은 감독의 사각지대라고 볼 수 있다. 2002년 10월 「전자금융거래법 제정안」이 국회에 제출되었으나 아직까지 계류중이다. 이 법에 의하면 모든 금융거래를 법률의 적용 범위로 삼고 있기 때문에 IT기술의 변화에 따른 신종 업종도 당국의 감독을 받게될 전망이다.

2003년 4월 금융감독원이 발표한 'IT 및 전자금융거래 안전성 제고 대책'에는 '온라인증권거래에 대한 공인인증서의 전면 도입,' '전자금융거래의 인증절차 강화,' '비밀번호 사전기재 방식에서 사후입력방식으로 변경,' '예금거래 신청서, 예금출금 의뢰서 등의 비밀번호란 폐지(03.12.31까지 완료),' '전자금융거래 비밀번호 자릿수를 4자리에서 6자리로 변경 및 전자금융거래 비밀번호와 통장거래 비밀번호 분리사용(2004년 이후),' '텔레뱅킹, 인터넷뱅킹 거래시 「1회용 비밀번호」 사용 및 고객이 비밀번호를 직접 입력하는 「핀패드 시스템」 도입(03.12.31까지 완료)' 등이 포함되어 있다. 현재는 제일은행, 우리은행, 부산은행, 하나은행이 핀패드 시스템을 채택중이다.

그러나 개인정보보호 인증제와 같이 기업간의 자율로 맡겨진 부분들은 참여가 저조하여 이용자 보호를 위한 기업의 노력이 부족하다고 볼 수 있다. 이를 위해서는 개인정보보호 인증의 의무화 같은 강한 정책 수단이 필요하고 금융감독원이나 정보통신부로 모호하게 나뉘어 있는 개인정보보호 감독 부분을 포괄적으로 규율 할 수 있는 국가 기관을 설립하거나 기존의 감독 업무 재조정을 통한 합리적인 관리방안 마련이 필요하다.

2. 개인정보 보호를 위한 관리적 대책 수립 실태

현재 기업 내에서 개인정보 보호를 위한 관리 대책이 어떻게 마련되고 있는지를 조사하기 위해, 10곳의 개인정보보호책임자·담당자들에 대한 면접 조사를 실시했다. 조사대상 기관은 은행·쇼핑몰·포털/커뮤니티 각 2곳, 카드사·보험사·증권사·언론사 각 1곳이다.

가. 개인정보관리책임자·담당자

정보통신부의 「정보통신망이용촉진및정보보호등에관한법률」과 「개인정보보호지침」에 따르면, 개인정보를 수집하는 서비스 제공자들은 이용자 개인정보의 보호와 이용자의 불만 처리를 담당하는 개인정보관리책임자를 두도록 하고 있다.[63] 그리고, 이 역할을 임원, 혹은 개인정보 고충처리 부서나 개인정보 취급 부서의 부서장이 담당하게끔 하고 있다.

개인정보관리책임자는 기업 내에서 개인정보보호 감독기구와 같은 역할을 해야 한다. 따라서, 지위와 업무에서 독립성과 자율성을 확보하는 것이 중요하다. 지위의 독립성과 관련하여서는 개인정보관리책임자의 임기 보장이 중요한 판단 기준이 된다. 또한, 업무의 독립성과 관련하여서는 개인정보 보호의 책임을 담당하는 부서가 개인정보를 활용하는 부서와 분리되는 것이 필요하다.

---

63) 개인정보보호지침(2002. 4)
제15조(개인정보관리책임자의 지정) ① 서비스제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 불만을 처리하기 위하여 다음 각호의 업무를 수행하는 개인정보관리책임자를 지정하여야 한다.
1. 이용자 개인정보의 수집·이용·제공 및 관리에 관한 업무의 총괄
2. 서비스제공자등의 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검
3. 이용자로부터 제기되는 개인정보에 관한 불만이나 의견의 처리 및 감독
4. 기타 이용자의 개인정보 보호에 필요한 사항
② 개인정보관리책임자는 서비스제공자등의 임원 또는 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장의 지위에 있는 자 또는 개인정보 취급부서의 장이어야 한다.

1) 지위의 독립성

이번 연구의 조사대상 기업들에서는 대개 인터넷 사이트 운영 관련 부서나 고객관리 부서의 부서장이 개인정보관리책임자의 역할을 맡고 있었다. 개인정보관리책임자가 이사 이상의 직위를 갖고 있는 곳은, 금융기관의 경우 단 한 곳에 그쳤으며, 일반 인터넷 사이트의 경우에도 쇼핑몰 2곳, 포털/커뮤니티 2곳, 언론사 1곳만이 개인정보관리책임자를 이사급 이상의 임원으로 임명하고 있었다.

『독일 정보보호법의 현대화 보고서』는 기업이나 행정관청의 정보보호담당자가 자율성과 독립성을 보장받아야 함을 지적하고 있다. 특히, 독립성과 관련하여 보고서는 부당해고 방지를 위해 최소 5년의 임기를 보장할 것을 제안하고 있다.[64] 우리 개인정보보호지침에서 개인정보관리책임자를 임원급으로 하도록 제안하고 있는 것도 유사한 맥락이라고 생각되지만, 여러모로 부족한 것이 현실이다.

우선, 국내 법령이나 지침에 따르면, 개인정보관리책임자가 반드시 임원급일 필요는 없으며, 개인정보 취급부서나 고충처리 부서의 부서장도 관리책임자의 임무를 맡을 수 있다. 그러나, 이 경우 기업 측의 부당한 압력에 대해 맞서기가 현실적으로 어렵다.

임원급으로 임명하더라도 지위의 독립성이 충분히 보장되지는 않는다. 감사의 경우, 일반적으로 약 3년의 임기가 보장된다. 그러나, 일반 임원들의 경우 사규에 특별한 규칙이 없는 한 주주총회에서 언제든 해임을 결의할 수가 있다. 개인정보관리책임자가 업무를 올바르게 수행하기 위해서는 감사와 같이 임기의 보장을 통한 지위 보장이 필요하다.

---

64) 이형규, 『독일 정보보호법의 현대화 추진방안』, 한국정보보호진흥원, 『각국 개인정보보호 법제도의 비교법적 접근』, 한국정보보호진흥원 2003년 제2회 개인정보보호 심포지움, 2003, p. 15.

2) 업무의 독립성

현재 정보통신부의 「개인정보보호지침」은 "임원, 혹은 개인정보 고충처리 부서나 개인정보 취급 부서의 부서장"을 개인정보관리책임자로 임명하도록 규정하고 있다. 그러나 기업에서 개인정보는 보호의 대상이기도 하지만, 영리상의 목적을 위해 활용하는 대상이기도 하다. 따라서 개인정보를 활용하는 부서는 업무의 편의를 위해 개인정보 보호의 임무를 소홀히 하거나 의도적으로 무시할 가능성이 있다.

따라서 마케팅 담당 부서를 비롯하여 활용의 목적으로 개인정보를 취급하는 부서가 개인정보 보호의 임무를 함께 수행하지 않게 할 필요가 있다. 한국표준협회의 「정보 기술 - 정보 보안 경영 실무 지침」에서는 시스템의 우발적, 고의적 오용의 위험을 줄이는 것이 중요하다고 설명하면서, 사건의 개시는 이에 대한 인가와는 분리되어야 할 것이라고 지적한다.[65] 뒤에 서술하겠지만, 국가 차원에서도 행정 효율성·산업 육성 등의 임무를 맡은 부처가 개인정보 보호의 임무도 맡는 것은 바람직하지 않은 결과를 가져온다. 물론, 개인정보 관련 업무만을 다루는 부서를 둘 필요까지는 없다.

개인정보를 취급하는 부서의 장도 그 부서의 개인정보 관리 실태를 감독하는 역할을 담당해야 한다. 다만, 전체적인 개인정보 보호 임무를 맡은 별도의 관리책임자가 각 부서의 개인정보 관리 실태를 총괄 감독하고, 각 부서장들이 맡은 개인정보 보호 임무에 대해서도 감독해야 한다.

조사 대상 기업들의 경우를 살펴보면, 개인정보관리책임자와 담당자가 E-비즈니스를 담당하는 부서 소속으로 되어 있는 경우가 많았다. 웹사이트 운영을 담당하는 부서에 개인정보관리의 책임을 맡기고 있는 것이다. 그런데, 개인정보관리담당자의 경우는 실무를 고려하여 사이트 운영 부서에 둘 수 있지만, E-비즈니스 업무를 총괄하는 부서장을 관리책임자로 두는 것은 바람직하지

65) 한국표준협회, 『정보 기술 - 정보 보안 경영 실무 지침』 (2002.8.26)

않아 보인다. 다음으로 콜 센터나 고객 상담실 등 고객 상담업무를 담당하는 부서에서 맡고 있는 곳이 많았다. 또한 개인정보관리책임자가 영업 담당 부서에 소속되어 있는 곳도 있었는데, 카드영업팀 소속이 1곳, 마케팅팀 소속이 2곳이었다.

나. 개인정보 관련 업무 체계

1) 개인정보 관련 업무 분담

한국표준협회의 「정보 기술-정보 보안 경영 실무 지침」에 따르면, 정보 보호에 대한 책임을 적절히 할당할 필요가 있음을 지적하고 있다.[66] 정보통신부의 『개인정보보호지침 해설서』에서는 복수의 개인정보관리책임자를 지정할 수 있으며, 이 경우 당사자간의 역할 분담을 명확히 해야 한다고 강조하고 있다.[67]

모든 개인정보 보호 임무를 한 사람 혹은 한 부서에서 관리하는 것은 소규모 기업에서는 가능할 수 있으나 대규모 기업에서는 사실상 어렵다. 따라서, 개인정보관리책임자는 기업 전체의 효율적인 개인정보 관리 프로세스를 설계한 후, 이 프로세스가 원활히 작동하는가를 검토하는 것을 주 임무로 삼아야 한다. 구체적인 관리·보호의 임무는 개별 부서와 담당자들에게 위임하는 것이 바람직하다.

규모가 큰 금융권들의 경우는 주로 전산 담당 부서에서 보안 시스템의 설계 차원에서 개인정보 관리 프로세스를 설계하고, 고객 데이터베이스 보호를 전담한다. 창구에서의 문서 보안이나 실무자 교육 등 실제 관리 활동은 현장의 지점장들에 의해 이루어지고 있다.

반면, 쇼핑몰이나 인터넷 기업들의 경우 기능별로 역할 분담이 이루어진다.

---

66) 한국표준협회, 『정보 기술-정보 보안 경영 실무 지침』, 2002. 8. 26. pp. 7-8.
67) 정보통신부, 『개인정보보호지침』 해설서, p. 69.

주로 고객관리 담당 부서에서 개인정보보호 프로세스에 대한 책임을 맡으나, 실제 업무는 고객 고충처리를 중심으로 이루어진다. 시스템의 설계와 고객 데이터베이스 보호는 전산 담당 부서에서 주로 담당하고 있으며, 개인정보 보호에 대한 감사나 교육 등은 경영 관련 부서나 감사실 등에서 맡는 경우도 많다.

<표 30> A 쇼핑몰의 개인정보관리규정의 일부

5.1.2. 부서별 역할 및 권한

(중략)

2) CS 지원부장
① 개인정보 수집 및 이용시의 검토 및 승인
② 전사적인 개인정보보호 규정의 마련 및 개정, 교육 업무
③ 개인정보보호에 관한 대내외 창구역할을 수행
④ 고객 상담창구를 설치 운영하며, 불만시고의 접수 처리
⑤ 고객정보DB 시스템 접근권한자 지정
⑥ 개인정보보호정책의 제정 및 개정 작업

3) 경영지원부장
① 개인정보관리책임자 및 담당자의 임명
② 개인정보보호 규정 이행사항 및 관련 직원의 준수 여부 파악 및 관리직원에 대한 개인정보보호 교육 실시 / 관리
③ 개인정보보호 관련 내부 감사규정을 수립 / 시행

그런데, 이처럼 기능이 분화될 경우, 각 기능이 잘 작동하는지를 감독하는 기능을 개인정보관리책임자가 담당할 수 있도록 보장하는 것이 중요하다. 예컨대, <표 30>에서 확인할 수 있듯이, A 쇼핑몰의 경우에는 고객관리부서장이 개인정보관리책임자로 임명되어 있으나, 실제 개인정보관리책임자를 지정할 권한과 사내 개인정보 보호 실태를 감독할 권한은 경영지원부서의 부서장이 담당하고 있다. 이 경우, 개인정보관리책임자가 충분한 권한을 행사하기 어려울 것이다.

언론사 사이트들의 경우에는 개인정보 관리가 대개 언론사의 소규모 자회사들에 의해 운영된다. 그렇기 때문에 개인정보 보호 및 각종 고충 처리의 임무

가 담당자에게 전적으로 맡겨지는 경우가 많다. 이 경우, 개인정보관리책임자만 규정을 준수하면 별 문제가 발생하지는 않는다는 점에서 바람직한 측면이 있으나, 반대로 개인정보관리책임자가 외근이나 휴가 등으로 자리를 지키지 못할 경우에는 고객 고충을 처리하지 못하는 문제가 발생한다.

금융기관들의 경우 사실상 단일한 개인정보 관리체계가 존재하지 않았다. A 보험사의 경우 웹사이트 담당 부서에 개인정보관리책임자가 지정되어 있었으나, 해당 부서원들조차도 관리책임자가 누구인지 모르고 있었다. 대신, 준법감시부라는 부서에서 개인정보 보호를 비롯한 전반적인 업무 통제를 수행했다. A 은행의 경우 개인정보관리책임자가 은행 전반의 개인정보 보호와 관련된 사항을 파악하지 못하고 있었으며, 전산담당 부서에서 관련된 답변을 들을 수 있었다. B 은행 역시 웹사이트 상의 개인정보보호책임자가 다른 분야들에 대한 업무를 담당하지 않았으며, 각 부서별로 부서장이 보안 업무를 맡고 있었다. 그러나, 각 부서들 사이의 정기적 의사소통 경로는 존재하지 않았다. 반면, A 카드사의 경우 정보보호, 보안, 개인정보보호 담당자들 사이의 부정기적 회의가 있었으나, 개인정보보호 담당자가 책임을 지는 구조는 아니었다.

2) 현장 직원들의 개인정보 접근 통제

상당수의 개인정보 유출 관련 사건이 기업 내부의 직원들에 의해 일어난다. 이를 예방하기 위해 「정보통신망이용촉진및정보보호등에관한법률」 및 「개인정보보호지침」은 개인정보를 취급하는 자를 최소한으로 제한할 것을 규정하고 있다.[68]

---

68) 개인정보보호지침(2002.4)
제10조(개인정보취급자의 제한) 서비스제공자등은 이용자의 개인정보를 취급할 수 있는 자를 다음 각호의 1에 해당하는 자로 정하여 최소한으로 제한하여야 한다.
1. 이용자를 직접 상대로 하여 마케팅 업무를 수행하는 자
2. 개인정보관리책임자 등 개인정보관리업무를 수행하는 자
3. 기타 업무상 개인정보의 취급이 불가피한 자

단순히 인원의 최소화에만 그치지 않는다. 더욱 중요한 것은 개별 개인정보 취급자가 접근할 수 있는 범위를 최소화하는 것이다. 「정보 기술-정보 보안 경영 실무 지침」은, 허가된 접근 수준이 업무 목적에 적절한지를 판단하여 개인의 기능상 역할에 필요한 최소한의 권한만이 할당되어야 할 것이라고 지적하고 있다.[69]

이와 관련되어 가장 중요한 관리상의 문제는 금융기관의 창구나 정보통신서비스제공자들의 콜 센터, 쇼핑몰의 텔레마케터 등 현장에서 근무하는 직원들의 고객 개인정보 접근에 대한 통제이다.

대부분의 조사대상 기업에서 일반 직원들은 고객 데이터베이스에 접근할 수 없도록 시스템이 구성되어 있었다. 포털/커뮤니티 사이트 등의 경우 비밀번호 분실 등의 민원에 대해서 콜 센터에서는 처리 권한이 없었으며, 온라인 상에서 자동 처리되도록 하고 있었다.

은행권의 경우, 고객이 비밀번호를 제시할 경우에 한해 해당 고객의 데이터베이스에만 접근이 가능했다. 다만, 이 과정에서 창구 직원이 고객의 계좌번호와 비밀번호를 알아낼 가능성도 전혀 없지는 않다. 때문에, 최근 몇몇 은행에서는 비밀번호를 입력하는 것조차 고객이 '핀 패드'라는 장치를 통해 직접 입력하도록 하고 있다.

쇼핑몰의 경우에는 상담원들이 전화를 통해 직접 주문을 받거나 물품 구매에 대한 확인 혹은 취소 등의 업무를 담당하게 되므로, 개인정보 유출의 가능성이 없지 않다. 지난 2002년, 한 쇼핑몰에서 일하는 아르바이트생들이 회원들의 신용카드번호와 비밀번호 앞 두 자리 숫자를 열람할 수 있도록 되어 있었다는 문제점이 언론을 통해 지적된 바 있다.[70]

이 문제에 대해 현재 쇼핑몰들의 관리 체계를 살펴보았다. A 쇼핑몰의 경우, 전화 구매를 희망하는 사람들의 경우 상담원들이 일단 카드 번호와 비밀번호를 물어볼 수밖에 없었다. 그러나 일단 해당 개인정보들이 입력되어 데이

69) 한국표준협회, 앞의 책, p. 30.
70) 시사저널 제 651호(2002.4.18.)

터베이스에 저장되고 나면, 상담 직원들은 그 정보에 대해 접근할 수 없도록 되어 있었다. 데이터베이스 접근권은 결재처리 담당자와 개인정보관리책임자에게만 부여되었다.

그렇더라도 유출의 가능성을 조금 더 줄이기 위해서는 신용카드 번호나 비밀번호는 고객 쪽에서 전화 다이얼을 눌러 바로 데이터베이스에 저장되도록 하는 방식이 바람직할 것이다.

3) 관리자들의 개인정보 접근에 대한 통제

기업 특성에 따라서는 중간관리자들의 개인정보 접근이 필요한 경우가 많다. 이 경우 각 기업별로 접근에 대한 적절한 통제 장치들을 마련해두고 있다. 일반적으로 접근권한을 ID/패스워드를 통해 제한하고 있으며, 접근가능한 IP를 지정하여 이중으로 접근권을 제한하는 경우도 있었다. 많은 기업들이 고객정보 DB에 대한 열람·제공, DB 접근·수정에 대한 기록을 유지하고 있었다. 고객 DB가 지점별로 혹은 업무 분야별로 분리되어 있을 경우, 담당 업무와 무관한 DB에 접근하지 못하도록 방화벽을 설치하고 있는 경우도 많았다.

조사대상이었던 A은행의 경우에는 지점의 부점장들에게 발급된 책임자 카드를 통해서만 고객 개인정보에 접근할 수 있었으며, 이 카드의 사용 내역은 자동 기록되어 감사 자료로 사용되었다.

한편 A 언론사의 경우 계열 사이트 운영자들에게는 개인정보 접근 권한을 인정하고 있었는데, 오직 열람 권한만이 허용되고 있었다. 대신 접근에 대한 기록은 유지하지 않고 있었다.

4) 외부 위탁관리에 대한 규정

조사대상 기업 중, 고객 개인정보를 외부에 위탁하여 관리하는 경우는 거의 없었다. 특히, 금융권은 고객 정보의 관리가 매우 중요한 부분이니만큼 위탁

관리하는 경우가 거의 없었다.[71] 그러나, 포털 사이트나 쇼핑몰, 언론사 등 정보통신서비스제공자 중 몇몇 기업은 텔레마케팅이나 보험상품 판매 업무를 위탁하는 경우가 있었다. 이 경우, 대개 유출 방지, 사용 후 파기, 실제 유출 사건 발생시 손해 배상 등을 내용으로 하는 계약서를 작성하고 있다. 그러나 개인정보를 위탁 관리하는 경우에도 개인정보 침해 방지를 위해 좀 더 적극적으로 노력을 할 필요가 있다. 예컨대 위탁관리 업체를 대상으로 계약 이행 여부를 심사할 권리를 계약서 상에 반영하고, 실제 감사를 수행해야 한다.[72]

한편, A 쇼핑몰은 고객 상담 업무를 외부 업체에 맡기고 있지만 오히려 그 업체의 직원들을 A 쇼핑몰 내에 와서 근무하도록 했다. 위탁 과정에서 발생하는 DB 유출을 막기 위해 개인정보 DB를 회사 건물 밖으로 나가지 못하게 한 것이다.

다. 내부 감사

개인정보관리책임자는 기업 내부의 개인정보 보호 프로세스가 원활히 작동하고 있는지, 직원이 사내 개인정보관리규정 및 준수사항을 성실히 이행하는지에 대하여 내부 감사를 실시할 권리를 가져야 한다.[73]

사실상 개인정보관리책임자 및 담당자에게 개인정보 관련 업무가 국한되어 있는 A 언론사에서는 내부 감사를 진행하지 않았다. 상대적으로 회사 규모가 작은 B 포털/커뮤니티 역시 내부 감사가 없었다.

---

71) 다만 A 증권사 개인정보관리책임자의 말에 따르면, 경쟁 관계에 있는 몇몇 증권사에서 개인정보 관리 업무를 위탁하고 있는데, 이 역시 계열사이기 때문에 가능한 일이라고 한다.

72) 한국표준협회, 앞의 책, p. 6.

73) 개인정보보호지침(2002.4)

제26조(내부감사) ① 서비스제공자등은 소속 직원이 이 지침에서 정하는 개인정보 보호의무를 성실히 이행하는지 여부를 감사하여야 한다. 이 경우 개인정보관리책임자는 감사대상, 감사절차 및 방법 등 감사의 실시에 관하여 필요한 지침을 수립하여야 한다.

② 서비스제공자등은 제1항의 규정에 의한 감사를 실시한 결과 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 이 지침을 위반한 사실을 발견한 때에는 시정·개선 또는 인사발령 등 지체없이 필요한 조치를 취하여야 한다.

감사를 실시하는 기관은 다양했다. A 쇼핑몰의 경우, 개인정보관리 전담부서인 고객관리 부서가 경영지원 부서와 협력하여 감사를 실시했다.[74] 반면, B 쇼핑몰의 경우는 전적으로 개인정보관리 전담부서가 감사 권한을 보유하고 있었다. A 은행의 경우 본점 검사부가, A 포털/커뮤니티의 경우 감사위원회가 감사를 실시하고 있었다. A 보험사의 경우 감사부서 외에도 준법감시부가 내부 업무 통제를 하고 있었다.

한편, 개인정보 감독을 담당하는 정부 부처나 별도의 감독 기구는 각 기업의 개인정보관리책임자로부터 해당 기업의 개인정보 보호 관련 감사 계획과 결과를 정기적으로 보고받는 체계를 마련할 필요가 있다. 감독 기관이 개별 기업의 관리 실태를 일일이 직접 조사하는 것이 좀 더 확실한 조사 방법이겠지만, 모든 기업을 조사하기에는 비용이 너무 많이 든다. 반면, 개인정보관리책임자들의 활동을 감독하는 것은 직접 조사하는 것에 비해 확실하지는 않으나 비용이 적게 든다. 따라서, 주요 기업들은 직접 조사를 하되, 상대적으로 직접 조사의 필요성이 적은 기업들의 경우 개인정보관리책임자들의 감사 활동만이라도 감독할 필요가 있다.

라. 내부 교육

개인정보관리책임자는 사내의 개인정보 관련 업무 담당자들에게 적절한 교육을 시킬 의무를 가진다. 이는 자체적으로 실시할 수도 있고, 전문기관에 위탁하여 실시할 수도 있다.[75]

---

74) 위의 <표 30>에서 보듯이 A 쇼핑몰은 감사 권한을 경영지원부서의 권한으로 두고 있다.

75) 개인정보보호지침(2002.4)

제25조(교육) ① 서비스제공자등은 개인정보의 수집 또는 관리업무를 담당하는 직원에게 이용자의 개인정보를 보호하기 위하여 필요한 교육을 실시하여야 한다. 이 경우 개인정보관리책임자는 교육내용, 절차 및 방법 등 교육의 실시에 관하여 필요한 지침을 수립하여야 한다.

② 서비스제공자는 제1항의 규정에 의한 교육을 자체적으로 실시하거나 해당 분야의 전문기관에 위탁하여 실시할 수 있다.

조사대상 기업 중 B 은행은 월 1회별로 정보보호 교육을 실시한다고 답했으며, A 보험사는 분기별 1~2회 사이버 교육을 실시하고 있었다. 쇼핑몰 A, B는 모두 연 2회 이상 교육을 실시한다고 밝혔다. 쇼핑몰 A의 경우 정기적으로 실시하는 교육은 한국정보보호진흥원(KISA)에 위탁을 하고 있었으며, 신입사원 채용 등의 경우 수시 교육을 실시하고 있다고 답했다. A 포털/커뮤니티의 경우 연 1회 교육을 실시하고 있었다.

A 은행과 A 증권사는 정기적 교육은 없으나 수시로 교육을 진행한다고 밝혔다. 특히, A 은행의 경우에는 정기 교육은 없지만, 금융감독위원회에서 금융실명확인 및 비밀보장에 관련된 지침을 전달할 때마다 교육이 이루어진다고 한다. 개인고객부에서 각 지점에 관련 지침을 공문을 통해 내용을 내려보내면, 각 지점에서 창구 직원들에게 교육을 실시한다.

대부분의 기업에서 신입 사원에 대한 개인정보 교육을 실시한 후 업무별 교육을 실시하고 있었다. A 포털/커뮤니티의 경우, 신입사원에 대해서는 3일간 개인정보 관련 교육을 실시하고 이후에는 담당 업무별로 1일간 간단한 교육을 실시한다고 밝혔다. 반면에 소규모 기업인 A 언론사의 경우 특별히 교육을 실시하지는 않고 있었다.

마. 내규 및 지침 수립 여부

조사 대상 기업 중 쇼핑몰 2곳은 개인정보 보호와 관련된 내규를 제정하고 있었다. 이는 지난 2002년 정보통신부의 요청에 따라, 한국정보통신산업협회와 개인정보관리책임자협의회가 공동으로 쇼핑몰에 대한 개인정보 가이드라인을 만들면서 이루어진 일이라고 한다.

그 외에, A 포털/커뮤니티는 내부 매뉴얼에 따라, A 증권사는 HOST 정보보호 지침, 서버 지침, 네트워크 지침, 응용시스템지침, DB지침, PC지침, 관리적 지침, 물리적 지침 등 상세한 목차를 담은 매뉴얼에 의해 개인정보를 관리했다. A 은행의 경우 전산업무 관리 지침과 예금별 규정집 등에 따라 개인정

보를 관리했다. 지침이나 내규를 가지고 있지 않은 곳은 전혀 없었다.

바. 고객 고충·불만의 발생 건수와 주요 내용

B 포털/커뮤니티는 하루 100건 정도의 개인정보 관련 민원을 접수하고 있었다. 그 중 주민등록번호 도용과 관련된 민원이 월 100여건에 달했다. 반면, A 언론사의 경우 하루 평균 25건 정도의 개인정보 관련 고충·불만이 접수된다고 했으나, 그 중 실제로 ID나 주민등록번호 등이 도용된 경우는 1주일에 2~3건 정도에 불과했다고 답했다. 특히, 가족이나 친지 등에 의해 도용된 경우를 제외하면 그 수는 더욱 줄어 한 달에 3~4건에 그쳤다. A 쇼핑몰의 경우는 민원이 접수되는 경우가 하루 2건 정도밖에 되지 않으며 사고 발생 역시 2~3개월에 1건에 불과했다.

이는 쇼핑몰의 경우 회원 가입을 하지 않아도 서비스를 이용할 수 있기 때문인 것으로 보인다. 꼭 필요한 경우가 아니라면 회원 가입을 시키지 않는 것이 개인정보 관련 사고를 방지하는 것임을 새삼 확인할 수 있었다.

사. 애로사항

개인정보관리책임자들은 자율 규제가 잘 이루어지지 않는 원인에 대해 다양한 의견을 제시해주었다.

> "개인정보 보호를 잘 하려면 많은 돈이 드는데, 실제로 이 투자가 곧바로 이익으로 이어지지는 않습니다. 그렇다면, 마케팅 측면에서라도 도움이 되어야 기업이 이 분야에 투자를 할 것입니다. 문제는 유출 같은 사고에 대해서는 언론에서도 크게 떠들고 관심이 집중되지만, 개인정보 보호를 잘 했다고 해서 관심을 받지는 못한다는 점입니다. 그러니, 대부분의 기업들이 개인정보 보호에 투자를 하는 것을 성과 없는 투자라고 생각하게 됩니다." (A 쇼핑몰)

"개인정보 보호라는 게 아무리 대비를 잘 해도 아주 사소한 곳에서 사고가 발생하곤 합니다. 그런데, 평소에 열심히 하던 기업에서 사고가 나든, 전혀 개인정보 보호에 투자하지 않던 기업에서 사고가 나든, 보는 사람들은 똑같은 사고로 취급합니다. 분야는 다르지만 공정거래위원회에서 『공정거래 자율준수 프로그램』이라는 것을 운영하는데, 여기에 적극적으로 참여한 기업이 과실을 저질렀을 경우 과징금 감면 혜택을 줍니다. 똑같은 사고라 하더라도 노력을 안 해서 사고를 낸 기업이 더 크게 징벌을 받아야 합니다. 그렇지 않으면, 투자하려는 의욕이 생기지 않지요." (B 쇼핑몰)

이와 관련하여, 최근 i-safe 마크의 홍보 방식을 주목해볼 만하다. i-safe 마크는 한국정보통신산업협회가 실시하는 개인정보보호 우수기업 인증제도이다. 그런데, 전통적으로 해오던 i-safe 마크를 웹사이트에 게시하는 방식으로는 시민들에게 별로 홍보 효과가 없음을 깨닫게 되었다. 때문에, 최근 정보통신산업협회는 지하철에 i-safe 마크를 홍보하면서 인증받은 기업들을 함께 소개하기로 했다. 인증마크의 위상도 제고하고 인증받은 업체들에 대한 홍보 효과도 유발시키겠다는 것이다.

한편, B 포탈/커뮤니티의 개인정보관리담당자의 경우 개인정보 도용 방지를 위해서는 실명확인이 중요한데, 신뢰성 높은 실명확인 DB가 없다는 점을 문제로 삼고 있었다. 때문에 행정자치부의 주민등록DB를 개방하기를 원하고 있었다. 물론, 정확한 신원 확인을 원하는 기업의 입장에서는 그런 방식도 생각할 수 있겠으나, 이는 개인정보 보호의 측면에서는 오히려 바람직하지 않다.[76] 기업의 개인정보관리책임자들이 자기정보통제권에 대한 인식이 부족함을 알

76) 인터넷 실명제 논란의 와중에 행정자치부의 DB를 실명확인 용도로 개방하는 문제가 논의되자, 진보네트워크는 행정자치부의 주민등록 데이터베이스를 실명확인 용도로 사용하는 것은 목적외 사용이라고 지적한 바 있다. 진보네트워크센터 성명, 『인터넷 게시판 실명제가 노무현 정부식 '참여 민주주의'인가』, 2003.9.18. 진보네트워크센터는 성명과 더불어 행정자치부에 대해 공개질의를 했으며, 이에 대해 행정자치부는 민간에 실명확인 서비스를 제공할 계획은 없으나 공공기관의 확인 요청에 대해서는 신중히 검토할 것이라고 답했다. 진보네트워크 보도자료, 『행정자치부, "현재로서는 인터넷 실명제 계획 없다"』, 2003.10.9.

수 있었다.

아. 기타

언론사나 포털/커뮤니티의 경우, 게시물 작성자의 개인정보 보호 문제가 중요한 문제였다. 이는 표현의 자유와 연결되는 문제이기도 하다. B 포탈/커뮤니티의 경우 수사기관의 개인정보 제공 요청이 월 60여건에 달한다고 답했다. IP, 주민등록번호, 접속 시간, 메일 수신·발신 시간과 대상 등이 주요 요청 내용이었다.[77] 담당자는 수사협조의뢰서와 경찰관 신분증을 확인한 후 관련 자료를 제공하고 있으며, 제공 과정의 합법성에 대해 수사기관 감찰부서로부터 감사를 받고 있다고 답했다. 반면, A 언론사의 개인정보관리담당자는 월 평균 1회 정도 수사기관으로부터 게시판 게시물에 관한 개인정보 제공 요청을 받고 있었다. 특히 선거기간에는 이런 수요가 급증했다. A 언론사 개인정보관리담당자는 영장을 제시하지 않는 경우에 대해서는 개인정보 제공 요청에 응하지 않는다고 답했다. 개인정보 보호의 궁극적 임무를 맡고 있는 국가의 공권력이 스스로 규칙을 무너뜨리는 행위에 해당하는 만큼 이에 대한 각별한 조치가 필요하다.

3. 개인정보 보호를 위한 기술적 대책 수립 실태

개인정보의 보호를 위해서는 관리적 대책과 더불어 이를 구현할 수 있는 기술적 대책이 수립되어야 한다. 여기서는 각 기업들이 채택한 기술적 대책들에 대한 현황을 간략히 살펴보고 관련된 제도적 환경을 검토한다.

---

77) 이 정보들은 현행 통신비밀보호법상 통신사실확인자료로 분류되어 영장 없이 검찰이나 정보기관 요원들이 수집할 수 있다. 그러나, 통신사실확인자료 역시 통신비밀의 영역에 해당한다는 비판이 많다. 이은우, 앞의 책, pp. 87-88.

가. 개인정보 데이터베이스에 대한 접근권 설정 방식

개인정보의 유출 가능성을 최소화하기 위해서는 업무에 따라 데이터베이스에 대한 접근권을 적절히 설정하여 접근을 최소화하는 것이 중요하다. 접근권의 적절한 설정 방식에 대해서는 관리적 대책의 영역에서 다루었으나, 여기서는 기술적 측면에 대해서만 간단히 살펴본다. 금융기관 전자금융업무 감독규정 시행세칙에 따르면, 고객 데이터베이스에 대한 접근을 통제하기 금융기관들은 단말기에 대한 인증과 사용자에 대한 개인 인증을 하도록 되어 있다.[78)]

이를 위한 기술적 조치로서 금융기관들은 단말기에 고유번호를 부여하고 있으며, ID와 패스워드를 사용하여 개인 인증을 하고 있다. 다른 기업들도 ID와 패스워드를 통해 개인 식별을 하고 있으며, IP 주소를 통해 단말기를 식별하고 있다. 특기할 것은 은행권의 경우 관리자 카드를 통해 개인식별을 하고 있다는 점이다.

나. 결재시스템

전자상거래의 개인정보 보호에 있어서 가장 문제가 되는 것은 역시 전자결재 시스템이다. 다른 개인정보와 달리 결재정보의 유출·남용은 정보주체에게 직접적인 재산상의 피해를 가져다주기 때문에 문제가 특히 심각하다. 때문에, 안전한 결재시스템은 전자상거래의 발전의 핵심적 과제 중 하나이다.

조사대상 기업들의 전자결재시스템은 대동소이했다. 기본적으로 신용카드, 핸드폰 결재, ARS 전화 결재, 계좌이체 등이 거의 모든 기업에서 사용되고 있다. 신용카드를 통한 결재에 입력하는 정보 역시 주민등록번호, 카드번호, 사용 기한, 비밀번호 중 두 자리를 입력하는 것으로 통일되어 있다.

다만 몇몇 조사대상 기업이 채택하고 있는 '초고속통신 결재시스템'의 경우

78) 금융감독원의 금융기관전자금융업무감독규정시행세칙 제5조 단말기 보호대책 및 제6조 전산자료 보호대책을 참고할 것.

안전성에 다소 문제가 있었다. 초고속통신 결재시스템이란, 요금을 지불할 때 초고속통신 가입자임을 인증하면 이후 해당 통신사의 초고속통신 이용료에 포함되어 청구되는 방식이다. 이 때 인증은 아이디와 비밀번호, 주민등록번호만 입력하면 되도록 되어 있어 다른 결재 수단에 비해 도용의 가능성이 높은 편이다. 현재 한국통신의 메가패스 결재시스템을 프리챌, 세이클럽, 네띠앙, 엠파스의 4개 포털 사이트가 채택하고 있었으며, 하나로통신의 하나포스 결재시스템을 세이클럽, 엠파스, 네띠앙의 3개 포털 사이트가 이용하고 있었다.

신용카드를 통한 결재시스템의 경우, 해당 쇼핑몰이 수집하게 되는 정보는 카드번호와 사용 기한, 주민등록번호이다. 비밀번호 첫 두 자리의 경우 결재대행사가 수집하여 카드사의 인증을 받는 수단으로 사용되며 전자상거래 기업으로 전달되지는 않는다. 다만, 인터넷 쇼핑몰들의 경우에도 콜센터에서 전화 주문을 받는 경우가 있다. 이 때 창구 직원들에 의해 비밀번호가 유출될 가능성이 있다. 이를 방지하기 위해서는 홈쇼핑들이 채택하고 있는 자동응답(ARS) 시스템을 도입할 필요가 있다. 홈쇼핑들의 경우 ARS 시스템을 구축하여 비밀번호도 소비자가 직접 입력하도록 하고 있다. 그러나, 시스템 구축 비용상의 문제로 LG, CJ, 현대 등 쇼핑몰과 연계된 인터넷 쇼핑몰 외에는 이 시스템을 채택하고 있는 곳이 없다. 비용 문제를 극복하기 위해 기업들이 공동으로 ARS 결재 시스템을 구축하거나, 국가의 지원을 받는 방안 등을 고려할 필요가 있다.

한편, 일부 카드사는 최근 비밀번호 뿐 아니라 카드번호 자체를 보호하기 위해 ISP 결재 시스템을 채택했다. 이는 카드사가 직접 고객을 인증한 후, 인증 여부만 쇼핑몰·포털 등 전자상거래 기업에 알려주는 시스템이다. 때문에, 기업들은 이 시스템을 채택한 카드사 회원들에 대해서는 신용카드번호나 사용기한 등의 정보도 수집하지 않게 되었다. 현재 국민카드와 BC카드가 이 시스템을 채택하고 있다.

다. 온라인 뱅킹

온라인 뱅킹의 경우 조사대상 11개 은행이 모두 동일한 시스템을 채택하고 있다. 모든 기관이 로그인을 위해 공인인증서를 요구하고 있었으며, 자금 이체를 위해서는 보안카드와 이체비밀번호를 별도로 요구했다. 또한, 해킹으로 인한 정보 유출을 막기 위해 해킹방지 프로그램과 암호화 모듈을 자동으로 내려받도록 하고 있다.

라. CD/ATM 기기

올 들어 현금자동지급기(CD)와 현금자동입출금기(ATM) 등 오프라인 자동화기기와 관련된 정보 유출의 문제가 빈번히 발생했다. 오프라인 자동화기기의 경우 원칙적으로 기기에는 정보가 내장되지 않도록 되어 있어 소비자가 주의를 기울이기만 한다면 안전한 시스템으로 알려져 있었다. 그러나, 편의점, 백화점, 극장 등 금융기관 외부에 설치된 자동화기기의 숫자가 급증하면서 관리상의 문제점이 많이 발생하게 되었다. 상당수 자동화기기가 위탁 사업자들에 의해 운영되고 있으며, 이들이 또 가맹점 형태로 위탁을 하면서 사실상 커피자판기와 다를 바 없을 정도로 관리가 소홀해졌다.

그 중에서도 가장 문제가 되는 것은 도청을 통한 유출이다. 자동화기기 자체는 금융기관으로 정보를 송신하는 역할만 하고 있으나 자동화기기와 금융기관 사이의 회선을 도청하거나 자동화기기 내부에 데이터 리더기를 장착함으로써 정보가 유출되는 경우가 발생했다.[79]

금융감독원은 이 문제를 해결하기 위해 자동화기기와 금융기관 사이의 정보 송·수신을 암호화하여 수신하도록 하고, 자동화기기를 공급·관리하는 VAN(부가가치통신망) 사업자들의 경우 고객 정보를 수집하지 못하도록 조치를 취했다.[80] 그러나, 실제 자동화기기 설치나 운영에 대한 감독은 개별 은행에 맡

79) 2003년 5월 29일『디지털타임스』

겨져 있어서 엄격한 감독이 이루어지지 못한다는 비판이 있다. 이에 대해 금융감독원은 CD기 관리자를 전자금융거래법상 '전자금융보조업자'로 간주하여 직접 감독하고 나아가 사업자의 자격 제한 등 규제를 위한 법적 근거를 마련하겠다고 밝힌 바 있으나,[81] 아직 현실화되지는 않고 있다.

80) 금융감독원 보도자료, 『현금카드 복제사고관련 조치내용 및 대응책』, 2003. 5. 29.
81) 한국일보 2003년 7월 7일자.

4. 기업 담당자 면담 결과 기록

면접대상 기업	A 보험사	대상자 구분	개인정보관리담당부서원
주 요 내 용			

금융감독원의 지침, 법규에 따라 정보보호가 이루워진다. 법이 아니라도 신뢰의 문제이기 때문에 중요하게 정보보호 업무를 하고 있다. 정보보호메뉴얼을 갖고 있으며, 회사 기밀사항으로 취급되고 있었다.

준법감시부라는 부서가 있어서 개인정보보호 업무 뿐아니라 가타 문제들에 대한 내부통제를 실시하고 있다. 물론, 업무에 관한 감사는 다른 감사부서에서 받는다. 고객민원의 경우 개인정보보호 업무를 하고 있는 팀들이 업무를 숙지하고 있기 때문에 홈페이지상의 담당자가 아니더라도 적극적으로 민원에 대처하고 있다. i-safe, e-privacy 마크 인증을 갖고 있다.

개인정보관리책임부서는 온라인 담당 부서에서 맡고 있었다. 각각의 정보보호 업무를 담당하는 구성원들 사이의 정기적인 미팅은 없지만 어떤 사안에 따라서는 정보를 공유하기 위한 회의가 열리기도 한다.

직원들을 상대로한 정보보호 교육 안에 개인정보보호 내용이 있으며 분기마다 한, 두차례 사이버 교육이 진행되고 있다. 개인정보관리책임자는 시스템적인 관리책임을 맡고 있으며, 소소한 것들은 민원실에서 처리하고 있었다.

그러나, 회사내의 개인정보보호 책임자가 웹상에 있음에도 그 책임자가 누구인지 알지 못했던 것으로 보아 개인정보보호 업무라인의 최종 책임자가 형식적이지 않을까 하는 의문이 든다.

면접대상 기업	A 증권사	대상자 구분	개인정보관리책임자
주 요 내 용			

개인정보관리책임자는 시스템적인 관리책임을 맡고 있으며, 소소한 것들은 민원실에서 처리하고 있었다.

증권사의 경우 신속성이 중요하기 때문에 개인정보 보호를 비롯해 완벽한 보안을 갖추는 것이 쉬운 일은 아니지만, 다른 한편 신용이 핵심이므로 중요성에 대한 인식은 높았다. A 증권사는 금융감독원의 감독을 충실히 이행하고 있다고 답했다.

정보보호메뉴얼은 회사 기밀사항이므로 목차만 확인시켜주었다. ▲ 2000 정보보호지침 ▲ 정보보호정책 ▲ HOST정보보호지침 ▲ 서버지침 ▲ 네트워크지침 ▲ 응용시스템지침 ▲ DB지침 ▲ PC지침 ▲ 관리적지침 ▲ 물리적지침 등으로 구성되어 있었다. 물리적 지침에 따라, 설문조사나 방문도 엄격히 제한되며 접견실도 따로 마련하고 있었다.

기술적으로는, PK인증을 실시하고 있었으며, 비밀번호나 계좌번호 등은 DB에서 암호화처리되므로 보안이 취약하지 않다고 강조했다. 오프라인 문서들도 보안 조치를 취하고 있으며, 독립적인 방에 모아 놓는다.

담당자들은 개인정보 보호에 대한 자신감이 높았다. 정보보호책임자들은 CISA(보안감사), PMP(전산프로젝트) 자격증을 취득하도록 되어 있었다. 관리책임자의 임기가 따로 규정되지는 않았으며, 전문성을 관리책임자의 조건으로 하고 있었다. 면접자는 2년 동안 관리책임자로 일하고 있었다. 2년 전 경실련으로부터 개인정보보호 우수 기업으로 선정되기도 했었다.

개인정보와 관련해 아웃소싱은 이루어지지 않고 있었다. 다른 일부 증권사 중에 DB를 아웃소싱하는 경우가 있으나 계열사에 맡기는 것이라고 설명했다. 아무에게나 생명줄인 정보들을 맡길 수는 없다는 것이었다.

BS7799 인증 가입에 대한 의향을 묻자, 금감원의 지침 수행만으로도 상당히 강한 보호 업무를 하는 것이며, 또한 BS에 버금가는 ISAC(보안 컨설팅)을 받으므로, 더 많은 돈을 투여할 의미는 없다고 보고 있었다.

보안 및 개인정보 보호 관련 교육은 수시로 진행되고 있었으나, 정기 교육은 없었다. 모든 사람에게 매뉴얼 전체를 숙지하게 할 수는 없으므로, 담당업무에 따라 교육하고 있었다. 내부 감사도 진행되고 있었다.

면접대상 기업	A 은행	대상자 구분	전산담당자
주 요 내 용			

웹페이지 상의 개인정보관리책임자는 은행 전반의 개인정보 문제에 대해서는 별로 아는 바가 없었다. 은행 전체를 대상으로 개인정보 관리를 책임지는 관리책임자는 따로 없었으며, 상대적으로 전산담당부서가 전반적인 관리 실태에 대해 가장 잘 파악하고 있었다. 현장의 개인정보 관리를 실제로 감독하는 임무는 지점장이 맡고 있었다.

창구 직원들은 개인정보에 대한 접근권을 갖고 있지 않았다. DB에 대한 접근은 고객으로부터 비밀번호를 받은 경우에만 가능했으며, 이 경우에도 저장, 출력 등은 금지되어 있었다. DB 일반에 대한 접근은 지점별로 부점장이 관리하는 책임자카드를 통해서만 가능했다. 카드 사용 내역은 감사 대상 자료로 보관하도록 되어 있다. 또, DB에 접근하더라도 비밀번호는 암호화되어 있어 유출될 수 없다.

출금 내역서 등 오프라인 문서는 5년간 보관한다. 보안을 위해 넘버링을 통해 대조를 하게 하고 있으며, 보안장치가 되어 있는 금고에 보관하게 되어 있다.

각 예금별로 규정집이 있다. 이 규정집들과 전산업무관리지침에 따라 정보보호 활동을 수행한다. 지점에 대해서는 본점 검사부가 감사를 하며, 본점에 대해서는 감사원이 감사를 한다. 교육의 경우 정기적으로 진행되지는 않으며, 재정경제부로부터 관련 공문이 내려올 경우, 금융실명제를 담당하는 개인고객부에서 지점으로 공문을 다시 내려보낸다. 그러면, 지점에서 현장 교육을 실시한다.

면접대상 기업	B 은행	대상자 구분	개인정보관리책임자
주 요 내 용			

B은행의 경우 담당책임자가 임무를 최근에 부여받았기 때문에 현재의 업무를 파악하고 있지 못한 상태였기 때문에 하급자와의 상담이 이루어졌다. 이것으로 유추할 수 있는 것은 정보보호책임자가 전문적 코스를 거쳐 임명되는 것이 아님을 알 수 있다. 개인정보관리책임자는 시스템적인 관리책임을 맡고 있으며, 소소한 것들은 민원실에서 처리하고 있었다.

인터넷 웹 개인정보보호 책임자는 공식적으로 명시되어 있지만, 다른 분야들은 나타나 있지 않았다. 다만, 각 부서의 장이 보안, 보호 업무를 하고 있고 시스템적인 부분에 관한 보안책임자가 있다고 한다. 임원급의 개인정보보호 책임자가 명시적으로 존재하지 않았다. 각 정보보호를 담당하는 책임자 혹은 담당자들의 정기적인 미팅은 없다고 했다. 면접자는 웹이 아닌 영역에서의 정보보호에 대한 정보를 잘 알고 있지 않았다. 상호간의 정보보호 업무를 특별히 교류하지 않고 있음을 알 수 있었다. 다만, 제3의 기관으로부터 보안 컨설팅을 받으면서 보다 체계적인 정보보호업무를 구축 중에 있다고 했다. 그 과정에서 지적된 부분들을 고쳐나가겠다고 했지만 지적사항들이 무엇인지에 대해서는 알려주지 않았다. 지적 사항들이 수정되면 개인정보보호 인증마크를 향후 신청할 계획이라고 했다.

회사 기밀이라는 이유를 들어 정보보호 매뉴얼 목차조차도 공개하지 않아서 세부적인 내용을 파악할 수 없었다. 개인정보보호에 대한 민원처리는 민원업무를 보는 곳에서 처리하기 때문에 책임자가 직접적으로 민원을 상담하는 사례는 없다고 했다.

자체 감사가 있으며 월 1회마다 정보보호 교육을 진행시킨 다고 했지만 교육의 내용 중에 개인정보보호에 대한 중요도가 어떻게 반영되는지 불확실했다.

면접대상 기업	A 카드사	대상자 구분	개인정보관리담당부서원
주 요 내 용			

개인정보관리책임 담당부서는 마케팅팀이었다.

개인정보보호 업무를 진행하면서 어려움이 있다면 이용자들의 보안관리가 아쉽다는 것이다. 본인의 부주의로 가족과, 친지 등에 의해서 발생하는 문제들이 많은데 이러한 부분들은 이용자 스스로 자신의 정보를 보호해야 한다.

금융감독원으로부터 지적 받은 적이 없을 만큼 정보보호는 확실히 지켜진다고 자부한다. 회원 정보를 아웃소싱하지 않으며 홈페이지 상에 제휴된 사이트들은 콘텐츠 제휴일 뿐 회원정보를 공유하는 것은 아니다. 담당 부서에 발령을 받으면 개인정보보호 업무는 부가된다. 정보보호, 보안, 개인정보보호 담당자 사이의 부정기적인 회의가 있다. 정보보호 업무에 대한 자체 감사가 당연히 있으며 금융감독원의 감독도 받고 있다. 내부 교육은 콜센터 사원들에 대해서는 수시로 진행되고 있지만 전체 사원 대상의 교육은 신입사원교육 이외 특별히 없다.

면접대상 기업	A 쇼핑몰	대상자 구분	개인정보관리책임자
주 요 내 용			

고객관리부서장이 개인정보보호책임자를 맡고 있었다. 임원급은 아니었으나, 개인정보 관련 권한은 모두 위임받고 있으며, 개인정보관리책임자 결재가 없으면 일을 진행하지 않도록 되어 있다고 한다.

관련 내규를 제정하고 있었다. 정보통신부에서 쇼핑몰 분야 개인정보 가이드라인을 만들면서 그 결과로 내규까지 제정하게 되었다고 한다. 관련 교육은 정기 교육과 수시 교육으로 나뉘어졌다. 정기 교육은 KISA에 위탁하여 연 2회 2시간씩 전 사원을 대상으로 진행하며, 수시 교육은 신입사원 입사 등의 경우에 자체 진행한다. 연 1회 정기 감사도 진행된다. 교육 및 감사권은 경영지원부에 있는데, 이는 회사에 별도의 감사실이 없는 상황에서 경영지원부가 감사실의 역할을 하고 있기 때문이라고 했다.

전화 구매의 경우 상담원들이 고객의 개인정보를 듣게 되지만, 일단 입력하고 나면 DB에 접근할 수 없으므로 유출 우려는 낮다고 한다. 주문 취소의 경우, 컴퓨터에서 취소키를 누르면 결재처리 담당자에게 통보되는 방식으로 처리하므로, 상담원이 결재 관련 정보를 들을 일은 없다고 답했다.

DB에 대한 접근권은 몇 단계로 구분되었다. 고객 상담원의 경우, 성명・이름・주소 등을 열람할 수 있으며, 대금결재 관련 정보는 개인정보관리책임자・담당자와 결재처리 담당자만 확인 가능하다고 한다. 마케팅 부서에서는 ID와 이름 정도만 열람가능하다.

상담원들은 용역업체에 아웃소싱을 하고 있었다. 그러나, DB가 유출되지 않도록 회사 건물 내에서 근무하게 되어 있었으며, 담당 업체는 물론 상담원 개개인에게 개인정보 보호에 관한 서약서를 받는다고 답했다. 물론, 상담원들은 교육도 받고 있었다.

개인정보 관련 민원은 하루에 2건 정도에 불과했다. 그 중 ID나 주민등록번호 도용을 비롯한 사고는 한 달에 한 건도 안 된다고 한다. 그나마, 가족・친지 등의 도용을 제외하면 실제적인 도용은 거의 없었다고 답했다.

애로사항을 묻자, 개인정보 보호에 투자가 많이 필요한데 수익성에는 별로 도움이 되지 않는다는 점을 지적했다. 마케팅 측면에서라도 도움이 되어야 하는데, 유출 같은 사고만 언론에 크게 날 뿐 잘 했다는 이유로는 주목을 받지 못한다고 한다. 때문에, 기업 측에서는 투자할 의욕이 안 생기는 점이 문제라고 한다.

여러 곳에서 우수 사이트로 선정되고 있었다. 다른 기업들이 왜 인증을 안 받으려 하는지를 묻자, 돈이 많이 드는데 소비자 유치 효과는 별로 없다는 문제점을 지적하면서, 정부와 소비자 단체가 공동으로 제대로 된 마크를 만들고 적극적으로 홍보하면, 참여의 유인이 생길 것이라고 답했다.

면접대상 기업	B 쇼핑몰	대상자 구분	개인정보관리책임자
주 요 내 용			

내규와 교육 자료를 받을 수 있었다. 교육 자료는 KISA에서 제작된 자료와 자체 발생 사례를 모은 자료로 구성되어 있었다. 두 자료 모두 사례 중심으로 구성되어 있었다. 다양한 사례를 통해 설명하고 있어 실제 고객의 민원에 대처하는 데 도움이 될 것으로 보였다.

개인정보관리책임자가 고객 민원 처리, 개인정보 보호 교육, 관련 감사, DB 접근권한 설정 등 개인정보 관련 업무 전반을 담당하고 있었다. 개인정보의 수집, 이용, 제공 관련 업무도 개인정보관리책임자의 업무로 되어 있었다. 교육과 감사는 각각 연 2회, 연 1회 실시되고 있었다.

내부 방화벽을 설정하여 DB를 보호하고 있었으며, 고객 DB에 대한 접근자는 물론, 열람이나 제공 요청에 대해서도 기록을 남기고 있었다. DB 열람을 위해서는 현장 직원이 담당 부서와 개인정보관리책임자의 승인을 받도록 하고 있었다. 한편, 주민번호 뒷자리와 비밀번호는 암호화하여, 열람 승인을 받은 직원들도 볼 수 없도록 하고 있었다.

개인정보관리책임자협의회에도 주도적으로 참여하고 있었다. 때문에 애로사항을 묻자 B쇼핑몰이 아닌 전체 업계 차원의 답변을 했다. 아무리 개인정보 보호를 잘 해도 아주 사소한 곳에서 사고가 발생하는 경우들을 막을 수 없다고 했다. 그런데, 평소에 열심히 하던 기업이나 전혀 투자하지 않던 기업이나, 사고가 나면 똑같이 취급받는다는 것이다.

그는 공정거래위원회의 『공정거래 자율준수 프로그램』 같은 방식을 대안으로 제시했다. 평소에 개인정보 보호 프로그램에 적극적으로 참여한 기업의 경우, 과실이 발생하더라도 과태료나 과징금을 감면해주자는 것이다. 그렇지 않으면, 잘 하던 기업조차 투자 의욕이 떨어진다는 것이다.

또한, 규모가 있는 기업들만이 주로 규제의 대상이 되고 있다는 점도 문제로 지적했다. 사실 어느 정도 인지도가 있는 기업들은 기업 이미지상 보호 노력을 할 수밖에 없다는 것이다. 반면 취약한 곳들은 중소형 기업들이므로 이들에 대한 적극적 교육과 홍보가 필요하다고 지적했다.

면접대상 기업	A 포털/커뮤니티	대상자 구분	개인정보관리담당자
주 요 내 용			

부사장이 개인정보관리책임자를 맡고 있다고 한다. 관리책임자는 정식 발령을 받으며 임기는 1년으로 규정되어 있었다. 특이한 점으로는 다른 기업에서 대개 고객관리팀에서 개인정보관리담당자를 지정하는 반면, A 포털의 경우 개인정보관리담당자가 법무팀 소속이었다.

콜 센터에서의 개인정보 유출 가능성을 묻자, 모든 개인정보 관련 민원을 기계적으로 처리하도록 되어 있어 직원들의 DB 접근은 아예 금지되어 있다고 한다. 때문에, 콜 센터를 통한 유출 가능성은 전혀 없다고 대답했다. 기계적으로 처리되다보니 특별히 민원에 대한 통계는 갖고 있지 않았다.

개인정보 DB에 대한 로그 기록을 유지하고 있었으며, DB에 접근가능한 IP를 따로 배정하고 있다고 답했다. 직위별, 서비스별로 DB에 대한 접근 제한이 이루어지고 있었다.

개인정보 관련 교육은 연 1회 자체적으로 진행하고 있었다. 신입사원 교육 시에는 3일간 실시되며, 이후 업무가 배정될 때, 혹은 변동될 때 수시로 담당 업무에 관한 개인정보 보호 교육이 이루어진다고 한다. 감사의 경우 감사위원회가 별도로 설치되어 있어 감사를 담당하며, 연 2회 이루어졌다.

면접대상 기업	B 포털/커뮤니티	대상자 구분	개인정보관리담당자
주 요 내 용			

개인정보관리책임자는 부사장이 맡고 있으며, 담당자가 일선에서 관련된 업무를 수행한다. 법적, 정책적으로 중요한 사안의 경우 주1회 보고를 통해 결재를 맡는다고 한다. 사내 정책의 경우 담당자가 발의하고 부서의 부장과 관리책임자의 결재를 받는다. 관리책임자에 대한 정식 발령이나 임기 규정은 없다.

현재 관리담당자를 포함하여 9명의 상담원이 개인정보 관련 상담을 맡고 있다. 이들에 대해서는 DB에 대한 열람과 비밀번호 수정이 허용되었다. 개발자 2명은 DB 전체에 대한 수정이 가능했다. DB에 접근할 수 있는 IP를 제한하고 있으며, 패스워드를 설정하고 있었다. 그러나, 패스워드가 개인별로 부여되는 것이 아니라, 하나의 패스워드를 9명의 상담원이 공동으로 사용한다고 한다. DB 접근에 대한 로그 기록은 유지하고 있었으며, DB를 별도로 저장하는 것은 기술적으로 금지되어 있다.

개인정보 보호에 대한 내규는 없으나, ▲ 회원 개인정보는 절대 비밀 ▲ 정식 공문을 통한 수사협조 요청에는 응할 것 등을 지침으로 하고 있다고 답했다. 월 평균 60건 정도의 수사협조 요청이 있으며, 이 경우 수사협조 의뢰서 양식과 경찰관 신분증을 확인하여 개인정보를 제공하고 있었다. 제공되는 내용은 주로 메일 사용 내역, 접속 시간, 주민등록번호, IP 등이 있다고 한다. 정보통신윤리위원회의 경우 게시물 삭제 등을 요청하기는 하나 개인정보를 요구하는 경우는 없다고 답했으며, 개인정보 관련 사건 조사와 관련해 KISA에서 요구하는 경우는 있다고 답했다. 명예훼손 등 회원간 분쟁에 대해서는 회사가 중재를 하나, 이 때 분쟁 당사자에게 상대방에 대한 정보를 알려주지는 않는다고 답했다.

특별히 내부 감사는 없으나, 년 2회 DB에 대한 점검을 하고 있다고 한다. 외부 감사로는 수사협조 의뢰가 합법적으로 이루어졌는지에 대한 수사기관 감찰팀의 감사가 있었다. 교육은 상담직원들에 대한 상담 교육과 병행하여 자체적으로 이루어지고 있는데 연간 10시간 정도 진행되었다. 한편 관리담당자의 경우 KISA 등에서 진행하는 교육에 참여했다.

개인정보 관련 민원은 하루 약 100건 정도 접수되며, 그 중 주민등록번호 도용과 관련된 민원은 약 100여건 정도라고 한다. 이 문제를 해결하기 위해서는 실명 확인이 필요한데, 신뢰할만한 DB가 없는 것이 문제라고 답했다. 현재로서는 1차 : 한신평 DB를 통한 확인과정과 2차 : 타 사 DB와의 대조를 통한 확인을 함께 실시하고 있으며 이 두 과정에서 모두 실명확인이 된 경우에만 가입을 시키고 있는데, 10대의 경우 실명확인이 어렵다는 문제가 있다고 답했다. 때문에 행자부의 주민등록DB 개방이 필요하다고 보고 있었다.

면접대상 기업	A 언론사	대상자 구분	개인정보관리담당자
주 요 내 용			

개인정보관리책임자는 상무이사가 겸임하고 있었다. 그러나, 개인정보관리담당자는 웹사이트 회원 관리만을 담당하고 있었다. 소속은 원래 컨텐츠팀이었으나, 최근 회사 조직 개편과 함께 마케팅팀으로 옮겨졌다고 한다. 함께 운영되는 여행사나 쇼핑몰 등의 텔레마케팅에 사용되는 개인정보에 대해서는 권한을 갖고 있지 않았다.

콜 센터가 운영되고 있는데, 콜 센터 직원들은 회원 DB에 접근하는 것도 불가능하다고 한다. 오직 사업별 웹사이트 관리자만 회원 DB에 접근할 수 있는 ID를 부여받고 있었으며, 이것도 열람만 할 수 있게 되어 있었다. 개인정보 DB를 수정하는 작업은 개인정보관리담당자만 할 수 있도록 되어 있었다. 그러나, 로그 기록은 남기지 않고 있었다.

관리담당자만 DB 수정 업무를 할 수 있다보니 예상치 않은 문제가 발생했다. 담당자가 자리를 비울 경우, 회원들의 긴급한 민원을 처리해줄 수 없는 경우가 발생한다는 점이었다. 개인정보 관련 민원은 하루에 대략 25~30건 정도가 들어오는데, 그 중 주민등록번호 도용 같은 유의미한 민원은 주당 2~3건 정도밖에 없다고 한다. 그것도 대부분 가족, 친지 등에 의한 도용이어서, 실제로 도용되는 경우는 월 3~4회에 불과할 것이라 대답했다.

나머지 대부분의 경우는 예전에 가입했으면서도 그 사실을 모르는 채 도용당했다고 생각하는 경우라고 답했다. 이용자들이 자기 정보를 스스로 잘 관리하지 못하는 것이 개인정보관리담당자의 업무를 늘리는 요인이라고 지적했다.

한편, 개인정보 취급자가 거의 없다보니, 교육이나 감사는 진행되지 않고 있었다. 외부 감사로는 분기별로 정보통신부에 보고하는 일이 있다고 한다. 내규도 없으나 정보통신부지침과 통신업무관리지침을 따르고 있다고 답했다.

특이한 것으로는 언론사이기 때문에, 게시판에 게시물을 올린 이용자들에 대한 정보요구가 수사기관이나 선관위 등에서 자주 온다고 한다. 대개 월 1회 정도 요청이 들어오지만 선거기관에는 급증하는 편이며, 이 경우 영장을 달라고 요구하고 있었다.

Ⅵ. 국내외 개인정보 보호 법제에 대한 검토

1. 종합적 검토

가. 개인정보일반법의 필요성

1) 개인정보 보호법제의 체계 분류

<표 31> 각 국의 개인정보보호법제 유형

유형	옴니버스 방식		영역별(Segment) 규율방식	분야별(Sector) 규율방식
	공/사 영역 동일 기준	공/사 영역 별도 기준		
내용	하나의 법률에 공적 영역과 사적 영역을 규제하는 법률을 모두 포괄하는 일반법 제정, 통합된 감독기구 설치됨		공적 영역의 일반법과 사적 영역의 일반법을 구분하여 제정. 감독기구가 분리.	개별 이슈에 따른 규제 법률 제정. 각 이슈별로 보호기구 설치됨.
장점	·사각지대를 없앰 ·인권 존중 원칙에 충실	·사각지대를 없앰 ·시장 영역의 특성 다소 고려	·사각지대를 없앰 ·시장 영역 특성 고려 수준 높음	·기술 발전 양상에 신축적으로 조응 ·분야별 특수성을 충분히 반영
단점	·시장 영역의 특성을 고려하지 못함. ·기술변화에 대한 적응력 부족 ·선언적 규정에 그침으로써, 보호 수준이 오히려 낮아질 위험	·기술 변화에 대한 적응력 부족 ·민간 영역에 대해서는 여전히 선언적 규정에 그칠 위험성	·기술 변화에 대한 적응력 부족 ·민간 영역에 대해서는 여전히 선언적 규정에 그칠 위험성 ·인권적 측면 고려 부족	·일반 원칙의 부재 ·사각지대가 많음
채택 국가	스웨덴, 프랑스, 벨기에, 영국 등	독일 등	일본, 캐나다, 호주 등	미국, 한국 등

개인정보 보호법제의 체계는 각 국가별로 개인정보 보호의 역사가 발전해온 방식에 따라 다르게 나타난다. 이를 유형별로 분류하면 크게 <표 31>과 같이 구분할 수 있다.

일반적으로 지적되는 옴니버스 방식이나 영역별 규율 방식의 장점은 사회 모든 구성원을 대상으로 법률이 집행된다는 점이다. 따라서 보호를 받지 못하는 영역이 없게 되는 반면 일반법이므로 구체적 이슈에서 나타나는 다양한 침해 양상에 정확하게 대응하기 어렵다는 문제가 발생한다. 반대로 분야별 규율 방식은 기술 변화에 따라 나타나는 구체적 문제에 대한 해결책을 제시한다는 장점이 있는 반면, 법률의 보호를 받지 못하는 분야가 너무 많다는 문제점이 발생한다.

영역별 규율 방식과 옴니버스 방식 중 공공/민간 영역을 구분하여 규율하는 방식은 법이 구분되어 있느냐, 통합되어 있느냐의 차이일 뿐, 민간 영역과 공공 영역의 규율 원리가 서로 다르다는 인식에 기초하고 있다는 점에서 유사한 성격이 많다. 다만, 옴니버스 방식을 채택할 때는 공공·민간 영역을 단일한 감독(보호) 기구에서 감독하는 것이 일반적이다.

2) 국내의 개인정보보호법제 체계의 현황과 문제점

국내에도 프라이버시 보호를 위한 여러 가지 법률이 제정되어 있다. 먼저 공공 영역의 일반법으로 「공공기관의개인정보보호에관한법률」이 있다. 민간 영역의 경우 「정보통신망이용촉진및정보보호등에관한법률」이 일반법적 내용을 담고 있으나, 정보통신서비스제공자, 학원·항공·여객·숙박 등 몇몇 제한된 분야를 중심으로 적용되고 있어 한계가 많다. 또한, 이 법은 목적 자체가 정보통신망 이용 촉진과 네트워크 보안, 개인정보 보호라는 서로 다른 문제들을 하나로 엮고 있어서 일반법으로 기능하기에 문제가 있다. 그 외에 분야별 법률로, 「신용정보의이용및보호에관한법률」, 「금융실명거래및비밀보장에관한법률」, 「통신비밀보호법」과 「위치정보의보호및이용에관한법률(안)」 등이 제정되

어 있거나 혹은 준비되고 있으며, 「여신전문금융업법」, 「의료법」, 「주민등록법」, 「전자상거래등에서의소비자보호에관한법률」, 「방문판매등에관한법률」 등 개인정보 보호를 목적으로 하지 않는 법률들에도 개인정보 보호와 관련된 조항들이 일부 포함되어 있다.

한국의 개인정보 보호법제는 분야별 입법 체계를 갖고 있다고 분류할 수 있겠다. 그런데, 이러한 법률 체계는 여러 가지 문제점을 안고 있다.

첫째, 개인정보 보호의 사각 지대가 많다. 현재 법률에서는 민간의 도서/비디오 대여 기록이나 기업이 보유한 직원 인사 기록 등은 현실적으로 보호받기 어렵다. 부동산 거래 기록이나 사회복지대상자의 정보 등은 부동산 중개업법이나 사회복지사업법 등 각 분야별 법률에 '비밀을 지킬 의무'라는 단 하나의 조항에 의해 보호되어지고 있다. <표 32>에서 확인할 수 있듯이, 보호의 필요성이 특히 큰 의료 정보조차 의료법 상의 비밀누설 금지 조항 단 하나에 의해 보호되고 있다.

<표 32> 의료정보의 관련법령의 체계

의료법	비밀누설금지(제19조) 환자기록의 열람·사본교부 등 내용확인 금지(제20조1항) 3년 이하의 징역 또는 1천만원 이하의 벌금, 친고죄
응급의료법률	응급구조사의 직무상 지득한 비밀누설금지(제40조) 3년 이하의 징역 또는 1천만원 이하의 벌금, 친고죄
의료기사법률	비밀누설금지(제10조) 3년 이하의 징역 또는 1천만원 이하의 벌금, 친고죄
의료보험법	업무상 알게 된 비밀의 누설 금지(제79조) 1년 이하의 징역 또는 1천만원 이하의 벌금
전염병예방법	건강진단 등 전염병 관련 업무상 지득한 타인의 비밀누설금지(제54조의6) 3년 이하의 징역 또는 1천만원 이하의 벌금(제55조 1항)
AIDS예방법	감염자에 관하여 직무상 알게 된 비밀의 누설 금지(제7조) 3년 이하의 징역 또는 1천만원 이하의 벌금(제26조)

출처 : 정영화, 『개인정보보호 감독기구 도입을 위한 법제도 개선방안 연구』, 서울 : 한국정보보호센터, 2000, p. 52.

둘째, 첫 번째 문제점과 연결되는 것으로서 정보 보호를 목적으로 제정된 몇몇 법률을 제외하면 보호 조항 자체가 부실하다. 개인정보를 보호하기 위해서는 단순히 유출을 금지하는 것만으로는 부족하다. OECD가 제정한 「개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인」에서 규정하고 있는 수집 제한의 원칙과 이용 제한의 원칙, 목적 명확화의 원칙, 개인 참가의 원칙, 공개의 원칙 등이 정보 주체의 권리와 정보 수집자의 의무로 부과되어야 한다. 그러나 대부분의 법률이 '비밀 보호 의무' 정도로 규정하고 있어 정보 주체의 다양한 권리들이 보장되지 않고 있다.

셋째, 대부분의 개인정보 침해는 온라인 상에서만 발생하는 것이 아니라, 오프라인 상에서도 발생한다. 그러나 「공공기관의개인정보보호에관한법률」, 「정보통신망이용촉진및정보보호등에관한법률」 등 비교적 잘 정비된 보호 법률들은 주로 온라인 상의 개인정보 보호 문제만을 다루고 있다.

3) 문제 해결 방안

현재 한국의 개인정보 보호법제 체계가 지니고 있는 문제점은 분야별 보호 체계를 택하고 있기 때문에 발생하는 문제들이다. 따라서 이 문제들을 해결하기 위해서는 온라인과 오프라인 구분 없이 공공 영역과 민간 영역의 구분 없이, 누구나 지켜야 할 개인정보 보호 원칙을 천명하는 일반법을 제정하는 것이 필요하다.

일반법 체계에 대해서는, 공공 영역과 민간 영역의 규율 원리가 다른 현실을 무시한다는 비판이 있다. 그러나 공공 영역에서든 민간 영역에서든, 침해받는 법익이 다른 것은 아니다. 정보 주체의 동의나 정보 주체의 대표자들로 구성된 의회가 결의한 법률에 의하지 아니하고서는 개인정보를 수집할 수 없다는, 자기정보 통제권의 일반 원칙이 달라지는 것도 아니다.[82] 따라서, 국내 개

82) 이인호, 『토론 : 프라이버시보호 감독기구의 독립성 확보의 필요성』, 『함께하는 시민행동 연속 워크숍, 제2회 프라이버시 감독체계의 개선방안 모색』(2003.8.21) 자료집

인정보 보호법제도 일반법 체계가 기본이 되어야 한다.

그러나 일반법을 제정하는 것이 현재의 개별 법률들을 없애는 것을 의미하지는 않는다. 오히려 개별 법률들을 없애고 일반법으로 통합하는 것은 하루가 다르게 변화하는 기술 발전을 따라잡지 못하는 문제점을 야기할 수 있다. 일반법의 경직성을 탈피하기 위해서는 분야별 입법을 통해 해당 분야에 맞는 세부적 보호 방식을 규정하는 것이 바람직하다.

다시 말하면, 일반법에서 개인정보 보호를 위해 누구나 지켜야 할 일반 원칙을 천명하고, 이 원칙만으로는 적절하게 보호받기 어렵거나 다른 방식의 보호가 필요한 분야에서는 분야별로 개별 입법을 제정하는 것이 양 쪽 방식의 문제점을 공히 해소하는 방식이다.

개인정보보호를 위한 보다 합리적인 방안을 찾는 과제는 개인정보보호에 관한 법률의 개정 및 제정과 정보보호의 주체로서 적절한 개인정보보호 기구의 설립으로 모아질 수 있다. 우선 개인정보보호에 관한 법률을 검토하고 이어서 개인정보보호 기구의 설립에 관해 논의해 보기로 한다.

나. 개인정보 일반법의 주요 내용

1) 주요 국가의 개인정보보호 원칙

각 국가별로 부분적 차이는 있지만, 개인정보보호법제를 갖춘 주요 국가들은 OECD 가이드라인에서 제시하고 있는 8원칙을 담는 개인정보보호법률을 제정하고 있다.

가) 프랑스의 정보처리(파일)자유에관한법률

공공기관이 법령에 명시되지 않은 개인정보 파일을 축적하고자 할 때는 정보처리와자유위원회의 허가를 받아야 하며, 민간의 경우에도 위원회에 신고를

하도록 되어 있다. 또한, 정확성 유지의 원칙을 엄격하게 적용하고 있다. 정보수집자는 보유한 타인의 개인정보에 변화가 있음을 알게 된 경우 의무적으로 수정하도록 되어 있으며, 그 정보를 제3자와 공유했을 경우 공유한 쪽에도 변경 사실을 통보하도록 규정하고 있다. 수집 목적 명시에 대해서는 분명한 언급을 하고 있지 않으나, 법정 저장기간을 초과하여 개인정보를 보유하는 것을 금지하고 있다. 그 외에 정보수집자에게 민감한 정보의 제외, 안전성 확보의 의무를 두고 있으며 정보주체에게 동의권, 고지받을 권리, 수집 여부를 확인할 권리, 열람·정정·삭제 청구권, 피해를 보상받을 권리 등을 인정하고 있다.

<표 33> 주요 국가의 개인정보보호법의 내용

구분	프랑스	독일	영국	캐나다	미국	벨기에
동의권	제26조	제4조		제7조, 부칙 4.3.	제555조의2 ②	
DM 거부권			제11조			제12조
민감한 정보 제외	제31조		제12조			
고지받을 권리	제27조	제33~34조	제7조	제5조	제555조의2 ⑤	제8조
수집목적 제시		제34조	제7조	부칙 4.2.	제555조의2 ③	
기간초과 금지	제28조		제10조	부칙 4.5.		제4조
목적외 사용 금지		제14~17조		부칙 4.4.		
안전성 확보	제29조	제9조		부칙 4.7.		제16조
수집여부 확인	제34조					
열람	제35조	제19, 34조	제17조	부칙 4.9.	제555조의2 ④	제13조
정정, 삭제/파기	제36조	제20조	제17조	부칙 4.9.	제555조의2 ④	제14조
공시 및 등록	제15조 :허가제(공공) 제16조 :신고제(민간)	제23조 : 신고제	제17~19조	부칙 4.8,	제555조의2 ⑥	제18조 : 신고제
보상	제13조		제13조		제555조의2 ⑦	제7~8조
관리책임자		제36조		부칙 4.1.		
정확성 보장	제37조 :수정의무 제38조 :변경통보*			부칙 4.6.		제15조 : 분쟁정보 사용 금지
권리양도금지		제6조				

옴니버스 형식 중 공공 영역과 민간 영역을 구분하지 않고 규율하는 법률의

전형적 형태이다. 예외적으로 의료 관련 정보에 대해서만 특별히 따로 규율하고 있다. 또한 감독기구로, 상·하원 의원 각 2명과 기술·회계감사·시민사회 등 각 분야의 전문가를 포함하여 17명으로 구성되는 국가정보처리자유위원회를 두고 있다.

나) 독일의 연방정보보호법

이 법은 정보보호책임자의 지정을 명문화하고 있다는 점이 특징적이다. 감독기관이 정보보호책임자의 업무 수행을 감독할 수 있으며, 심지어 해고를 요청할 권한까지 가지고 있다. 또한 개인정보수집자들은 수집하는 개인정보를 정보보호감독관에게 등록하도록 규정하고 있다. 개인정보와 관련하여 규정된 정보주체의 권리는 양도불가능함을 명문화하고 있다. 그 외에 정보주체의 권리로 고지 및 동의권, 목적외 사용 금지, 열람·정정·삭제 청구권을, 정보수집자의 의무로 목적 외 사용 금지를 규정하고 있다.

옴니버스 형식의 법률이면서 공적 영역과 사적 영역을 분리하여 규율하는 법률 유형의 전형이다. 감독 기구 또한 규율 대상에 따라 분리되어 있다. 연방정보보호감독관은 연방정부의 개인정보 보호를, 주 정보보호감독관은 주 정부와 민간 영역의 개인정보 보호를 담당하도록 되어 있다. 연방정보보호감독관은 내무부 관할인 반면, 주 정보보호감독관은 주 의회 산하에 위치하고 있다.

다) 영국 데이터보호법

이 법에서는 동의권이 분명하게 인정되지 않고 있다. 대신 민감한 정보의 수집을 금지하고 있으며, 불필요하게 오래동안 개인정보를 보유하여 정보 주체에게 불이익을 주는 것을 금지하고 있다. 또한, 어떤 경위로 수집되었든 간에 다이렉트 마케팅의 목적으로 개인정보를 사용하려 할 경우 정보주체가 거부권을 행사할 수 있도록 규정하고 있다. 그 외에 정보주체의 권리로 열람·

정정·삭제 청구권과 피해보상을 받을 권리를, 정보수집자의 의무로 수집 목적 제시와 데이터감독관에 대한 신고 의무를 규정하고 있다.

공공 영역과 민간영역을 동일하게 규율하고 있다는 점에서 옴니버스 형식이라고 할 수 있다. 그러나 보건, 교육, 사회사업, 신용 관련 정보에 대해 별도의 규율 조항들을 두고 있으며, 안보, 범죄, 과세, 언론, 문화예술, 연구, 조사, 통계, 이미 공개된 정보, 가정 내의 정보 등에 대해 광범위한 예외 규정을 두고 있어, 결과적으로는 분야별 입법과 유사한 양상을 띤다. 감독기구로는 데이터감독관을 두고 있는데, 다른 나라와 달리 국가 기구가 아니라 독립법인의 위상을 갖고 있다.

라) 캐나다 개인정보보호및전자문서법

개인정보의 수집·이용·공개에 있어 정보주체의 고지받을 권리와 동의권을 명문화하고 있으나, 그 외의 수집 목적 제시, 지나치게 오랜 기간의 보유 금지, 목적외 사용 금지, 안전성 확보, 현황에 대한 공개, 관리책임자 임명, 정확성 유지 등 정보 수집자의 의무와 정보주체의 열람·정정·삭제 청구권은 부칙에서 권장사항으로 규정하고 있다.

이처럼 느슨하게 되어 있는 것은 이 법이 민간영역에 적용되는 일반법이기 때문이다. 공공기관에 적용되는 별도의 법인 프라이버시 법(Privacy Act)에서는 많은 내용이 강제 규정으로 되어 있다. 감독기구 역시 공공부문을 관장하는 정보보호감독관(Information Protection Commissioner)과 민간 영역을 관장하는 프라이버시 감독관(Privacy Commissioner)로 이원화되어 있다.

마) 미국 프라이버시법

정보 수집에 있어 정보주체의 동의권과 고지받을 권리, 열람·정정·삭제 청구권 및 보상받을 권리를 명시하고 있으며, 정보수집자의 의무로는 수집에

관한 현황을 공개할 것을 규정하고 있으나 목적 명확화, 안전성 확보, 정확성 유지 등의 원칙을 명시하지는 않고 있어 OECD 8원칙에 비추어볼 때 구체성이 부족한 편이다. 다만 프랑스와 더불어 아동의 개인정보 수집과 관련된 규제 조항을 포함시키고 있다.

또한, 미국 프라이버시법은 연방 공공기관에만 적용되며, 민간 영역에 적용되는 일반법이 없다. 별도의 국가감독기구도 존재하지 않는다.

바) 벨기에 개인정보보호법

정보수집자에게 감독 기구에 신고할 의무, 과도하게 오랜 기간 보유하지 않을 의무, 안전성 확보의 의무를 부과하고 있으며, 정보주체의 고지받을 권리와 보상받을 권리, 열람·정정·삭제 청구권을 보장하는 등 프랑스의 법제와 유사한 내용이 많다. 다만 동의권을 일반적으로 인정하지 않은 채 다이렉트 마케팅에 대한 거부권을 인정하고 있다는 점은 영국과 유사하다. 또, 개인정보와 관련된 분쟁이 발생했을 경우, 분쟁 기간 동안 그 개인정보의 사용을 금지하고 있다는 점도 눈에 띈다.

공공 영역과 민간 영역의 구분 없이 단일한 규율 원리를 적용하고 있다. 상·하원에서 각각 8명씩 구성되는 개인정보보호원을 감독 기구로 두고 있다.

2) 국내 개인정보보호법에 들어가야 할 내용

우리 나라의 개인정보보호법 제정도 역시 OECD 가이드라인의 8원칙을 기본으로 해야 한다. ▲ 목적 명확성의 원칙 ▲ 수집 제한의 원칙(정보주체의 동의권과 정보수집자의 고지의 의무 이행 여부) ▲ 이용 제한의 원칙 ▲ 정보내용 적합성의 원칙 ▲ 안전성 보장의 원칙 ▲ 공개의 원칙 ▲ 개인 참가의 원칙 ▲ 책임의 원칙 등이 이 법의 전반에 포함되어야 한다.

그 외에 개인정보 보호를 효율적으로 하기 위한 여러 가지 제도적 장치들을

법률 속에 담아야 한다. 국가 개인정보 감독기구를 운영하는 방안이나, 개인정보 영향평가제도를 실시하는 방안, 집단소송제를 도입하여 정보주체들의 소송부담을 줄이는 제도의 도입 등이 검토되어야 한다.

2. 웹사이트에 적용되는 개인정보보호법제 검토

현행 「정보통신망이용촉진및정보보호등에관한법률」은 그 수범 대상을 정보통신서비스제공자로 규정하고 있다. 이 법 제2조 2항 2호에 따르면, 정보통신서비스제공자란, "전기통신기본법 제2조제7호의 규정에 의한 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다"고 되어 있다. 즉, 전화나 인터넷 등의 유·무선통신 사업자와 인터넷을 기반으로 사업을 하는 쇼핑몰, 온라인 언론, 포털, 커뮤니티, 온라인 교육 사업 등이 모두 포함된다. 따라서, 이 법은 사실상 온라인 상에서는 일반법적 성격을 지니고 있다. 그 외에 웹 상에서의 고객 프라이버시 보호와 관련하여 고려해야 할 법률로는 「전자상거래등에서의소비자보호에관한법률」과 「위치정보의보호및이용에관한법률(안)」 등이 있다.

그러나 「전자상거래등에서의소비자보호에관한법률」의 경우, 제11조 1항에서 개인정보 관련 사항은 정보통신망법의 규정을 받도록 하고 있어, 크게 중요하지 않다.[83] 다만 21조 금지행위의 일부 조항이 개인정보 보호 및 스팸 메일과 관련을 갖고 있다.[84] 「위치정보의보호및이용에관한법률(안)」의 경우, 아직 제

83) 제11조 (소비자에 관한 정보의 이용 등) ① 사업자는 전자상거래 또는 통신판매를 위하여 소비자에 관한 정보를 수집 또는 이용(제3자에게 제공하는 경우를 포함한다. 이하 같다)하고자 하는 경우에는 정보통신망이용촉진및정보보호등에관한법률 등 관련 규정에 따라 이를 공정하게 수집 또는 이용하여야 한다

84) 제21조 (금지행위) ①전자상거래를 행하는 사업자 또는 통신판매업자는 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.
1. 허위 또는 과장된 사실을 알리거나 기만적 방법을 사용하여 소비자를 유인 또는 거래하거나 청약철회등 또는 계약의 해지를 방해하는 행위
5. 소비자가 재화를 구매하거나 용역을 제공받을 의사가 없음을 밝혔음에도 불구하고 전화,

정되지는 않았으나 향후 무선 인터넷이 더욱 활성화되면 개인정보 보호에 매우 중요한 영향을 미칠 법안이다.

가. 정보통신망이용촉진및정보보호등에관한법률 검토

이 법은 민간영역에서의 일반법적 성격을 자처할 정도로 개인정보에 대해 비교적 상세히 규정된 법률이다. 개인정보 보호와 관련하여 이 법은 ▲ 수집 및 수집 제한에 대한 규정 ▲ 이용 및 제3자 제공에 대한 규정 ▲ 위탁·양수·양도에 관한 규정 ▲ 기술적·관리적 대책 수립에 관한 규정 ▲ 정보주체의 열람·정정·삭제에 관한 규정 ▲ 파기에 관한 규정 ▲ 개인정보관리책임자 지정에 관한 규정 ▲ 개인정보분쟁조정위원회 설치에 관한 규정 ▲ 아동의 개인정보 수집에 관한 규정 ▲ 스팸 정보에 관한 규정 등을 포함하여 OECD 가이드라인 등 국제적 기준에 비교적 부합하는 보호 규정들을 담고 있다.

1) 법률의 목적 자체의 문제점

정보통신망법은 기본적으로 정보통신망을 활성화하기 위한 법률이다. 그런 목적 하에서, 망의 안정성을 위협할 수 있는 행위들에 대한 규제들을 정보 보호라는 이름으로 포괄하고 있다. 때문에 정보통신망 이용 촉진, 네트워크 보안, 개인정보 보호라는 서로 다른 세 가지 목표가 혼재되어 있다.

물론 넓게 보면 정보통신망의 발전을 위해서 필요한 요소들을 고루 서술하

모사전송, 컴퓨터통신 등을 통하여 재화를 구매하거나 용역을 제공받도록 강요하는 행위
6. 본인의 허락을 받지 아니하거나 허락 받은 범위를 넘어 소비자에 관한 정보를 이용하는 행위. 다만, 다음 각목의 1에 해당하는 경우를 제외한다.
가. 재화등의 배송 등 소비자와의 계약의 이행에 불가피한 경우로서 대통령령이 정하는 경우
나. 재화등의 거래에 따른 대금정산을 위하여 필요한 경우
다. 도용방지를 위하여 본인확인에 필요한 경우로서 대통령령이 정하는 경우
라. 법률의 규정 또는 법률에 의하여 필요한 불가피한 사유가 있는 경우

고 있는 것이기는 하다. 그러나 현실적으로는 개인정보 보호가 다른 두 요소들과 충돌하는 측면도 많다. 사업자들의 이해를 고려하여 혹은 통신정책 차원의 고려로 인해, 개인정보 보호를 소홀히 하거나 일관되지 않게 적용하는 경우가 발생할 수 있다. 한 예로, 2003년 국정감사에서 밝혀진 바에 따르면, 이동통신 3사가 가입해지한 소비자 정보 1천만명분을 그대로 보관하고 있었는데도 정보통신부는 수수방관하고 있었다. 게다가, 같은 사실이 감사원에 의해 지난 2002년에 지적되었음에도 별다른 조치를 취하지 않고 있었던 것으로 드러나, 정보통신부가 기업 운영의 편의성만을 일방적으로 강조한다는 비판을 받았다.[85]

네트워크 보안과 개인정보 보호 사이에도 충돌이 발생한다. 한 예로, 2003년 초 1·25 인터넷 대란에 대한 대응의 하나로 정보통신부는 6월 11일 공청회를 열어 이 법률의 개정안을 내어놓았다. 그런데, 이 법은 네트워크의 보안을 강화하기 위해 ▲ 네트워크에 장애를 발생시킬 수 있는 우려가 있을 경우 대형 ISP 업체에게 일부 이용자 혹은 이용자 전체에 대한 서비스를 중단시킬 권한을 부여하며 ▲ 정보보호조치가 미흡한 이용자의 정보통신망으로의 접속을 제한할 수 있게 했으며 ▲ 정보통신부가 침해사고 원인분석을 위하여 정보통신서비스제공자에게 관련자료[86]의 제출을 요구할 수 있도록 하며 ▲ 정보통신망에 장애를 일으키는 행위에 대해서는 미수범까지 처벌하는 등 일반 시민들의 통신 자유와 비밀을 심각히 침해하는 내용들을 담고 있었다. 때문에, 함께하는 시민행동은 이 개정안을 국가보안법에 비유하기도 했다.[87] 이후 일부 독소조항들이 제거되어 7월 11일 개정안이 입법예고되었으나, 참여연대는 이 안에 대해서도, 시민행동이 지적한 것과 같은 문제들이 반복되고 있으며, 덧붙여 ▲

85) 함께하는 시민행동 외 7개 단체, 『독립적 개인정보 보호기구 설치를 촉구하는 정당·시민사회 기자회견 자료집』 중

86) 여기에는 로그파일을 비롯하여 이용자의 접속 관련 자료들이 포함되는데, 이는 영장에 의해 사법경찰관이나 정보기관의 수사요원만이 획득할 수 있는 통신 비밀의 영역에 해당한다.

87) 함께하는 시민행동 보도자료, 『국가보안법에 버금가는 '네트워크 보안법' 제정 시도 중단하라』, 2003. 6.11.

인터넷침해사고대응지원센터의 권한이 지나치게 광범위하다는 점 ▲ 장애의 우려에 대한 판단 기준이 여전히 자의적이라는 점 등을 지적했다.[88]

2) 정보수집의 정당성에 대한 검증 과정이 미비: 프라이버시 영향평가제 도입 필요

현재 민간 영역에서의 개인정보 수집 과정에서 가장 문제가 되는 것은 서비스 제공자와 이용자 간의 불균형 관계이다. 개인정보 수집은 원칙적으로 당사자의 동의에 의해 수집하도록 되어 있다. 그러나, 서비스 이용자는 서비스를 받기 위해서 서비스 제공자가 요구하는 개인정보들을 입력해야 하며, 이 과정에서 불필요한 개인정보를 수집한다고 판단되더라도 이용자로서는 사실상 이의를 제기할 수 없다. 서비스를 제공받지 않던지, 이용자가 요구하는대로 개인정보를 제공하던지 양자 택일을 할 수밖에 없게 된다.

물론, 서비스 제공자가 개별 이용자들과 모두 협상을 진행하는 것은 현실적으로 불가능하다. 결국 개인정보 수집의 정당성을 검증할 수 있는 장치가 필요하게 된다. 이와 관련하여, 최근 몇몇 국가에서 실시되는 프라이버시 영향평가제의 도입을 고려해볼 필요가 있다.

프라이버시 영향평가는 최초에 뉴질랜드, 캐나다 주 정부 등 비교적 규모가 작은 국가나 지역에서 시행되었으며, 최근 미국 정부가 전자정부 추진 과정에서 이 제도를 도입함으로써 주목을 받게 된 제도이다. 미 연방 정부는 최근 전자정부 추진 과정에서 정보 시스템을 개발하거나 개인식별이 가능한 전자정보를 수집하기 전에 그 시스템이나 정보 수집 행위가 프라이버시에 미치는 영향을 먼저 살펴보게 하였다. 그 평가 기준으로는 ▲ 수집할 정보 항목 ▲ 정보를 수집하는 이유 ▲ 수집되는 정보의 내용과 이를 공유하는 방식 ▲ 정보의 이용 목적 ▲ 정보 보안의 방안 등이 포함된다.[89]

---

88) 참여연대, 『정보통신망이용촉진및정보보호등에관한법률 개정안에 대한 의견서』, 2003.7.31
89) 권선경, 『미국과 한국의 개인정보보호법제도 비교 연구』, 한국정보보호진흥원, 앞의 책,

물론 미국에서는 공공기관에 한정하여 이 제도를 시행하고 있다. 그러나, 민간 영역에서도 일정 수 이상의 개인정보를 취득하는 정보 수집자나 일정 수 이상의 직원을 고용하는 법인 등, 사실상 다수 시민에게 영향을 미치는 정보 수집자에게는 이 제도의 도입을 검토할 필요가 있다. 평가 결과가 부정적으로 나왔다고 해서 수집을 금지시킬 수는 없다 하더라도 언론 공표 등을 통해 가입에 대한 판단 기준을 제시하는 역할을 할 수는 있을 것이다.

3) 제3자 제공에 대한 포괄적 동의의 문제 : 명시적, 선별적 동의 제도 도입 필요

정보 수집자가 개인정보를 제3자에게 제공할 때는 당사자의 명시적 동의에 의하게 되어 있다. 그러나, 많은 기업들은 약관에서 "고객들에게 더 낳은 서비스를 제공하기 위해 제휴사 등에 정보를 제공할 수 있습니다"라는 조항 하나만 집어넣은 채, 자유롭게 개인정보를 유통시켜왔다. 이처럼 포괄적으로 동의를 받는 방식이 가능하기 때문에, 개인정보 이용 목적에 대한 정보 주체의 동의는 사실상 무의미해진다.

때문에 이인호 교수는, 특히 제3자 제공과 관련해서는 선별적 동의를 보장하는 것이 필요하다고 주장한다.[90] 정보 제공에 대한 동의를 받을 때, 각각의 제공 대상에 대한 동의를 따로따로 받을 것을 법률로 강제할 필요가 있다.

4) 개인정보 취득 경위에 대한 설명 부재의 문제 : 개인정보 취득경위 공지 의무화 필요

어느 날 갑자기 잘 모르는 곳으로부터 텔레마케팅 전화가 걸려오는 경우, 정보 주체들은 개인정보의 유출을 의심하고 두려워하게 된다. 그러나, 정작 그

---

pp. 76-77.

90) 이인호, 앞의 책, p. 132.

회사에 개인정보 취득 경위를 물어보면 명확한 대답을 듣기가 쉽지 않다. 개인정보가 정상적으로 유통된 것인지, 불법적으로 유출된 것인지 확인하기 어렵기 때문에, 정보주체들은 권리 구제를 위한 적절한 행동에 나서기도 어렵고 정보 유출에 대한 두려움도 해소되지 않는다.

따라서 개인정보를 보유·활용하는 서비스 제공자에게 정보 수집의 경위를 정보주체에게 설명하도록 의무화할 필요가 있다. 실제로 이 법에서도, 스팸메일의 경우에 한해서는 정보 취득 경위를 명시하도록 제50조 2항을 통해 규정하고 있다.[91]

나. 위치정보의이용및보호등에관한법률 검토

무선인터넷의 활용이 점차 활성화되면서 위치정보의 보호가 중요한 과제로 떠오르게 되었다. 2003년 8월 11일 정보통신부는 「위치정보의이용및보호등에관한법률(안)」을 입법예고한 상태이다.

이 법은 정보통신망법과 동일하게 ▲ 위치정보의 수집 ▲ 위치정보의 이용 및 제3자 제공 ▲ 양수·양도에 관한 규정 ▲ 기술적· 수립에 관한 규정 ▲ 정보주체의 열람·정정·삭제에 관한 규정 ▲ 파기에 관한 규정 ▲ 통신위원회의 재정·조정에 관한 규정 ▲ 아동의 개인정보 수집에 관한 규정 등을 규정하고 있다.

그러나, 위치정보의 보호 필요성이 일반 개인정보에 비해 높기 때문에, 이 법에서는 몇 가지 더욱 강력한 보호장치가 포함되어 있다. 우선 정보통신망법보다 처벌의 강도가 크다. 둘째, 선택적 동의를 인정하고 있으며, 일시적 동의

91) 제50조 (영리목적의 광고성 정보전송의 제한<개정 2002.12.18>) ②제1항의 규정에 의한 영리목적의 광고성 정보를 전자우편·전화·모사전송 그 밖에 대 통령령이 정하는 매체를 이용하여 전송하는 자는 대통령령이 정하는 바에 따라 다음 각호 의 사항을 광고성 정보에 명시하여야 한다. 다만, 제3항에 해당하는 경우에는 그러하지 아 니하다. <개정 2002.12.18>
3. 전자우편주소를 수집한 출처(전자우편에 한한다)

철회를 가능하게 할 것을 강제하고 있다.[92] 셋째로 위치정보 사업에 대해 허가제를 적용하고 있으며, 업무의 위탁도 인정되지 않는다. 마지막으로, 일반적인 개인정보의 경우 개인정보분쟁조정위원회의 조정만을 인정하고 있으나, 위치정보의 경우 통신위원회의 재정 및 조정 권한을 적용하고 있다.

1) 법 목적의 혼재

정보통신망법과 마찬가지로 이 법 또한 위치정보의 보호와 위치정보 서비스의 활성화라는 서로 상충될 수 있는 목표를 다루고 있다. 또한 주요 보호 조치가 정보통신부 장관과 통신위원회에 의해 이루어지도록 되어 있다. 여러 차례 지적되었듯이 기본적으로 정보통신 산업의 촉진을 임무로 하는 정보통신부가 위치정보 서비스 산업의 이해를 고려하여 위치정보 보호의 임무를 소홀히 할 가능성이 있다.

2) 기기 소유자와 사용자가 서로 다른 경우의 문제점 : 소유자와 사용자의 권리 공히 인정 필요

정보통신망법과 마찬가지로, 이 법률의 기본 구도는 위치정보서비스 제공자와 이용자 사이의 관계를 기본으로 하고 있다. 때문에 '개인위치정보주체'가 정보 제공에 대한 동의 및 철회, 일시적 철회를 할 수 있다고 규정되어 있다.

그런데, 위치정보를 수집하는 것은, 실제로는 자연인으로서의 개인의 위치를 수집하는 것이 아니라, 이동통신기기의 위치를 수집하는 것이다. 현실적으로는 이동통신기기 소유자와 실사용자가 다른 경우가 많다. 그런 상황에서, 이동통

92) 제15조(개인위치정보의 수집) ②개인위치정보주체는 제1항의 규정에 의한 동의를 하는 경우 개인위치정보의 수집의 범위 및 약관의 내용 중 일부에 대하여 동의를 유보할 수 있다. 제16조(개인위치정보 등의 이용 또는 제공) ②개인위치정보주체는 제1항의 규정에 의한 동의를 하는 경우 개인위치정보의 이용목적, 제공받는 자의 범위, 제공할 정보의 내용 및 위치기반서비스의 일부에 대하여 동의를 유보할 수 있다.

신기기 소유자와 실사용자 중 어느 쪽을 '개인위치정보주체'로 규정할 것인지가 문제가 된다.

대개 위치정보 서비스에의 가입(위치정보 제공에의 동의)이나 탈퇴(동의 철회)는 기기 소유자에 의해 이루어질 가능성이 높다. 반면, 일시적 철회는 실사용자가 필요로 하는 권리일 가능성이 많다. 이를 구분하지 않으면, 실제 가입자의 동의 없이 실사용자가 서비스 자체를 탈퇴하는 경우가 발생할 수 있다. 또 반대로 실사용자가 일시적 철회를 요청할 때, 서비스 가입 당사자가 아니라는 이유로 권리를 보장받지 못할 수도 있다. 때문에, '개인위치정보주체'와 '위치정보서비스 가입자'를 구분할 필요가 있다. 특히, 가족이나 연인 사이에 위치정보의 추적으로 통한 폭력 행사나 스토킹 행위 등이 발생할 수 있으므로 이 점은 반드시 구분 인식되어야 한다.

3) 위치정보 수집 범위의 정당성 검증의 문제 : 사용자의 필요에 따른 정보수집 필요

위치 정보는 서비스의 유형에 따라 어느 정도로 정확하게 위치를 파악해야 하는지가 달라진다. 예컨대, 현행 이동전화 서비스를 받기 위해서도 위치정보는 수집된다. 약 2Km 정도의 반경으로 위치가 파악되는 것이다. 반면, 자동차 네비게이션 서비스를 받기 위해서는 상당히 정확한 위치를 파악해야 한다.

OECD 가이드라인에서 가장 중요한 원칙 중 하나가 목적 명확성의 원칙이다. 이는 목적에 부합하는 정보만을 수집할 것을 요구하고 있다. 위치정보 서비스에서 목적 명확성의 원칙과 관련하여 가장 중요한 것은, 바로 파악되는 위치의 정확도, 즉 수집 범위이다. 그런데, '어떤 서비스를 위해 어느 정도 정확하게 위치를 파악해야 하는가'라는 문제는 다분히 기술적 측면과 연관된다. 때문에 이용자들로서는 목적에의 부합 여부를 정확히 알기 어렵게 된다. 이는 동의의 과정을 무의미하게 만든다.

이 문제를 해결하기 위해, 이 법률은 정보통신부 장관이 고시를 통해 위치

정보의 등급을 정할 수 있도록 하고 있다. 그 등급에 따라 위치의 정확도나 응답 속도, 그리고 동의 절차 시행 여부까지도 결정할 수 있게 된다. 그러나, 이 역시 행정부처에서 임의로 결정하게 하기보다는 앞에서 제안된 프라이버시 영향 평가제도를 도입하여 해결하는 것이 바람직하다.

4) 긴급구조를 위한 위치정보 공유의 문제점 : 오남용 방지대책 마련 필요

이 법률 23조 1항은 위치정보 수집자로 하여금, 당사자의 구조 요청을 받은 긴급구조기관에게 위치정보를 제공할 것을 의무화하고 있다. 긴급구조라는 특성상, 위치정보 수집자가 직접 당사자로부터의 동의를 확인하지 못하더라도 정보를 제공하도록 한 것은 필요한 일이다.

문제는 긴급구조기관이 당사자로부터 구조요청을 받았는지를 확인하는 것이 쉽지 않다는 점이다. 때문에, 당사자의 요청이 없는 상황에서 긴급구조와 무관한 목적으로 위치정보 제공을 요구하는 경우가 발생할 수 있다. 사실 23조 5항에서 긴급구조를 위한 위치정보 요청 및 제공시, 기계적 방식으로 하도록 규정한 것이 곧 긴급구조 관련 오·남용 가능성을 줄이기 위한 대책이다. 그러나, 그 조문 자체가 오·남용을 차단할 구체적 방법을 제시하는 것은 아니므로 좀 더 분명한 대책을 법률로 강제해야 할 것이다.

5) 일시적 동의 철회를 위한 기술적 조치의 문제점 : 사용자에게 기술적 선택권 부여 필요

이 법률은 위치정보 제공에 대한 동의를 일시적으로 거부할 권리를 위치정보주체에게 부여하고 있다. 그리고, 그 권리를 보장하기 위해 위치정보사업자가 기술적 조치를 취하도록 되어 있다.

그런데 위치정보의 수집은 앞에서 이야기했듯이, 이동통신 기기의 위치를 수집하는 것이다. 때문에 자기정보통제권을 제대로 구현하기 위해서는 위치정

보사업자에게 기술적 조치의 의무를 부여할 뿐 아니라 기기 자체에 그러한 기능이 포함되어 있는 것이 바람직하다. 즉, 이동통신 기기에 위치정보 수집 기능을 포함시킨다면, 이를 작동하지 않게 하는 장치도 포함되어야 할 것이다. 이를 법률로 강제해둘 필요가 있다.

또한 이 경우에도 선택적 동의가 보장되어야 할 것이다. 예컨대 휴대전화의 경우, 위치정보 관련 부가서비스를 위해서 위치정보를 수집할 뿐 아니라 휴대전화 서비스 자체를 위해서도 위치정보를 수집하게 된다. 그런데 후자의 경우 전자에 비해 요구되는 정확도가 상대적으로 낮은 편이다. 그런 경우, 부가서비스를 이용하지 않기 위해 휴대전화 자체를 꺼야 한다면 일시적 동의 철회의 권리가 잘 작동하기 어렵다. 따라서 정밀하게 위치를 추적하는 장치만 따로 켜고 끌 수 있게 해야 한다

3. 금융기관에 적용되는 개인정보보호법제 검토

가. 주요 법제의 현황

금융 거래와 관련된 개인정보의 종류로는 크게 두 가지를 들 수 있다. 하나는 금융거래 사실과 직접 연결된 정보인 (금융)거래정보이다. 다른 하나는, 금융거래나 다른 경제 행위의 결과에 따라 개인의 신용상태를 확인할 수 있게 하는 정보인 신용정보이다. 이 두 정보는 일반적인 개인정보에 비해 개인의 사생활과 관련이 매우 큰 정보이기 때문에, 더욱 엄격한 보호를 요구하는 정보이다. 그 중에서도 거래 사실을 직접 다루는 금융정보는 신용정보에 비해서도 더욱 엄격한 보호를 채택하고 있다.

전자의 개인정보를 다루는 법률로는 「금융실명거래및비밀보장에관한법률」이 있으며, 후자의 개인정보를 다루는 법률로는 「신용정보의이용및보호에관한법률」이 있다. 이외에 「특정금융거래정보의보고및이용등에관한법률」이 개인정보

문제와 관련이 있으나, 자금세탁행위 등 범죄 수사를 위해 금융정보를 제공하는 것을 목적으로 하고 있어, 자기정보통제권에 대한 제약이 인정되는 영역이다. 따라서, 이 논의에서는 제외하기로 한다.

「금융실명거래및비밀보장에관한법률」은 엄격한 보호를 요하는 금융거래정보의 특성상 원칙적으로 당사자의 동의 없는 거래정보의 제3자 제공을 금지하고 있다. 다만 금융거래 질서를 문란케 하는 행위를 포함하여 범죄를 수사하기 위한 경우에는 이를 예외로 하며, 이 경우에도 몇몇 특별한 경우를 제외하고는 원칙적으로 당사자에 통보하도록 되어 있다.[93] 금융거래의 개인정보 보호와 관련하여 주로 쟁점이 되는 것은 「신용정보의이용및보호에관한법률」이다.

나. 신용정보의이용및보호에관한법률 검토

신용정보는 금융 거래 이외에도, 개인의 다양한 상거래행위의 결과에서 얻어질 수 있다. 예컨대, 조세 및 공과금의 납부, 할부 거래의 할부금 납부 등이 이에 해당한다. 때문에, 단순히 금융 영역에 국한되는 것이 아니라 소비자 보호 전반과 관련된 영역이다.

1) 해외 법률의 동향

신용정보 보호를 위한 법률 체계는 크게 두 종류로 구분된다. 우선 별도의 법률로 소비자 신용정보를 보호하는 법률이 있는 미국의 경우이다. 이는 일찍부터 금융 거래가 발전했고, 이에 따라 신용정보 관련 산업이 발전해온 역사적 경험이 반영된 것이다. 1968년 공정신용보고법(Fair Credit Reporting Act of 1968)을 제정하여 신용정보에 대한 보호를 다루어왔으며, 1996년에 보호 조

93) 여기서 당사자 통보의 의무가 면제되는 경우는, 업무의 성격상 금융기관 상호간에 거래정보를 전달하는 경우와, 금융감독 기관이 금융기관에 대한 감독·조사 업무를 수행하기 위해 금융기관으로부터 거래정보 제출을 요구하는 경우이다.

항을 강화한 소비자신용보고개혁법(Consumer Credit reporting Act of 1996)으로 대체되었다. 이 법률은 ▲ 신용정보를 제공받을 수 있는 기관의 자격 요건 ▲ 오래된 정보의 경우 제공 회피 ▲ 제공할 정보의 정확성 확인 ▲ 신용정보 이용에 대한 정보주체에의 고지 의무 ▲ 이의에 대한 재조사 의무 등으로 구성된다.

이 법은 개인정보자기통제권의 원리를 온전히 실현하는 것보다는 신용정보의 합리적 유통 과정을 확립하는 것이 목적으로 하고 있다. 따라서, 개인정보보호의 일반 원칙들이 그대로 적용되지는 않는다.

반면에 대부분의 유럽 국가들은 신용정보를 따로 규율하는 법률이 없으며, 개인정보보호 일반법에 의해 규율되고 있다. 따라서, 자기정보통제권에 충실하게 보호할 수 있다는 장점이 있는 반면, 신용정보 활용의 측면에서는 한계가 존재한다.

한편 영국의 경우는, 1974년에 소비자신용법(Consumer Credit Law)을 제정하여 보호를 시도했으나, 이후 영국의 개인정보보호 일반법인 데이터보호법(Data Protection Act)이 제정되면서 보호의 역할을 나누어맡고 있다. 일본의 경우도, 최근 개인정보보호일반법 제정 논의와 동시에 신용정보에 대한 별도의 법률을 제정하려는 논의가 계속되고 있다.

2) 국내의 신용정보의이용및보호에관한법률 검토

한국은 미국과 같이 신용정보에 관한 법률을 따로 규정하고 있다. 이 분야에 적용되는 개인정보 일반법이 없는 관계로 자기정보통제권이 온전히 반영되지는 않는다. 그럼에도 미국에 비해 상대적으로 보호 정도가 강한 편인데, 이는 한국의 관치금융의 전통과도 관련이 있는 것으로 판단된다.

이 법률은 정보주체에 대한 보호 조항으로 ▲ 목적에 부합하는 정보만을 수집할 의무 ▲ 정보의 열람 및 갱신 청구권 ▲ 불이익이 초래될 수 있는 오래된 신용정보의 파기 ▲ 일반적 사항에 대한 공시 의무 ▲ 손해배상 책임의 입

증 전환 등을 규정하고 있으며, 신용불량자 등재시에는 통지 조치를 규정하고 있다.

가) 자의적 법 적용 가능성 : 구체적 적용조항 구비 필요

이 법률은 신용정보 처리와 관련된 상당 부분을 시행령이 아닌 '금융감독위원회가 정하는 바'에 따라 처리하도록 규정하고 있다.[94] 자기정보통제권에 대한 제약은 당사자의 동의나 법률에 의해서만 가능하다는 OECD 가이드라인의 정신에 비추어보면 이것은 상당히 위험한 요소이다. 또한, 애매모호한 표현으로 법 집행 기관의 자의적 해석을 인정하는 경우가 있다.

재정경제부의 경우, 신용정보의이용및보호에관한법률 조항들을 임의로 해석하면서 심지어 같은 법률 조항을 업종에 따라 달리 적용하는 양상까지도 보였다. 예컨대, 신용정보법 26조 7항 '나'목에는 '정당한 사유없이 채무자의 관계인에게 연체사실을 통보하는 행위 금지'에 대한 조항이 있다.[95] 이에 따라 재정경제부는 2002년 5월 카드사 규제 대책을 발표할 때, 이를 철저히 처벌하겠다고 밝혔다. 그러나 2003년 3월 카드사 종합대책을 발표하면서는 '1개월 이상

94) 예컨대, 제21조(폐업시 보유정보의 처리)는 "신용정보업자 및 신용정보집중기관이 폐업하고자 하는 경우에는 보유정보를 금융감독위원회가 정하는 바에 의하여 처분·소거 또는 폐기하여야 한다"고 규정하고 있다. 물론, 조항의 취지는 명확하게 처분 혹은 폐기될 수 있도록 보장하기 위한 것으로 이해된다. 그러나, 이 조항대로라면, 금융감독위원회가 폐기를 보류시키더라도 이를 문제삼을 근거가 없다. 본 조문을 2개 항으로 나누어 "① 신용정보업자 및 신용정보집중기관이 폐업하고자 하는 경우에는 보유정보를 처분·소거 또는 폐기하여야 한다. ② 금융감독위원회는 ①항을 위한 절차를 고시할 수 있다"로 나누는 것이 더 바람직할 것이다.

95) 제26조 (신용정보업자등의 금지사항) 신용정보업자 등은 다음 각호의 행위를 하여서는 아니되며, 신용정보업자외의 자는 제5호 본문의 행위를 업으로 하거나 제6호의 행위를 하여서는 아니된다. <개정 1997.8.28, 2001.3.28>

7. 채권추심업무를 행함에 있어서 다음 각목의 1에 해당하는 방법을 사용하는 일

나. 채무자의 채무에 관한 사항을 정당한 사유없이 그의 관계인[채무자의 보증인, 채무자의 친족(채무자와 동거하거나 생계를 같이 하는 자를 포함한다), 채무자가 근무하는 장소에 함께 근무하는 자를 말한다. 이하 같다]에게 알리어 부담을 주는 방법

연락이 두절된 연체자'에 대해서는 이를 허용했고, 2003년 5월에는 허용 조치를 저축은행으로 확대하겠다고 밝혔다. 시행령도 아니고 법으로 규정된 내용에 대해 1년 사이에 완전히 다른 해석을 하는가 하면, 당연히 모든 기관에 동일하게 적용해야 할 법률을 임의로 어떤 금융기관에는 적용하고 어떤 금융기관에는 적용하지 않았던 것이다.[96]

나) 정보주체의 동의, 혹은 고지 절차 부재 : 정보주체의 명시적 동의 필요

이 법률은 신용정보의 수집과 관련하여 정보주체의 동의할 권리, 혹은 고지받을 권리를 보장하지 않고 있다. 다만, 금융거래 관련 정보, 질병 관련 정보 등 일부 정보에 대해서만 사전 동의를 의무화하고 있다. 그러나, 자기의 정보가 자기도 모르는 사이에 수집되고 있다면, 그 자체로 심각한 자기정보통제권의 침해이다. 사전 동의를 원칙으로 하고 불가피한 경우에는 사후 동의를 얻도록 하되, 신용불량자의 등재 등 동의 없이 수집할 필요가 있는 경우에도 고지를 의무화해야 한다.

다) 선택적 동의 가능성 부재 : 제3자에 대한 정보제공과 서비스 이용을 분리하고 관련 법률 제정 필요

신용정보법에도 금융기관이 금융거래 정보 등 일부 정보를 제3자에게 제공할 경우, 동의 절차를 거치도록 요구하고 있다. 그러나, 정보통신망법과 마찬가지로 매우 간략한 동의서에 동의하지 않을 경우 사실상 금융 관련 서비스를 전혀 이용할 수 없다.

이 문제를 개선하기 위해, 금융감독위원회는 신용정보 제공·활용동의서를 계약서류와 분리하고, 동의 여부를 서비스 제공 조건으로 삼을 수 없도록 지시한 바 있으나, 법률로 규정되어 있지 않다보니 많은 기관에서 이를 무시하

96) 함께하는 시민행동 보도자료, 『시민행동, 역감시 카메라 설치 캠페인 시작』

고 있는 실정이다. 위의 지시를 법률로 구체화할 필요가 있으며, 더불어 동의의 경우에도, 신용정보 제공 대상 기관별로 따로 동의할 수 있도록 법률로 보장할 필요가 있다.

<표 34> 개인신용정보의 제공·활용동의서 사례

개인신용정보의 제공·활용동의서

_____ 기관(신용정보제공·이용자) 귀하

이 계약과 관련하여 귀사가 본인으로부터 취득한 다음 신용정보는 신용정보의이용및보호에관한법률 제23조의 규정에 따라 타인에게 제공·활용시 본인의 동의를 얻어야 하는 정보입니다. 이에 본인은 귀사가 다음의 신용정보를 신용정보집중기관, 신용정보업자, 신용정보제공·이용자등에게 제공하여, 본인의 신용을 판단하기 위한 자료로서 활용하거나 또는 공공기관에서 정책자료로서 활용하는 데 동의합니다.

년 월 일

(서명 또는 인)

4. 단일한 독립적 개인정보 보호기구의 설치 필요성

개인정보 보호를 위해서는 기존 법률의 정비와 함께 개인정보 보호를 위한 일반법의 제정이 필요하지만, 이에 못지 않게 중요한 것은 개인정보 보호를 위한 독자적 보호기구의 설립이다.

가. 개인정보 보호 집행 모델의 분류

특히 민간 영역에서의 개인정보 보호를 위한 집행 모델은 크게 세 가지로 나뉘어진다. 미국식의 시장중심적 모델과 유럽식의 권리중심적 모델, 그리고

기술중심적 집행 모델이 그것이다.[97]

1) 기술중심적 집행 모델

기술중심적 집행 모델은 비교적 최근에 등장한 것으로 시스템 설계자가 선택하는 초기 설정(default settings), 기술 표준과 규약(technical standards and protocols) 등이 개인정보를 보호하거나 침해하는 능력을 결정짓는 변수라는 인식에서 출발한다. 따라서, 익명성, 혹은 개인정보 보호를 보장하는 시스템을 설계하는 것이 중심 과제가 된다. 이 모델에서 프라이버시 보호를 위한 정책적 논의는 기술자들의 토론의 장에서 이루어진다.
문제는 기술적인 토론 공간이 공공성을 반영한다는 보장이 없다는 점이다. 이인호 교수는 다음과 같이 지적하고 있다.

> 흔히 기술적 설계에 대한 결정은 공학자 집단 내부의 비밀스러운 토론에서 또는 근시안적인 정책적 관점에서 이루어지는 경향이 있다. 여기에 소비자 개인별 판매 전략과 정보보안이라고 하는 산업적 관점이 더해지면 네트워크 설계는 더욱 더 개인에 관한 상세한 정보를 수집하는 방향으로 압력을 받게 된다.[98]

2) 미국식(시장중심적) 집행 모델

이 모델은, 다른 누군가가 "이것이 너의 프라이버시"라고 규정해줄 수 없는 것이 프라이버시 권리의 기본적 특성이라는 것을 가정으로 삼고 있다. 따라서 보호의 주체는 기본적으로 개인의 선택에 맡겨진다. 그런데, 민간 영역에서 개인정보 보호가 문제가 되는 것은 주로 기업과 소비자 관계에서 발생한다. 그러다보니 이 모델은 사실상 개인정보를 재산권의 문제로 보는, 시장 선택의

97) 이 논의는 이인호, 위의 책을 주로 참조한 것이다.
98) 이인호, 위의 책, p. 150.

모델이 되었다. 실제로 이 모델을 선택하고 있는 미국의 경우 개인정보 보호를 위한 일반 원칙을 규정하는 법률이 없으며, 부문별로 존재하는 입법들도 주로 개인정보의 정확성을 유지하는 것에 초점을 맞추고 있다.

시장 중심적 모델의 문제는, 우선 자기정보통제권이라는 기본권을 구성하는 세부적 권리와 의무들 - 열람, 정정, 삭제의 권리, 수집 및 이용 제한, 정보 주체의 알 권리 - 이 법적으로 보장되지 않는다는 것이다. 또한, 개인정보보호 시장은 정보 수집자와 정보 주체 사이의 심각한 정보 불균형으로 인해 공정한 선택이 이루어지지 않는다. 때문에, 전형적인 시장 실패의 사례가 될 가능성이 높다.[99]

3) 유럽식(권리중심적) 집행 모델

이 모델은 개인정보 보호를 국가가 보호할 기본권의 문제로 간주한다. 때문에 개인정보 보호에 대한 일반적 행위 규범이 법적으로 규정되고, 국가 차원에서 설립된 전담 기구가 이 원칙들에 입각하여 정보 수집자의 수집 행위를 감독·규제하는 방식으로 이루어진다. 대개 행정부로부터 독립적인 전담기구가 설치되어 있으며, 기능은 국가별로 차이가 있지만, 감독·조사·분쟁조정·교육 등의 역할을 맡는다.

이 모델은 미국식 모델에 비해 이용자의 권리가 뚜렷하게 보장된다는 장점이 있으나, 효율성의 측면에서 많은 비판을 받고 있다. 제한된 인원과 자원을 가진 전담기구가 수많은 정보수집자들을 일일이 통제할 수 없다는 것이다. 이 모델 자체가 메인프레임 컴퓨터에 대규모 데이터베이스가 구축되던 시대적 배경 하에서 만들어진 모델이므로, 현재와 같이 수많은 컴퓨터들이 네트워크 형태로 연결된 시대에서는 적절하지 않은 측면이 있다. 실제로도 각국의 개인정보 전담 기구들이 제 역할을 다하고 있는지에 대해서도 긍정적으로 평가되지 않는 현실이다.[100]

---

99) 이인호, 위의 책, p. 145.

4) 대안적 입장

위에서 평가되었듯이, 개인정보 보호는 국가 규제나 시장 원리 중 어느 한 쪽에 맡기는 것은 한계가 있다. 이인호 교수는 유럽식 모델을 평가하면서, 클리퍼 칩 논쟁[101]이나 "Know Your Customer"[102] 제안에 대한 미국 시민사회의 대응이 오히려 효과적인 결과를 가져왔음을 지적하고 있다. 즉, 시장의 힘에 의한 자율 규제가 아닌, 진정한 의미에서의 자율 규제 - 국가와 시장으로부터 공히 독립된 시민사회의 자율 규제 - 가 가장 효과적인 방식이다.

국가 개입보다는 정보 주체의 자율 규제를 기본으로 하되, 정보수집자와의 역관계에서의 불균형을 시정할 수 있는 사회적 규제 모델을 만들어내는 것이 중요하다. 국가 차원의 전담 기구는 이러한 사회적 규제가 잘 작동하는지를 점검하고 육성하는 역할을 함으로써 기존에 제기된 효율성의 문제를 완화할 수 있다. 물론, 이런 모델이 아직 현실적으로 구현되고 있지는 않다. 그러나 몇 가지 단초들은 찾아볼 수 있다. 우선, 지난 2001년말 독일에서 발간된 「정보보호법의 현대화」 검토보고서는 공인된 소비자단체나 정보보호단체들에게 단체 소송권을 부여하는 것과 개인정보 수집에서 불공정한 행위를 한 기업에 대해 경쟁 기업이 소송을 할 수 있는 경쟁자 소송권을 부여하는 것을 제안하고 있다. 또, 일본의 경우 '인정 개인정보보호단체'를 규정하여 분쟁조정의 기능을 수행할 수 있게 하는 안이 제안되었다. 법안에는 인정 단체로 관련 사업자단체만을 인정하고 있었으나, 비영리단체로 확대하자는 안도 제시된 바 있다.[103]

---

100) 이인호, 위의 책, p. 143.

101) 미국 정부가 시도한 암호 표준화 계획. 사실상 국가의 암호 독점 시도라는 이유에서 시민사회의 강력한 저항에 부딪혔다. 상세한 내용은 사회적 책임을 위한 컴퓨터 전문가들의 모임(Computer Professionals for Social Responsibilities)의 웹사이트에서 제공되는 관련 자료들을 통해 확인할 수 있다. http://www.cpsr.org/program/clipper/clipper.html

102) 미국 연방준비제도이사회(FRB)가 1998년 제안한 금융거래 감시 계획으로 시민사회의 반발에 부딪혔다. 자세한 내용은 Privacilla 웹사이트의 "Know Your Customer" 웹페이지를 참조할 것. http://www.privacilla.org/government/kyc.html

이 외에도 집단소송제를 도입하는 방안도 검토해볼 수 있으며, 좀 더 급진적으로는 이용자 단체를 법제화[104]하여 정보 수집자들과 대등한 교섭력을 갖게 하는 방안도 검토해볼 수 있다.

나. 개인정보 담당기구의 요건

개인정보에 관한 국가의 책임을 강조하는 것은 앞에서 설명한 대로 유럽식(권리중심적) 모델에서 나타난다. 유럽 여러 국가에서는 오래 전부터 다양한 형태의 개인정보 감독 기구가 존재해왔다. 이러한 전통에 따라, 유럽의 개인정보 관련 일반 원칙을 규정한 1995년 EU의 「개인정보의 처리와 자유로운 이동에서 개인을 보호하기 위한 지침(이하 EU 개인정보보호지침)」 28조는 감독기구에 대한 규정을 다루고 있다. 이 조항은 가장 우선적으로 기능의 수행에 있어 독립적일 것을 요구하고 있다. 이는 국가 권력으로부터 인권으로서의 프라이버시를 보호하기 위한 국가기구라는 특성에서 기인한다.

1) 개인정보 담당기구의 위상 : 인사권과 예산권의 독립

독립성에 있어서 핵심적인 것은 인사권과 예산권이다. 인사권과 관련해 각국에서 공통적으로 택하고 있는 것은 추천제이다. 즉 입법, 사법, 행정부의 여러 기관이 각각 주어진 일정 숫자의 위원을 추천하여 구성하는 것이다. 감독기구가 행정부 산하 기관이나 대통령 직속 기관으로 되어 있는 경우에도, 위원 구성은 국회, 법원 등의 추천에 의해 이루어진다. 인사권에서 또 하나 중요한 것은 임기를 보장함으로써 업무의 자율성과 책임성을 높이는 일이다. 예산

103) 한국에서도 공정거래위원회의 승인을 얻은 소비자단체들의 경우 분쟁 조정을 수행할 권한을 갖고 있다.

104) 이는 전례가 없는 제도이기는 하나, 개인정보 침해나 감시 문제로 인해 분규가 존재하는 기업에서 노동조합들이 벌이는 활동이나, 예전 4대 통신망(하이텔, 천리안, 나우누리, 유니텔)에 존재하던 이용자 위원회 등이 수행한 역할에서 유추해볼 수 있다.

권의 경우, 편성의 독립성이 가장 중요하다. 완전 독립된 기구의 경우 국회로부터 직접 예산을 지원받으며, 편제상 행정부 산하 기관인 경우에도 행정부처가 실제 예산 사용에 대해 감독할 수 있는 권한을 갖지 않는 것이 일반적이다.[105]

<표 35> 각 국의 개인정보 감독기구의 위상

국가		소관	운영	위원 구성	임기	예산
프랑스		독립기구	합의제	의회, 회계검사원, 국참사원, 행정부에서 17명	5년, 의원의 경우 임기	법무부
벨기에		독립기구	합의제	상·하원에서 각 8명	의원 임기	법무부
독일	연방	연방 내무부	독임제	연방정부 추천 연방의회 동의	5년	내무부
	주	주 의회	독임제	주 의회 선출	5년	주의회
영국		공익법인	독임제	여왕 임명	5년	내무부·법무부
캐나다		의회	독임제	의회 임명	7년	의회

정영화, 『개인정보보호 감독기구 동입을 위한 법제도 개선방안연구』, 2000, 한국정보보호진흥원, pp. 129-187을 참조하여 에서 재구성

2) 개인정보 담당기구의 권한

EU 개인정보보호지침 28조 2항과 3항은 개인정보 전담기구가 다음과 같은 역할을 할 수 있어야 한다고 지적한다.

105) 이창범, 『현행 프라이버시 보호 담당기구의 성과와 한계』, 함께하는 시민행동 외 8개 시민사회단체 공동 주최, 『연속 워크숍 : 프라이버시 보호법제 개선의 쟁점들 - 제2회 워크숍 : 프라이버시 감독 체계의 개선 방안을 모색한다』 자료집 중.

2. 회원국은 개인정보처리와 관련된 개인의 권리와 자유의 보호에 연계되는 행정 수단이나 규정을 제정할 때 이 감독기구의 자문을 받아야 한다.

3. 감독기구는 특히 다음과 같은 권리를 갖는다.

- 처리 과정의 내용을 형성하는 데이터에 대한 접근권과 감독 의무의 수행에 필요한 모든 정보를 수집할 권리와 같은 조사권
- 제20조[106]에 따라 정보처리 과정이 있기 전에 의견을 제출할 권리, 그리고 그런 견해를 적절히 공표할 권리, 혹은 데이터의 차단, 삭제, 파기할 권리, 혹은 정보 처리에 대한 일시적이거나 한정적인 금지를 부과할 권리, 혹은 관리자에게 경고할 권리, 혹은 국회나 다른 정치적 기관에 문제를 언급할 권리
- 이 지침에 의거해 채택된 국내 법조항의 위반 사항에 대한 법적 절차에 개입할 권리와 위반 사항을 사법 당국에 알릴 권리

<표 36> 각 국의 개인정보 감독기구의 기능과 권한

구분		호주	캐나다	영국	독일	프랑스
공공 및 민간 모두를 적용 대상으로		○	○	○	○	○
기능 및 권한	민원고충처리	○	○	○	○	○
	법률준수여부 조사 및 감독	○	○	○	○	○
	교육·홍보	○	○	○	○	○
	정책지원·개발·자문	○	○	○	○	○
	조사권·자료제출요구권	○	○	○	○	○
	시정조치	×	○	○	○	×
	분쟁조정	×	×	×	×	×
	민간프라이버시규칙 승인 및 준수 여부 조사	○				
	언론 공표권			○		
	실무지침 제정		○	○		
	개인정보보호정책 검토				○	
	비공식적 화해 조정			○		

강달천, 『프라이버시 보호를 위한 감독기구의 사전적 권한』, 함께하는 시민행동 외 8개 시민사회단체 공동 주최, 『연속 워크숍 : 프라이버시 보호법제 개선의 쟁점들 – 제2회 워크숍 : 프라이버시 감독 체계의 개선 방안을 모색한다』 자료집 중.

106) 사전 조사와 관련된 조항이다.

이에 따라 각 국가 감독기구는 개인정보를 보호할 다양한 권리를 갖는다. 일반적으로 갖는 권리를 살펴보면, 사전적 권리로 법률 준수 여부 조사 및 감독, 교육·홍보, 정책지원·개발·자문, 자율규제를 위한 지침 권고, 그리고 최근에 일부 국가에서 도입되고 있는 사전 프라이버시 영향평가제도 실시 등이 있다. 또 사후적 권리로는 조사권·자료제출 요구권, 시정 조치, 분쟁 조정, 사법 당국에의 고발, 언론 공표권 등이 있다.

다. 국내 개인정보 보호기구의 현황과 평가

앞에서 살펴보았듯이 사회적 규제를 위해서도 이를 뒷받침할 전담 기구는 여전히 필요하다. 게다가 한국의 경우 아직 개인정보 보호에 대한 사회적 인식의 부족으로 사회적 규제의 기반이 될 자율 규제의 가능성이 취약하다. 때문에 적절한 국가의 역할이 강조되고 있다.

1) 국내 개인정보 보호 감독 기능에 대한 종합적 평가

국내 개인정보 보호 법제는 미국식의 분야별 보호 체계를 취하고 있다. 따라서 해당 법률을 담당하는 정부 부처가 분야별로 개인정보 보호 책임을 맡고 있다. 그러나 정보사회에서 정보는 정치 권력과 경제적 자원의 원천이다. 이러한 중요성에도 불구하고 행정 부처들은 자기 분야의 발전을 위해 개인정보 보호의 임무를 소홀히 하거나, 자의적으로 권한을 행사하는 경우가 많다는 점에서 문제가 있다.

특히 공공기관의 개인정보 보호를 전담하고 있는 행정자치부는 주민등록 데이터베이스를 비롯하여 가장 많은 개인정보를 수집하는 기관이다. 또한 인터넷 상의 개인정보 보호를 담당하는 정보통신부는 IT 산업의 발전을 책임지고 있는 기관이다. 금융기관의 개인정보는 금융감독원에서 담당하는데, 이 역시 상급 기관인 재정경제부의 정책적 판단에 따라 보호의 정도가 자의적으로 결

정된다.

2) 국내의 개인정보 담당기구의 현황과 평가

<표 37> 국내 프라이버시 보호기구 현황 (공공)

기관명	근거법률	관할범위	주요기능
개인정보보호심의위원회	공공기관의개인정보보호에관한법률	공공기관의 개인정보	정책 및 제도개선 사항 심의 공공기관 간 의견조정 사항 심의 법령 등의 정비·개선 사항 심의
행정자치부	공공기관의개인정보보호에관한법률	공공기관의 개인정보	각 기관의 개인정보 파일 보유 현황 접수/공고 의견제시·권고
국민고충처리위원회	민원사무처리에관한법률	행정기관 관련 민원 사무	민원 안내·상담 고충민원 조사·처리 위법·부당 처분에 대한 시정 권고 행정제도 및 운영의 개선에 대한 권고/의견 표명
인권위원회	국가인권위원회설립에관한법률	인권 침해 일반	법령·제도·정책·관행 조사·연구 개선 권고 및 의견 표명 침해 구제 지침의 제시·권고

이창범, 『현행 프라이버시 보호 담당기구의 성과와 한계』, 함께하는 시민행동 외 8개 시민사회단체 공동 주최, 『연속 워크숍 : 프라이버시 보호법제 개선의 쟁점들 - 제2회 워크숍 : 프라이버시 감독 체계의 개선 방안을 모색한다』 자료집

개인정보를 담당하는 기구로는 공공 영역을 담당하는 개인정보심의위원회와 민간 영역을 담당하는 개인정보분쟁조정위원회, 개인정보침해신고센터가 있다. 그러나 개인정보심의위원회는 행정자치부 차관이 위원장을 맡고 위원은 위원장이 추천하는 구조이다. 기능 또한 자문 기능 이상을 하지 못하고 있으며, 별도의 사무국도 없기 때문에, 행정자치부로부터 전혀 독립적이지 못하다. 실제로도 지난 5년간 단 3차례밖에 회의가 개최되지 않았으며 그 중 모여서 회의를 진행한 것은 1차례에 불과했다. 나머지 2차례는 서면심의로 대체되었다.[107]

107) 참여연대 보도자료, 『개인정보보호심의위원회, 지난 5년간 단 1차례 회의』, 2003. 8. 5.

한편 개인정보분쟁조정위원회는 정보통신부 장관이 위원장과 위원을 모두 정보통신부 장관이 임명한다. 예산 역시 정보통신부 산하 한국정보보호진흥원을 통해 지원되고 있다. 기능 역시 분쟁조정에 국한되어 있다. 개인정보침해신고센터는 정보보호진흥원이 운영하고 있으며, 상담, 고충 처리, 교육·홍보, 정보통신부 장관에 대한 자문 등 통상적인 개인정보 감독기구의 권한 중 일부를 수행하고 있다.

<표 38> 국내 프라이버시 보호기구 현황 (민간)

기관명	근거법률	관할범위	주요기능
개인정보분쟁조정위원회	정보통신망이용촉진 및정보보호등에관한 법률	민간의 개인정보	분쟁조정 신청·접수 사실 조사 및 청문 합의 권고, 분쟁 조정 위법사실 통보
개인정보침해신고센터	정보통신망이용촉진 및정보보호등에관한 법률	정보통신서비스 호텔, 항공사, 학원 등	상담 및 고충처리 교육 홍보, 기술적 자문
정보통신부	정보통신망이용촉진 및정보보호등에관한 법률	정보통신서비스 호텔, 항공사, 학원 등	법률 제·개정 및 기준 제정 시정 권고 및 명령 과태료 부과
금감위·금융감독원	신용정보의이용및보 호에관한법률	금융거래	상담 및 피해구제 시정권고 및 명령 기준제정
전자거래분쟁조정위원회	전자거래기본법	전자거래	상담 및 피해구제
한국소비자보호원	소비자보호법	소비자거래	상담 및 피해구제
민간소비자보호단체	소비자보호법	소비자거래	상담 및 피해구제

이창범, 『현행 프라이버시 보호 담당기구의 성과와 한계』, 함께하는 시민행동 외 8개 시민사회단체 공동 주최, 『연속 워크숍 : 프라이버시 보호법제 개선의 쟁점들 - 제2회 워크숍 : 프라이버시 감독 체계의 개선 방안을 모색한다』 자료집

이 외에 금융기관의 개인정보 침해에 대해서는 금융감독원이, 전자상거래상의 개인정보 침해에 대해서는 전자거래분쟁조정위원회가, 소비자 거래와 관

련된 경우는 소비자보호원 등이 직·간접적으로 관여하고 있다. 그러나, 전문성의 측면에서 개인정보 담당 기구로 보기에는 어려우며 소비자 보호기구 정도로 이해할 수 있다. 그리고 금융감독원의 경우, 독립성 차원에서도 재정경제부로부터 자유롭지 않다.

라. 문제 해결 방안 : 독립된 기구의 설치 및 통합 기능의 수행

한국의 개인정보 보호 기능이 원활하지 못한 것은 하나의 부처가 진흥의 업무와 규제의 업무를 동시에 수행하기 때문이다. 각 부처가 보유하고 있는 개인정보 보호 기능을 분리하여 독립적인 감독 기구로 통합할 필요가 있다.

앞서 설명한 바와 같이 기본권으로서의 자기정보통제권의 기본 정신과 원칙은 공공기관이나 민간 영역이나 동일하다. 그렇기 때문에, 단일한 감독기구가 개인정보 보호를 위해 활동할 필요가 있다. 물론, 민간 영역과 공공 영역에서 개인정보 처리 및 보호의 방식은 다소 다를 수 있다. 그러나 그 차이 역시 단일한 감독기관에 의해 자기정보통제권의 정신에 비추어 확인되어야 할 것이다. 게다가 최근 공공 영역과 민간 영역의 차이 역시 점차 희석되고 있는 상황이다.

기술적 차원에서도, 개인정보침해기술의 영향을 검토하고 적절한 규제 대책을 세우고 개인정보보호기술의 발전을 지원하는 것이 감독 기구의 중요한 역할 중 하나라는 점에서 기구 단일화가 필요하다.

따라서 현재 각 영역별로 분산되어 있는 개인정보 감독·보호 기능을 하나의 기구로 통합할 필요가 있다. 향후 정보사회의 진전에 따라 모든 영역에서 개인정보 보호의 중요성이 점차 확대되는 것이 필연적이므로 기구의 통합은 기능 수행 뿐 아니라 예산 차원에서도 오히려 바람직하다.

앞서 일반법 외에도 분야별로 개인정보 보호를 위한 개별법이 필요하다고 지적한 바 있다. 마찬가지로 고도의 전문성이 필요한 영역은 해당 부처에 개인정보 감독 기능을 위임할 수 있을 것이다. 그러나 이 경우에도 해당 부처들

의 업무 수행에 대해 독립된 개인정보 감독기구가 감독하거나 평가할 수 있는 권한이 보장되어야 할 것이다.

Ⅶ. 개인정보 보호를 위한 가이드라인

1. 새로운 원칙의 도입

앞에서 자기정보통제권이 맞닥뜨린 현실을 금융기관과 인터넷 기업들의 실태 검토 및 국내외 법제의 검토를 통해 살펴보았다. 그 근본적인 문제는 역시 자원과 권력을 독점한 정부·기업과 일반 정보주체 사이의 권력 불균등 및 정보 불균형을 해소하는 것이라 하겠다. 이 근본적 문제의 해결을 위해, 아래와 같은 새로운 방식의 자기정보통제권 구현 원리들이 제안될 수 있을 것이다.[108]

가. 집단적 참가의 원칙

개별 정보주체와 정보 수집자와의 계약을 바탕으로 하는 OECD 가이드라인은 개인 참가의 원칙을 채택하고 있다. 그러나 권력 불균형 상태를 해소하기 위해서는 정보 수집자에 대항하여 정보주체들이 집단적으로 권리 행사를 할 수 있게 해야 한다.

앞에서 말한 국가 차원의 개인정보 감독기구 역시 국가기구로 이해할 것이 아니라 국가에 대항하여 집단적 참가를 실현하는 기구로 이해되어야 할 것이다. 마찬가지로 소비자는 기업의 개인정보 수집에 대해 그리고 노동자는 고용주의 개인정보 수집에 대해 집단적으로 협의·감독할 권리를 가져야 하며, 이를 위한 정보주체 단체를 구성할 권리를 가져야 한다.

---

108) 아래에 제시되는 원칙들은 정보사회세계정상회의(WSIS)를 위한 시민사회네트워크가 2003년 5월에 발표한 『정보사회에 대한 한국 시민사회 선언문』(http://www.wsis.or.kr/principle.html)에 담겨진 내용이다.

나. 분산의 원칙

정보수집자의 정보 수집이 대규모로 이루어지면 이루어질수록 개별 정보주체의 자기정보통제권은 실현되기 어려워진다. 뿐만 아니라, 데이터베이스가 거대화되고 통합될수록 빅브라더의 실현 가능성은 높아진다. 따라서 개인정보는 수집 목적 - 물론 이 수집 목적은 정당한 동의를 얻은 목적이어야 한다 - 을 달성할 수 있는 한에서는 최대한 분산되는 것이 바람직하다. 개인정보의 통합 시스템이 가져다 줄 수 있는 편리함의 이면에는 개인의 프라이버시에 대한 위협이 놓여있기 때문에 개인정보의 데이터베이스는 가능한 한 분산화될 필요가 있다.

따라서 개인정보의 경우 원칙적으로 수집된 목적 이외에는 공유하지 않는 것이 바람직하며, 반드시 공유해야 하는 상황이라 하더라도 공유의 폭을 최소화하는 방식을 택해야 할 것이다. 이러한 원칙에 입각한다면, 국가가 담당해온 개인정보 관련 사무는 가급적 지방자치단체의 사무로 이전해야 할 것이다. 이는 시대적 요청이 되고 있는 자치와 분권이라는 정책 방향에도 부합한다.

다. 회피의 원칙

프라이버시를 침해하지 않거나 혹은 덜 침해하면서 감시 목적을 달성할 수 있는 다른 방법이 있는 한 감시 행위를 회피할 수 있는 선택의 여지가 주어져야 한다. 그러나 감시 주체와 감시 대상 사이의 정보의 불균형으로 인해 감시 대상자들은 감시 행위가 감시 대상의 인간 존엄성을 발전시키는 데 있어 필수불가결한 것인지를 판단하기 어렵다.

따라서 정보 수집 행위에 대한 공적 평가가 이루어져야 한다. 새로운 감시 장비가 도입될 때, 새로운 개인정보 데이터베이스가 구축될 때, 기존의 데이터베이스들이 연동될 때에는 이 감시 행위가 필수불가결한 것인지 그리고 프라이버시에 미칠 악영향이 어느 정도인지를 평가하는 프라이버시 영향평가제도

를 도입해야 한다.

라. 정보 주체의 법적 대응 능력 보완

정보주체와 정보 수집자 사이에 분쟁이 발생했을 때, 최종 해결은 법정에서 이루어지게 된다. 그러나 사법 절차는 많은 비용이 소모되기 때문에 개별 정보주체로서는 쉬운 선택이 아니다. 또한 결정이 이루어질 때까지 기간도 매우 오래 걸리므로 정보주체의 개인정보 침해상태를 장기간 지속시키는 결과를 낳는다. 이러한 문제를 해결하기 위해 손쉽게 피해 구제를 받을 수 있도록 대안적 분쟁조정제도를 도입하는 것이 필요하다.

또 개인정보 침해는 수많은 사람을 대상으로 동시에 이루어지기 때문에 개별 정보주체에 대한 배상에 소요되는 비용보다 개인정보 침해로 얻는 이익이 훨씬 크다. 이 문제를 해결하기 위해 집단소송제도를 고려할 필요가 있다. 한 사람의 정보주체가 배상 판결을 받으면 다른 정보주체들은 긴 소송과정을 거치지 않고도 동일한 판결을 받을 수 있게 함으로써 정보 수집자의 개인정보 침해를 예방할 수 있다.

2. 핵심적 정책 과제

이번 연구를 통해 자기정보통제권을 심각하게 위협하는 몇 가지 우리 사회 고유의 관행들이 발견되었다. ▲ 주민등록번호의 수집 ▲ 개인정보 공유에 대한 포괄적 동의 방식 ▲ 개인정보보호정책/약관에 대한 이해 부족 등이 그것이다. 이에 대해서는 법제의 정비, 지침의 마련, 교육 등을 통해 적절한 해결책이 제시되어야 할 것이다.

가. 개인정보 일반법의 제정 및 독립적 감독기구 설치

앞에서도 설명했듯이, 우리 사회의 개인정보 보호 체계 자체에 대한 재검토가 필요하다. 공공 영역과 민간 영역을 동일한 원리 하에 규율하는 개인정보 일반법을 제정함으로써 ▲ 현재 분야별 보호법제 안에 포괄되지 않는 분야들을 보호의 대상으로 포괄할 수 있고 ▲ 공공 영역과 민간 영역의 구분이 흐려짐으로써 인한 책임 소재의 불분명함을 해소할 수 있을 것이다.

또한 개인정보를 활용하는 정부 부처들이 보호의 책임까지 담당함으로써, 자의적으로 감독 임무를 소홀히 하는 문제점을 해결하고, 정보주체가 자기정보를 스스로 통제해야 한다는 자기정보통제권의 원리를 공공 영역과 민간 영역에 공히 적용하기 위해서는 독립적 감독 기구를 설치해야 한다.

신설될 독립적 감독기구는 우선, 감독기구들의 전통적 임무인 ▲ 각 분야의 개인정보 보호 실태 조사 ▲ 개인정보 보호 교육의 실시 ▲ 주요 법제와 정책에 대한 의견 제시 등을 담당해야 한다. 또한 시대적 변화에 걸맞게 ▲ 개인정보 관련 분쟁을 신속히 처리할 수 있는 '대안적 분쟁 조정 기능'과 ▲ 신기술 및 개인정보 데이터베이스 연동으로 인한 프라이버시 침해 가능성을 사전에 평가하는 '프라이버시 영향평가제도 실시 기능'을 가져야 할 것이다.

아울러 앞서도 지적했듯이, 개인정보 보호를 전적으로 감독기구에 의존할 경우 효율성과 능력 면에서 한계를 보일 수밖에 없다. 시민사회가 스스로 감독기구의 역할을 할 수 있도록 하기 위해 선진국에서 시도하고 있는 사회적 규제의 도입을 적극 검토해야 한다. 개인정보 보호에 대한 집단소송제의 도입이나 소비자 단체·정보보호 단체들에 분쟁조정 권한을 부여[109]하는 것 등이 검토될 필요가 있다.

---

109) 정상호, 『일본 개인정보보호법(안)에 대한 고찰』, pp. 34-35.

나. 주민등록번호 수집 관행 시정

이번 연구에서 조사된 거의 모든 웹 사이트(조사 대상 사이트의 92.5%)가 주민등록번호를 수집하고 있었다. 이는 크게 두 가지 요인에서 기인한다. 하나는 주민등록번호가 전 세계에서도 유래 없는 평생 불변의 고유 식별번호라는 점이다. 때문에 주민등록번호는 개인정보 데이터베이스의 연동을 위한 효율적인 매칭 키가 된다. 다시 말하면 주민등록번호가 없는 개인정보 데이터베이스는 그 상업적 가치가 매우 감소한다는 것이다.

또 하나는 주민등록법 상의 신분확인 조항 때문이다. 주민등록법 제17조의9는 모든 영역에서 신분확인을 위해서는 주민등록증을 사용하도록 규정하고 있다.

주민등록법

제17조의9 (주민등록증에 의한 확인<개정 1999.5.24>) ①국가기관·지방자치단체·공공단체·사회단체·기업체등에서 그 업무를 수행함에 있어 다음 각호의 1에 해당하는 경우에 17세이상의 자에 대하여 성명·사진·주민등록번호 또는 주소의 확인을 필요로 하는 때에는 증빙서류를 첨부하지 아니하고 주민등록증에 의하여 이를 확인하여야 한다. 다만 대통령령으로 정한 경우에는 그러하지 아니하다.[110]<개정 1999.5.24>

110) 주민등록법 시행령 제36조에서는 주민등록증을 이용하지 않고 신분확인을 할 수 있는 경우를 다음과 같이 제한하고 있다.

주민등록법 시행령

제36조 (주민등록증에 의한 확인) ①법 제17조의9 단서의 규정에 의하여 국가기관·지방자치단체·공공단체·사회단체 또는 기업체등에서 17세 이상의 자에 대하여 성명·사진·주민등록번호 또는 주소의 확인을 필요로 하는 때에 주민등록증에 의하지 아니하고 증빙서류에 의하여 확인할 수 있는 경우는 다음 각호와 같다.

1. 민원서류 기타 서류를 우송의 방법으로 제출한 경우
2. 주민등록증의 발급 또는 재발급을 받지 못하여 주민등록증을 소지하지 아니한 경우
3. 법령에 의하여 증빙서류를 제출하도록 되어 있는 경우. 다만, 증빙서류를 제출하

1. 민원서류 기타 서류를 접수할 때
2. 특정인에게 자격을 인정하는 증서를 발급할 때
3. 기타 신분을 확인하기 위하여 필요할 때

이러한 관행이 온라인에서도 그대로 이어진 탓에, 모든 웹 사이트가 주민등록번호를 통해 신원을 확인하는 것으로 보인다.

그런데 이처럼 주민등록번호의 수집이 지나치게 광범위하게 이루어지는 탓에 발생하는 문제점이 최근 심각한 사회 문제로 떠오르고 있다. 가장 일반적으로 일어나는 문제는 타인의 성명과 주민등록번호를 알아내서 그 사람의 명의로 웹 사이트에 가입하는 것이다. 현재까지 이로 인해 발생한 직접적인 피해가 드러난 경우는 별로 없지만, 오프라인(off-line) 상에서는 개인의 신분을 도용해서 일어난 금융사고가 흔히 있어왔었다. 이러한 피해가 온라인에서 일어날 가능성은 충분히 있다. 또한 비록 물질적 피해는 아니라고 하더라도 어떤 개인의 명의를 도용한 가공의 인물이 온라인상에서 하는 여러 비합리적 비도덕적 행위로 인해 정신적 피해를 가져 올 수 있을 것이다. 다른 개인의 신분을 도용했다는 것이 이미 비도덕적 행위를 온라인에서 일으키겠다는 의지의 표현으로 이해될 수 있을 것이다. 실제로 주민등록번호 등 신상명세가 유출되어 50여 곳의 성인사이트에 자기도 모르게 가입된 경우가 최근 언론에 보도된 바 있다. 이 사람은 각종 음란성의 스팸 메일이 날아들어 상당한 정신적 피해를 겪었다고 한다.[111] 앞의 설문조사에서도 전체 응답자의 26.4%가 주민등록번호를 도용당하여 웹 사이트에 가입하지 못한 것으로 나타났다.([그림 6] 참조)

더욱 문제가 되는 것은 주민등록번호와 성명을 입력하면 아이디와 비밀번호를 알려주는 사이트가 많다는 점이다. 이를 이용하여 타인의 이메일을 훔쳐보

게 하는 법령을 제정하고자 하는 때에는 주무부장관은 행정자치부장관과 협의하여야 한다.

4. 기타 주민등록증으로 확인이 불가능한 경우

111) 한겨레신문 2003년 10월 6일자.

는 등의 사생활 침해가 발생한다. 이는 특히 잘 아는 사이에서 자주 발생하는 문제이다. 도용한 성명과 주민등록번호로 신용카드를 발급하는 등의 물질적 피해를 발생시키는 경우도 있다.

최근 함께하는 시민행동이 자체 웹 사이트 상의 프라이버시 침해 제보게시판에 올라온 상담글들을 분석한 결과에서도 주민등록번호 유출과 관련된 내용이 전체의 25.9%를 차지하고 있었다.[112]

앞서 말했듯이, 주민등록번호는 평생불변의 전국민 고유 식별번호이다. 따라서 일단 유출되면 사실상 권리 회복이 되지 않는다. 그럼에도 너무 많은 곳에서 주민등록번호를 신원 확인정보로 사용하고 있어서, 일단 번호가 유출된 사람들은 피해를 막을 방법이 없다. 따라서 현행 주민등록번호 제도에 대한 근본적인 재검토가 필요하다. 그 방향은 두 가지여야 할 것이다.

첫째, 앞에서도 말했듯이 평생불변의 고유 식별번호라는 점에서 일단 번호가 유출된 피해자의 경우 권리 회복이 불가능하다. 따라서 주민등록번호의 재부여를 가능하게 해야 한다. 둘째, 주민등록번호의 민간 수집을 최소화해야 한다. 앞에서도 지적하였듯이, 현재 대부분의 웹 사이트에서 주민등록번호의 수집을 반드시 해야 할 당위성은 부족하다. 만약 주민등록번호 재발급이 가능해지면 기존에 수집한 주민등록번호 정보는 아무 의미가 없어질 것인데, 그렇다고 주민등록번호를 변경할 때마다 가입한 모든 웹 사이트를 찾아다니면서 주민등록번호 변경을 하는 것도 가능하지 않다. 따라서 주민등록번호는 반드시 수집해야 할 최소한의 경우를 제외하고는 수집하지 못하도록 하는 것이 바람직하다.

다. 개인정보 공유에 대한 포괄적 동의 방식 시정

설문조사에서 응답자가 가장 자주 이용하는 웹 사이트들의 개인정보 공유

112) 함께하는 시민행동 보도자료, 『인터넷시대 개인정보보호를 위한 발상의 전환 - '주민등록번호를 바꾸자'』 2003.10. 6

현황에 대해 질문을 했으나, 알고 있다고 응답한 경우가 평균 9.5%에 불과했다. 가장 자주 이용하는 사이트에 대해서도 그런 응답이 나왔다는 것은 개인정보 공유 문제에 대해 자기정보통제권이 전혀 구현되지 못하고 있음을 의미한다. 사실 자기 정보가 어떻게 유통되는지에 대해 개별 정보주체들이 전혀 확인할 수 없는 상황인 것이다.

이는 크게 두 가지 문제에서 기인한다. 먼저 정보 수집자들이 개인정보 제3자 공유 문제에 대해 정보주체에게 정확하게 고지하지 않고 있다는 점이다. <표 25>를 보면 조사 대상 사이트들 중 개인정보를 공유하는 기업의 명칭을 밝히고 있는 곳은 12개(17.9%)에 불과했다. 나머지 82%의 경우는 "서비스 증진을 위해 제휴사들과 개인정보를 공유할 수 있다"는 식으로만 서술하거나 아예 관련 사항에 대한 언급이 없었다. 자기정보에 대한 기본적 알 권리조차 실현되지 않고 있는 상황인 것이다.

또 하나는 역시 포괄적 동의라는 동의 방식의 문제이다. 조사 대상 웹 사이트들 중에 개개의 공유 대상 기업별로 선택적 동의를 받고 있는 곳은 전혀 없었다. 대부분의 사이트가 약관에 대한 동의로 동의 절차를 갈음하고 있었으며, 별도의 동의 절차를 마련한 일부 사이트들의 경우에도 개인정보 공유에 대한 정보 주체의 동의를 공유대상 기업 각각에 대해 따로 받는 경우는 없었다. 즉, 정보 주체들이 제3자 공유에 대해 어떤 선택권도 갖고 있지 못하는 상황인 것이다. 선택을 할 권리를 보장받지 못하기 때문에 그나마 주어진 알 권리조차도 적극적으로 활용하지 않게 되는 결과를 가져온다.

따라서 제3자 공유 문제의 중요성을 감안하면 약관에 대한 동의 절차와 개인정보 공유에 대한 동의 절차를 분리하여 제시하고, 각각의 공유 대상에 대해 동의 여부를 선택할 수 있도록 보장할 필요가 있다. 또한 관련 법률에서도 이용자들의 선택적 동의권을 명문화해야 한다.

라. 개인정보보호정책 및 약관 개선

이번 조사를 통해 제3자 공유 문제뿐만 아니라 전반적으로 약관과 개인정보보호정책에 대한 이용자들의 이해 정도가 매우 낮음을 확인할 수 있었다. [그림 9]부터 [그림 12』까지의 설문조사 결과를 살펴보면, 약관에 대해서는 57.0%의 응답자가, 개인정보보호정책에 대해서는 55.9%의 응답자가 거의 읽지 않는다고 응답했으며, 꼼꼼히 읽어보는 편이라고 대답한 응답자는 각각 8.3%와 11.3%에 불과했다. 또한 잘 읽지 않는 이유에 대해서는 양이 지나치게 많다는 응답이 각각 53.2%와 47.8%로, 어느 사이트나 내용이 거의 같기 때문이라는 응답이 각각 21.9%와 22.3%로 나타났다. 이런 응답 결과는 약관이나 개인정보보호정책이 정보주체들이 쉽게 이해할 수 있는 방식으로 제시되지 않고 있으며, 구체적 정보도 주지 않고 있음을 뜻한다.

약관은 그렇다 치더라도 개인정보보호정책은 이용자들이 개인정보 관련 사항을 쉽게 파악할 수 있도록 하기 위해 작성된 것이다. 따라서 한 편으로는 쉽게 작성되어야 하고 다른 한 편으로는 상세하고 구체적으로 작성되어야 한다.

서로 상충되는 듯 보이는 이 두 가지 문제를 해결하기 위해서는 약관이나 개인정보 보호정책을 2단계로 분리하여 제시하는 것이 바람직하다. 1단계는 매우 개괄적으로 작성하야 이용자가 읽기 쉽도록 제시할 필요가 있다. ▲ 개인정보의 보존 연한 관련 정보, ▲ 제3자 공유 관련 정보, ▲ 이용 요금 관련 정보, ▲ 개인정보관리책임자 관련 정보 등 해당 사이트에 고유한 정보들을 중심으로 정책을 제시함으로써 이용자들이 한 눈에 정보를 파악할 수 있게 한다. 이어서 2단계에서는 모든 사이트들이 유사하게 갖고 있는 개인정보보호정책의 전체 내용을 제시하는 것이다. 이 부분은 반드시 따로 제시할 필요는 없을 것이다. 1단계에서 더 자세한 내용 보기와 같은 메뉴를 두고 링크로 연결하는 것도 한 가지 방법일 것이다.

3. 개인정보 보호를 위한 일반 원칙

여기서는 개인정보 보호를 위해 우리 사회가 가져야 할 일반적인 원칙들을 가이드라인으로 제시한다. 즉, 개인정보 보호를 위한 일반법에 담겨야 할 내용들이 제시될 것이다.

가. 개인정보의 수집에 관한 원칙

1) 개인정보의 수집은 법률 혹은 당사자의 동의에 의해서만 수집되어야 한다.

개인정보의 수집은 기본적으로 정보 주체의 동의에 의해서만 가능해야 한다. 그러나 국가가 정책을 수행하기 위해 개인정보를 수집하는 경우는 일일이 개별 정보주체의 동의를 받는 것이 불가능하다. 따라서 국민의 대표자들로부터 집단적 동의를 구하는 과정을 거쳐야 한다. 즉, 국민의 대표자인 의회에 의해 통과된 법률에 따라 수집해야 함을 의미한다.

2) 동의에 의해 개인정보를 수집할 때는 정보주체가 부분적으로 동의를 거부할 권리를 최대한 보장해야 한다.

개인정보는 목적에 따라 수집해야 한다. 그런데 많은 경우 복수의 수집 목적에 대해 하나의 개인정보 수집 절차를 통해 동의를 받게 된다. 이 경우, 이용자들이 개개의 목적에 대해 별도로 동의 여부를 결정할 수 있도록 보장해야 한다.

3) 법률에 의해 개인정보를 수집할 때도 정보주체들에게 적절한 고지가 이루어져야 한다.

범죄의 수사 및 각종 불법 행위의 조사, 정책 집행 등을 위해 국가가 법률에 따라 개인정보를 동의 없이 수집하는 것은 불가피한 일이다. 그러나 이에 대한 통제 장치가 없다면, 임의적인 개인정보 수집이 남발될 것이다. 따라서

법률에 따라 개인정보가 수집되는 경우에도 당사자들에 대한 적절한 고지가 이루어져야 할 것이다.

4) 불법적이고 임의적인 차별을 유발할 수 있는 개인정보나 개인의 내밀한 사생활과 직결된 정보는 수집되어서는 안 된다.

EU의 1995년 개인정보보호지침은 단체/노동조합 가입 사항 뿐 아니라 인종적, 민족적 출신, 피부색, 성생활, 정치적 의견, 종교, 철학적 혹은 기타의 신념에 대한 정보 등을 불법적이고 임의적 차별을 유발할 수 있는 개인정보로 규정하여 수집을 금지하고 있다. 이러한 정보의 경우 해당 단체나 조합 혹은 교단 등에서만 수집하도록 해야 하며, 이런 정보의 유출에 대해서는 특히 엄격한 제재가 이루어져야 한다.

그 외에도, 의료 정보나 재산·금융거래 정보 등은 개인의 사생활과 매우 밀접한 관계가 있는 정보이므로 진료 기관이나 금융 기관 등 정보의 발생에 직접 개입한 기관 이외에는 수집해서는 안 된다. 다만, 사회적 필요에 의해 다른 기관이 수집할 필요가 인정되는 경우는 법률적 근거에 의하여 수집해야 할 것이다.

나. 개인정보의 수집 목적 제시에 관한 원칙

1) 개인정보의 수집은 목적에 부합하는 최소한의 정보에 국한되어야 한다.

개인정보를 수집할 때는 그 개인정보를 이용 목적에 맞는 정보들만을 수집해야 한다. 또한 수집 목적과 관련이 있는 정보라고 해서 무제한적으로 수집되어서는 안 되며, 그 목적을 달성하기 위해 필요한 최소한의 정보만이 수집되어야 한다.

2) 개인정보를 수집할 때는 개별 항목별로 이용 목적을 제시해야 한다.

정보 수집자는 이용자들이 개인정보 수집의 정당성을 확인할 수 있도록, 개

인정보의 수집 목적과 수집되는 개별 정보 항목을 직접 연결시켜 설명할 수 있어야 한다.

다. 개인정보의 이용 및 제3자 제공에 관한 원칙

1) 사전에 명시한 수집 목적에 부합하지 않는 방식으로 개인정보를 이용해서는 안 된다. 사전에 명시하지 않은 목적으로 개인정보를 이용하고자 할 때는 새로이 정보주체로부터 동의를 얻어야 한다.

개인정보를 제공할 때는 그 목적을 제시한 후 동의를 받도록 되어 있다. 때문에 사전에 명시하지 않은 목적으로 개인정보를 사용하는 것은 정보 주체의 동의권을 침해함을 의미한다. 개인정보 이용의 목적을 변경하고자 할 때 혹은 새로운 목적으로 사용하고자 할 때는 반드시 당사자의 명시적 사전 동의를 얻어야 한다.

2) 사전에 명시된 수집 목적이 변경되지 않는 양수·양도의 경우에도 사전에 고지가 이루어져야 한다.

기업이나 정부에서 개인정보를 수집했다가 운영의 주체가 변경되는 경우가 발생할 수 있다. 이 경우 사전에 명시된 수집 목적이 변경되지 않는 경우라면, 굳이 새롭게 동의 절차를 받을 필요는 없을 것이나 반드시 수집 주체의 변경에 대해서는 고지가 이루어져야 한다. 고지의 방식은 정보 주체들이 충분히 인지할 수 있는 적절한 기간과 매체를 이용해야 하므로, 구체적 내용을 법령에 규정할 필요가 있다.

라. 개인정보의 보유 및 파기에 관한 원칙

1) 개인정보는 그 수집 목적이 달성된 후 혹은 당사자의 동의가 철회된 후에는 반환 혹은 파기해야 한다.

개인정보를 무한 축적할 경우에는 개인에 대한 연대기적 재구성이 가능해진다. 이는 프라이버시에 대한 중대한 위협을 의미한다. 또한 수집 목적이 달성된 후에도 개인정보를 보유하는 것은 최초 수집 목적에 위배되는 것이므로 당사자의 동의권을 침해하는 결과가 된다. 따라서 개인정보의 수집 목적이 달성된 후 혹은 당사자의 동의가 철회된 경우에는 반드시 개인정보를 파기해야 한다. 다만, 거래의 투명성 확보나 분쟁에 대한 대비 등 사회적 필요에 의해 법률로 일정 기간 보관을 규정한 경우는 예외로 한다.

2) 개인정보를 수집할 때는 보유 기간을 명시해야 한다.

개인정보를 수집할 때 보존 기간을 명시한 상태에서 동의를 얻어야 한다. 그렇지 않을 경우, 당사자로서는 동의 철회만으로 파기가 이루어진다고 잘못 이해하게 된다. 기본적으로 수집 목적의 달성 후 또는 동의 철회 후에는 파기한다고 명시해야 하며, 예외적으로 법률이나 기타 서비스의 목적 상 일정 기간 보관하고자 한다면 수집에 대한 동의를 얻기 전에 그 기간을 정확하게 공지해야 한다.

3) 개인정보의 보유 기간은 보유 목적에 부합하게 설정해야 한다.

보유 목적에 필요한 기간 이상으로 개인정보의 보유 기간을 설정하는 것은 목적에 따른 개인정보 수집 및 이용이라는 원칙에 위배되는 행위이다. 그러므로 보유 기간은 보유 목적에 맞게 정해져야 한다.[113]

113) 앞에서 살펴보았듯이, 해지 후 재가입비 면제, 가입자와의 거래내역 분쟁 해결, 손해배상청구권의 시효 완성 등의 이유로, 이동전화사들이 해지자 가입정보를 10년간 보관하고 있음이 드러났다. 그러나, 해지 후 재가입비 면제의 경우 그 혜택이 3년에 불과한데도 10년간 정보를 보관하는 것은 파기 의무에 대한 위반이다. 함께하는 시민행동 외 7개 단체, 『독립적 개인정보 보호기구 설치를 촉구하는 정당·시민사회 기자회견 자료집』 중

마. 정보처리 과정에 대한 개별 정보주체의 참가 보장에 관한 원칙

1) 정보주체는 자기 정보에 대한 존재 여부를 확인할 권리를 갖는다.

정보주체는 특정 정보수집자에 대해 자기 정보에 대한 존재 여부를 확인해 줄 것을 요구할 수 있어야 한다. 정보수집자는 존재 여부에 대한 응답을 거부하거나 허위로 답변해서는 안 된다.

2) 정보주체는 정보 수집자가 자기 정보를 취득하게 된 경위를 확인할 권리를 갖는다.

정보주체는 자기 정보가 정상적 경로를 통해 유통되고 있는지를 확인할 수 있어야 한다. 정보 수집자는 이 확인 요청에 대한 응답을 거부할 수 없으며, 응답하지 않는 경우는 동의 없는 수집과 동일한 제재를 받아야 한다.

3) 정보주체는 정보 수집자에 의해 보관된 자기 정보를 열람할 권리를 갖는다.

정보주체는 정보 수집자가 자신에 대한 정보를 정확하게 유지하고 있는지 또는 사전에 동의하지 않은 목적으로 수집된 정보가 없는지 등을 확인할 수 있어야 한다.

4) 정보주체는 잘못된 자기 정보를 정정할 권리를 갖는다.

정보주체는 정보 수집자가 보관하고 있는 자기 정보의 오류를 수정할 수 있어야 한다. 정보 수집자는 정당한 수정 요청을 거부함으로써 발생한 정보주체의 피해에 대해 책임을 져야 한다.

5) 정보주체는 수집에 대한 동의를 철회할 권리 및 부분적으로 삭제할 권리를 갖는다.

정보주체는 개인정보 수집에 대한 동의를 자유롭게 철회할 수 있어야 한다. 수집 목적 이외의 정보가 수집되었을 경우에는 해당 정보에 대한 삭제를 요구

할 수 있어야 한다. 또한 정당한 목적을 가지고 수집된 정보라 하더라도, 그 정보의 수집 행위가 정보주체에게 부당한 피해를 주는 경우에는 해당 정보의 삭제를 요구할 수 있다. 정보 수집자는 법률에 의하지 아니하고는 정보주체의 동의 철회를 거부할 수 없다.

바. 정보의 유지에 관한 원칙

1) 정보 수집자는 수집된 개인정보를 최신의 상태로 유지해야 한다.

정보 수집자는 늘 최신의 정보 상태를 유지하기 위해 노력해야 한다. 정보 수집자가 부정확한 정보를 이용함으로써 정보주체에게 피해가 발생할 경우 정보 수집자가 책임을 져야 한다.

사. 정보의 안전성 확보에 관한 원칙

1) 정보 수집자는 수집된 정보의 안전을 위해 기술적·관리적 조치를 취해야 한다.

정보 수집자가 정보를 부당하게 사용하지 않으려 노력하더라도, 내부의 정보 취급자에 의한 유출이나 외부의 침입에 의한 유출이 발생할 경우 정보주체의 자기정보통제권은 침해받게 된다. 따라서 정보 수집자는 정보를 안전하게 보관하기 위한 기술적·관리적 조치를 취해야 한다.

2) 정보수집자는 수집된 개인정보를 취급하는 인원을 최소화해야 한다.

상당수의 개인정보 침해는 정보에 접근할 수 있는 내부자에 의해 발생한다. 따라서 정보수집자는 수집된 정보에 접근할 수 있는 인원을 최소화해야 하며, 역할에 따라 접근의 권한을 적절하게 배분해야 할 것이다. 또한 정보 취급자에 대한 적절한 교육이 이루어져야 한다.

3) 정보수집자는 개인정보의 이용에 대한 기록을 유지해야 한다.

정보수집자는 수집된 개인정보에 대한 접근이 이루어질 때, 접근 주체, 접근의 목적, 접근된 정보의 내용, 접근 형태(열람, 데이터 매칭 등) 등에 관한 기록을 유지해야 한다.

아. 개인정보 수집과 관련된 사항의 공개의 원칙

1) 정보 수집자는 정보 수집시 정보주체에게 정보의 수집, 이용, 보유와 관련된 일반적 사항을 공개해야 한다.

정보 수집자가 정보 수집시 정보주체에게 공개해야 하는 일반적 사항에는 수집하고 있는 개인정보의 목록 및 세부 내용(수집 목적, 수집 항목, 보존 연한, 제3자 제공 여부 등), 수집된 정보의 보호를 위한 기술적·관리적 대책, 이용자의 권리, 불만 처리 사항 등이 포함되어야 한다.

2) 일정 규모 이상의 정보 수집자는 위의 내용을 전자적 방식으로 상시 공개해야 한다.

공공기관이나 일정 규모 이상의 개인정보 데이터베이스를 축적한 민간 법인의 경우, 웹 사이트의 개인정보보호정책을 통해서 위의 내용을 상시 공개해야 한다. 이런 의무를 지니는 민간 법인에 대해 법률로 규정할 수 있다.

3) 정보 수집자는 개인정보 이용에 관한 기록을 정보주체 및 감독 기관에 공개해야 한다.

정보 수집자는 정보주체나 감독 기관의 열람 요청이 있을 경우 개인정보 이용에 관한 기록을 공개해야 한다.

자. 정보 수집자의 책임에 대한 원칙

1) 정보 수집자는 개인정보 관리 책임자를 지정하여 개인정보 보호를 위한 제반 규정을 준수할 임무를 부여해야 한다.

차. 개인정보 데이터베이스의 분리에 관한 원칙

1) 개인정보 데이터베이스는 가급적 분산하여 구축해야 한다.

개인정보는 통합될수록 정보의 축적에 따른 위험성이 증가한다. 또한 정보주체와의 권력 불균형도 증가한다. 따라서 수집 목적을 달성할 수 있는 한에서는 가능한 한 분리하여 구축해야 한다.

2) 구축된 개인정보 데이터베이스는 사전에 명시된 목적에 의하지 않고 연동해서는 안 된다.

구축 당시 명시한 목적 이외의 목적으로 둘 이상의 개인정보 데이터베이스를 연동하는 것은 자기정보통제권을 침해하는 행위이다. 구축 목적의 변경 혹은 새로운 목적으로 연동하고자 할 경우에는 정보 주체의 동의를 다시 얻어야 한다.

카. 사전 개인정보 영향평가제도의 실시에 관한 원칙

1) 일정 규모 이상의 개인정보 데이터베이스를 구축·통합·연동할 때는 사전 영향평가를 의무적으로 실시해야 한다.

공공기관이나 일정 수 이상의 개인정보 데이터베이스를 구축한 법인, 일정 수 이상의 직원을 고용하고 있는 법인이 개인정보에 관련된 새로운 시스템을 도입할 경우 프라이버시에 미칠 수 있는 악영향에 대한 사전 평가가 이루어져야 한다. 이 평가에는, 해당 정보수집의 목적을 달성할 수 있으면서도 보다 프

라이버시 침해가 적은 방식이 있는지에 대한 평가가 포함되어야 한다.

2) 개인정보 보호에 영향을 미칠 수 있는 새로운 기술 및 서비스에 대해서도 사전 영향평가가 실시되어야 한다.

개인정보에 영향을 미칠 수 있는 기술에 대해 사전 영향평가가 이루어지게 함으로써, 이후 그 기술을 활용하는 경우에 대한 평가의 기준을 마련해야 한다.

타. 감사[114]에 관한 원칙

1) 일정 규모 이상의 개인정보 데이터베이스를 보유하고 있는 정보 수집자는 정기적으로 내부 감사를 실시해야 한다.

공공기관이나 일정 수 이상의 개인정보 데이터베이스를 구축한 법인, 일정 수 이상의 직원을 고용하고 있는 법인은 개인정보와 관련된 내부 감사를 정기적으로 실시해야 한다. 감사는 개인정보 관리책임자에 의해 수행되어야 하며, 감사 결과는 감독기구에 의해 등록 및 고지되어야 한다.

2) 일정 수 이상의 정보주체의 발의가 있을 경우 정보수집자는 정보주체들의 대표 혹은 정보주체들이 지정한 개인정보보호 전문기관이나 단체로부터 감사를 받아야 한다.

정보주체들의 역감시권을 보장하기 위해, 법률로 규정된 일정 수 혹은 일정 비율 이상의 정보주체들이 연명으로 발의한 경우에는 정보 수집자가 이들로부터 개인정보 관리 실태에 대한 감사를 받아야 한다. 정보주체들은 전문적 능력을 가진 개인정보 보호기관이나 단체에 감사를 의뢰할 수 있다. 이 때, 감사

114) 개인정보 영향평가와 감사는 목적 뿐 아니라, 실제 내용에서도 차이가 있다. 감사는 명백한 불법 및 규칙 위반 사항에 대하여 조사하는 것이지만, 개인정보 영향평가는 잠재적인 부정적 영향을 밝히는 것이 포함된다.

를 대리하는 기관은 감독기구에 등록되어 있어야 한다.

파. 분쟁조정에 관한 원칙

1) 국가는 정보주체들이 손쉽게 개인정보에 대한 불만을 처리할 수 있도록 분쟁조정 제도를 마련해야 한다.

많은 비용과 긴 소송 기간이 소요되기 때문에, 사법 절차는 효과적인 개인정보 보호 수단이 되기 어렵다. 따라서 정보주체들이 빠른 시일 내에 저렴한 비용으로 개인정보 보호에 관한 분쟁을 해결할 수 있도록 국가는 대안적 분쟁조정제도를 도입해야 한다. 정보수집자가 분쟁조정 결과에 불복하는 경우, 분쟁조정기구가 정보주체의 소송 행위를 지원해야 한다.

하. 집단소송제 도입에 관한 원칙

1) 국가는 개인정보 관련 소송에 대해 집단소송제를 도입하여야 한다.

개인정보 침해는 수많은 사람을 대상으로 동시에 이루어지기 때문에 개별 정보주체에 대한 배상에 소요되는 비용보다 개인정보 침해로 얻는 이익이 훨씬 크다. 집단소송제도를 도입하여, 한 사람의 정보주체가 배상 판결을 받으면 다른 정보주체들은 긴 소송과정을 거치지 않고도 동일한 판결을 받을 수 있게 해야 한다.

갸. 개인정보 관리책임자의 지정에 관한 원칙

1) 일정 규모 이상의 개인정보 데이터베이스를 구축하는 기관은 개인정보 관리책임자를 지정하여 개인정보 보호의 임무를 맡게 해야 한다.

공공기관이나 일정 수 이상의 개인정보 데이터베이스를 구축한 법인, 일정 수 이상의 직원을 고용하고 있는 법인은 개인정보관리책임자를 지정하여야 한

다.

2) 개인정보관리책임자에게는 지위와 역할의 독립성을 보장해야 한다.

개인정보관리책임자에게는 감사의 수준에 준하는 지위의 독립성이 보장되어야 한다. 임기가 보장되어야 하며, 임무 수행에 대한 보복 조치로서의 해고를 법률로 금지해야 한다. 또한 업무의 독립성이 보장되어야 한다.

3) 개인정보관리책임자에게 그 직무 수행에 필요한 적절한 권한과 의무를 부여해야 한다.

개인정보관리책임자는 ▲ 개인정보 보호를 위한 업무 프로세스 제안, ▲ 개인정보 보호에 관한 내부 감사, ▲ 내부 교육, ▲ 내부 불법 행위에 대한 고발, ▲ 개인정보 수집 및 이용 기록의 유지, ▲ 고객의 상담 및 불만 처리 등의 직무를 수행해야 한다.

냐. 이용자 단체의 구성에 관한 원칙

1) 정보주체들은 이용자 단체를 구성하여 자기정보의 사용을 감독할 수 있다.

정보 수집자와 정보주체 사이의 정보 불균형을 완화하기 위해 일정 수 이상의 정보주체들이 모여 이용자 단체를 구성할 수 있다. 이 때, 이용자 단체는 국가 개인정보 감독기구에 신고함으로써 법적 지위를 획득한다. 구성에 관한 구체적 절차는 법령에 따라 규정된다.

2) 이용자 단체는 개인정보 수집 및 관리와 관련된 제반 사항에 대해 정보 수집자와 협의할 권리를 갖는다.

이용자 단체의 구체적 역할로는 ▲ 수집하는 사람의 의무 이행 여부를 확인, ▲ 수집의 구체적 내용에 대해 협의, ▲ 외부 감사의 발의, ▲ 규약에 따라 구성원들로부터 운영비 징수 등이 있다.

3) 이용자 단체는 민주적·공개적으로 운영되어야 하며, 구성원의 자기정보통제권을 제약해서는 안 된다.

이용자 단체가 그 활동 과정에서 정보 수집자와 협의한 내용이 개별 구성원의 의사에 반하여 강제될 수 없다.

다. 감독기구의 설치에 관한 원칙

1) 사회 전반의 개인정보 처리 활동을 감독하기 위해 권력으로부터 독립적인 개인정보 감독기구를 설치해야 한다.

개인정보 감독기구는 의사 결정 단위의 구성에 있어 행정부로부터 독립되어야 하며, 소관 업무를 수행하기 위해 사무국을 설치할 수 있어야 한다. 또한 사무국 구성과 예산 편성에 있어 독립성이 보장되어야 한다.

2) 개인정보 감독기구는 개인정보 보호와 관련된 정책에 대한 의견 개진, 사전 감독, 사후 분쟁조정, 교육 등의 기능을 수행한다.

개인정보 감독 기구는 법안, 조례 및 주요 정책에 대한 의견을 제시할 권리를 갖는다. 개인정보 영향 평가를 직접 수행하거나 위탁할 권리를 갖는다. 개인정보 보호실태를 정기적으로 조사할 권리를 가지며, 확인된 불법 행위에 대해서는 의무적으로 사법 당국에 고발해야 한다. 분쟁 발생시 조정 업무를 수행해야 하며, 정보 수집자가 그 결과를 받아들이지 않는 경우에는 법적 절차를 지원해야 한다. 마지막으로 개인정보 보호 교육을 활성화해야 한다.

3) 자치단체별로 개인정보감독기구를 구성할 수 있다. 자치단체별 감독기구는 국가 감독기구의 임무에 덧붙여 중앙 정부의 개인정보 수집 행위에 대한 의견을 제시할 수 있다.

자치단체별 개인정보 감독기구는 자치단체 보유 개인정보 데이터베이스에

대한 중앙 정부의 연동·통합 계획에 대해 의견을 제시할 수 있다.

4) 국가 개인정보 감독기구와 자치단체 개인정보 감독기구는 그 관할 범위를 적절하게 구분해야 한다.

국가 개인정보 감독기구는 중앙 정부 및 전국적 영향을 미치는 일정 규모 이상의 개인정보 데이터베이스를 보유한 기업들을 관할하며, 자치단체 개인정보 감독기구는 자치단체 및 국가 감독기구의 관할 밖에 있는 민간 영역을 관할한다.

랴. 교육에 대한 원칙

1) 자기정보 통제권에 대한 정보주체의 이해를 제고하기 위한 교육을 실시해야 한다.

초·중·고등학교에서는 학생들을 대상으로, 그리고 일정 수 이상의 직원을 고용하는 기업은 직원을 대상으로 자기정보 통제권에 대한 교육을 실시해야 한다.

2) 개인정보 교육은 권리 교육과 기술 교육을 포함해야 한다.

개인정보를 보호하기 위해서는 자기정보를 보호받을 수 있는 권리에 대한 교육과 더불어 자기 정보를 스스로 보호하기 위한 기술 교육이 함께 진행되어야 한다.

4. 정보통신서비스제공자의 개인정보 보호를 위한 가이드라인

여기에서는 개인정보 보호를 위한 일반 원칙에서 서술한 내용 이외에 정보통신서비스 제공자에 특별히 적용되어야 할 개인정보 보호에 관하여 서술한다.

가. 정보 수집자는 개인정보 수집에 대한 동의를 구하는 과정에서 개인정보의 제3자 제공에 대한 별도의 동의 절차를 마련해야 한다. 이 때, 각 정보의 제공 대상별로 구분하여 동의 여부를 선택할 수 있게 해야 한다.

일반적으로 개인정보 수집 시 제3자 제공에 대한 동의는 약관에 대한 동의로 대체된다. 그런데 대개 약관에서는 제3자 공유와 관련된 구체적 사항을 확인할 수 없다. 제3자 공유 문제의 중요성을 감안할 때, 약관에 대한 동의 절차와 개인정보 공유에 대한 동의 절차를 분리하여 제3자 제공 대상 기관 및 기업들을 구체적으로 제시해야 한다. 아울러 각각의 공유 대상에 대한 동의 여부를 따로따로 선택할 수 있게 해야 한다.

나. 이용자가 탈퇴를 하거나 정보를 수정하고자 할 때, 가입할 때 보다 어렵지 않게 할 수 있어야 한다.

이용자가 동의를 철회(회원 탈퇴)할 때, 가입시 요구하지 않았던 본인 확인 절차를 요구하는 경우가 있다. 예컨대 신분증 사본이나 주민등록 등본을 제출하라고 요구하는 경우가 이에 해당한다. 이는 자기정보의 동의 철회권을 부당하게 제약하는 행위로서 현행 법률로도 금지되어 있다.[115] 온라인상으로 가입이 가능하다면, 수정 및 탈퇴 역시 온라인상에서 해결할 수 있어야 한다. 이를 위한 메뉴를 웹 사이트에서 제공해야 한다.

다. 개인정보 수집 시 광고 정보 전송에 대해 거부할 수 있도록 해야 한다.

선택적 동의는 개인정보를 제3자에게 제공할 경우 뿐 아니라, 정보 수집자가 개인정보를 이용할 때도 적용되는 것이 바람직하다. 특히, 광고 메일은 원

115) 정보통신망이용촉진및정보보호등에관한법률 제30조는 다음과 같이 규정하고 있다.

제30조 (이용자의 권리 등) ⑥ 정보통신서비스제공자등은 이용자로부터 제1항 및 제2항의 규정에 의한 동의의 철회, 개인정보의 열람 또는 정정의 요구를 받은 경우에는 제22조 및 제23조의 규정에 의하여 개인정보를 수집하는 방법보다 쉽게 할 수 있도록 필요한 조치를 취하여야 한다.

하지 않는 이용자들에게 상당한 스트레스를 유발할 수 있기 때문에 개인정보 수집시 광고 정보 전송에 대해서는 거부할 수 있는 선택권을 제공해야 한다.

라. 개인정보 유출에 대비하여 보험에 가입하는 것이 바람직하다.

대량의 개인정보가 축적된 웹 사이트들의 경우, 일단 개인정보가 유출되면 그 피해의 규모가 매우 커지기 마련이다. 그럼에도 불구하고 해킹 등 외부의 공격에 의한 개인정보 유출은 근본적으로 차단하기 어렵다. 따라서 피해 발생시 보상을 위한 대책을 마련하는 것이 바람직하다. 앞에서 살펴보았듯이, 「전자상거래등에서의소비자보호에관한법률」에서는 소비자 피해에 대비하여 보험에 가입할 것을 권고하고 있다. 비단 쇼핑몰 뿐 아니라 모든 정보통신서비스 제공자가 보험에 가입하여 개인정보 유출의 피해에 대비하는 것이 바람직하다.

마. 고객센터 직원들이 이용자들의 개인정보 관련 고충에 대해 적절한 조치를 취할 수 있도록 교육이 이루어져야 한다.

대부분의 정보통신서비스제공자는 고객센터를 운영하고 있다. 개인정보와 관련된 이용자들의 민원은 이 곳을 거치는 경우가 많다. 그런데 고객센터 직원들이 개인정보 보호와 관련된 내용을 잘 이해하지 못한 탓에 이용자들의 고충 처리가 지연되는 경우가 많다. 개인정보 관리책임자는 고객센터 직원들에게 자기 회사의 개인정보 관리와 관련된 내용들을 구체적으로 교육시켜 고객센터 직원들이 이용자들의 개인정보 관련 불만을 즉각 처리할 수 있게 해야 한다. 이 때, 교육 내용은 개인정보의 제3자 공유 현황과 같은 구체적 내용을 포함해야 한다.

바. 개인정보보호책임자와 담당자의 직책과 성명과 신속히 연락 가능한 전화번호, 팩스번호, 이메일, 주소에 대한 정보가 웹상에 충분히 제공되어야 한다. 대부분의 정보통신서비스제공자는 개인정보보호정책에서 책임자와 담당자를

명시하고 있지만 연락을 취할 수 있는 방법은 제한적으로 고지된 경우가 많다.

5. 금융기관의 개인정보 보호를 위한 가이드라인

가. 이용자로부터 개인정보 제공 및 활용 동의를 받을 때, 동의서를 거래 개설 서류와 분리해야 한다. 또한 동의서는 정보 제공 대상 기관들과 제공 항목, 제공의 이유를 구체적으로 명시해야 하며, 각각의 제공 대상 기관들에 대해 따로따로 동의 여부를 선택할 수 있게 해야 한다.

나. 금융기관들은 거래 실적에 따라 이용자들에 대한 신용 한도를 설정하고 있다. 설정된 신용 한도가 변경될 경우 해당 정보주체에게 고지를 해야 하며, 고지의 내용에는 변경 사유가 포함되어야 한다.

다. 금융기관들은 수많은 기업과 제휴를 하고 있다. 제3자에 의해서 공유된 정보의 이용과 유지, 폐기에 관한 책임과 정책이 명기되어 있어야 한다.

라. 제3자에게 공유되어지는 정보의 목록을 명기해야 하며 각 항목(주민등록번호, 성명, 주소, 전화번호, 주소, 이메일, 기타)에 대한 선택권을 부여해야 한다.

마. 금융기관 탈퇴 시 금융거래내역 등 개인정보 보존 기한이 5년으로 법적으로 정해져 있으나, 3자 제공된 개인정보가 동일한 효력을 갖고 있지 못하는 현실이다. 금융기관 탈퇴 시 금융기관은 고객정보를 제공한 제3의 기관에 고객정보의 삭제를 요구하고 그 결과를 탈퇴 회원에게 고지하여야 한다.

바. 개인정보보호책임자의 전문 능력 향상을 위하여 유관 자격증 취득을 권고

하여야 하며 프라이버시에 대한 인권적 측면에 대한 교육이 부가되어야 한다. 이를 위하여 국가는 정책적으로 공공, 민간 영역의 프라이버시 책임자들을 대상으로 하는 인권교육을 진행하여야 한다.

사. 개인정보보호정책이 바뀌거나 수정되었을 경우 웹상 뿐 아니라 이메일을 통해서도 직접 공지가 될 수 있도록 하여야 한다.

아. 고객 정보에 접근할 때, 제한적이고 단계적 접근을 해야 하며 그 권한이 직무에 맞게 분리되어야한다. 고객과 전화 상담시 주민등록번호 또는 계좌정보를 입력하게 되어있는데, 그것으로서 알 수 있는 정보는 성명과 금융정보에 국한해야 하며 주소지와 연락처까지 단말기에 공개되기 위해서는 또 다른 확인 절차를 두어야 한다.

차. 계좌통합서비스를 원하지 않는 이용자들에 대해서는 물리적으로 정보 접근이 차단되어 있어야 한다. 즉, 계좌통합서비스 제공 업체와 금융기관과의 약정에 의한 일괄적인 계좌통합서비스 가능하도록 하는 것이 아니라 금융기관이 각 이용자들에게 관련 서비스 동의를 개별적으로 받아 서비스가 가능한 이용자와 가능하지 않은 이용자들을 별도 관리하여야 한다.

카. 각 금융기관은 자체 감사에서 도출된 개인정보보호 관련 사항을 공시하여 한다.

타. 개인정보보호에 관한 분야별(대출, 인터넷 etc), 책임자, 담당자의 직책과 성명과 신속히 연락 가능한 전화번호, 팩스번호, 이메일, 주소에 대한 정보가 웹상에 충분히 제공되어야 한다.

파. 개인정보관리책임자와 담당자들은 당사자간의 역할 분담을 명확히 규정하

여야 하며 홈페이지를 통하여 그 업무 내용을 공지하여야 한다.

6. 신용정보기관의 개인정보 보호를 위한 가이드라인

가. 신용정보의 수집 및 제3자 제공시 정보 주체의 동의를 얻어야 한다.

신용정보는 매우 중요한 개인정보이다. 신용정보의 수집 및 제3자 제공을 위해서는 당사자로부터 동의를 얻어야 한다.

나. 신용 거래의 안정을 위해 당사자의 동의 없이도 수집하도록 법률로 규정된 정보에 대해서도 수집 사실을 고지해야 한다.

신용불량자의 등재 등 신용거래의 안정을 위해 법률에 의해 동의 없이 신용정보를 수집·제공하는 경우가 있을 수 있다. 그러나, 이 경우에도 정보주체가 이 사실을 모르고 있다가 예상하지 못한 피해를 입지 않도록 고지를 의무화해야 한다.

나. 신용정보기관은 당사자에게 불이익을 초래할 수 있는 오래된 정보를 삭제해야 한다.

신용정보는 그 특성상 수집 목적의 달성 여부를 분명하게 규정하기 어렵다. 대신 지나치게 오래된 정보가 삭제되지 않고 당사자에게 계속 불이익을 주는 것을 막기 위해, 일정 기간이 지난 정보를 폐기하도록 규정하고 있다. 현행 「신용정보의이용및보호에관한법률 시행령」은 불이익을 초래할 수 있는 정보의 경우, 그 사유가 해소된 날부터 5년이 지나면 그 정보를 보유하지 못하도록 규정하고 있다.[116]

---

116) 제10조 (신용정보의 최신성 유지등) ①신용정보업자등은 신용정보의 정확성과 최신성이 유지될 수 있도록 금융감독위원회가 정하는 기준과 절차에 따라 신용정보의 등록·변경·관리등을 하여야 한다. <개정 1998.4.1>

②신용정보업자 및 신용정보집중기관은 법 제18조제2항의 규정에 의한 신용정보주체

Ⅷ. 결론

1. 연구의 결과

본 연구는 국내의 기업들의 개인정보 처리 과정 및 이를 규율하고 있는 법제를 자기정보통제권이라는 권리 개념을 기준으로 검토해보았다. 그 결과, 국내의 개인정보 보호 체계가 갖고 있는 몇 가지 약점들이 확인되었고, 이에 대한 대책이 절실히 요청된다.

우선, 국내의 개인정보 보호 체계가 자기정보에 대한 통제권이라는 국민의 기본권을 실현하는 데 초점을 맞추기보다는 유출로부터 정보를 보호하는 데 초점을 맞추고 있음이 확인되었다.

사실 「정보통신망이용촉진및정보보호등에관한법률」, 「신용정보의이용및활용에관한법률」 등 개인정보 보호와 관련된 국내의 주요 법률들은 몇 가지 문제점들을 안고 있음에도 불구하고 그 보호의 수준이 크게 낮은 편은 아니다. 그러나 이 법률들이 적용될 때 정보 주체들의 자기정보통제권을 실제로 보장해주지는 못하고 있음이 확인되었는데, 가령 제3자 제공에 대한 형식적 고지와 포괄적 동의 방식, 정보주체들에게 별다른 정보를 제공해주지 못하는 약관 및 개인정보보호정책 등이 그러하다. 개인정보 취득 경위에 대해서 설명을 요구했을 때, 제대로 설명을 듣는 경우도 많지 않았다. 더구나 자기정보통제권을 심각하게 위협하는 주민등록번호를 거의 모든 기업들이 수집하고 있었다. 따라서 개인정보 보호 제도가 엄격함에도 불구하고 실제로 수많은 개인정보유출 사고에 대해서 개별 정보주체들이 자신을 방어할 방법은 별로 없는 상황이다.

따라서 국내의 개인정보보호체계를 자기정보통제권을 중심으로 재편할 필요성이 지적된다. 자기정보 통제권을 위협하는 요소들의 제거와 구체적 권리들

에 대한 불이익을 초래할 수 있는 오래된 신용정보를 금융감독위원회가 정하는 바에 따라 그 불이익을 초래하게 된 사유가 해소된 날부터 5년 이내에 보유대상 또는 집중관리대상에서 삭제하여야 한다. <개정 1997.12.27, 1998.4.1>

의 법적 보장이 제도 개선의 핵심이 되어야 하며, 이러한 기반 위에서 정보 유출을 막기 위한 노력들이 전개되어야 한다.

둘째로, 기업들의 자율 규제가 작동하지 않는다는 점을 지적할 수 있다. 법률이나 지침에 의해 강제된 것을 형식적으로 따를 뿐, 개별 기업들이 개인정보 보호를 위해 자발적으로 노력하는 모습은 별로 보이지 않았다.

예컨대, 대부분의 기업이 개인정보보호정책을 제시하고는 있으나 그 내용은 천편일률적이었다. 정작 해당 기업이 고객의 개인정보를 어떻게 수집·활용·관리하고 있는지에 대한 구체적 정보는 제시되지 않고 있다. 지극히 형식적으로 개인정보보호정책을 게시하고 있을 따름이다. 또한 개인정보관리책임자에 대한 지정 역시 형식적이었다. 대부분의 금융기관들이 웹 사이트를 관장하는 온라인 사업부 담당자를 개인정보관리책임자로 두고 있었다. 따라서 해당 금융기관의 개인정보 관련 업무를 총괄적으로 관장할 수 없었다. 또 개인정보보호정책 상에 게시된 개인정보 관리책임자의 연락처로 연락을 시도하면 고객센터 직원이 받는 경우도 많았으며, 그 직원들이 실제 개인정보관리책임자가 누구인지도 모르는 사례도 있었다. 또한 자율규제 시스템의 하나로 정보통신산업협회에서 시행하고 있는 i-safe 마크와 e-Privacy 마크에도 대부분의 기업들이 별로 적극적으로 참여하지 않고 있었다.

셋째로, 기술 및 서비스의 변화에 따라 법제를 정비할 필요성이 제기되었다. 기존의 법제가 기술적 변화를 쫓아가지 못하면서 사각 지대가 발생하는 경우가 나타났다. 계좌 통합서비스 등의 예에서 드러나듯이, 금융기관과 일반 정보통신서비스 제공자 사이의 경계가 약화되면서 적용 법규와 감독의 권한이 불분명해졌다. 이러한 문제점을 해결하기 위해서는 개인정보보호를 위한 일반법을 제정하고 사회 전반의 개인정보 보호를 담당하는 독립적 감독기구를 설치하여, 사각 지대를 없애고 개인정보 보호라는 관점에서 종합적인 대책을 마련할 필요가 있다.

마지막으로, 개인정보 주체의 자기정보에 대한 주체의식 부족도 우려할 상황이었음이 확인되었다. 실제로 다양한 법적 장치와 제도적 규제로 인해 개인

정보보호에 대한 노력이 있었음에도 불구하고, 오히려 개인정보의 주체들인 시민들은 개인정보 보호가 얼마나 중요하며 역으로 개인정보의 유출이 얼마나 위험한지에 대한 인식이 거의 없는 상태였다. 인터넷 사이트에 가입할 때 회원약관을 제대로 읽지 않는 것은 물론이며, 쿠키에 대한 위험성에 대해서도 대부분 무지한 상태였으며, 개인정보의 공유에 대해서도 거의 관심을 두지 않고 있는 것으로 밝혀졌다. 심지어 자신의 주민등록번호가 도용되어 회원가입에 실패한 경우에도 대부분의 이용자들이 적극적으로 문제제기를 하지 않는 것으로 나타났다. 앞으로 개인정보를 보호하기 위한 제도적 장치의 구비와 법적 기반의 조성, 그리고 기술적 발전도 중요하지만 이에 못지않게 일반 시민을 대상으로 하는 개인정보보호의 필요성과 중요성을 강조하는 홍보와 교육이 적극적으로 도입될 필요가 있을 것이다.

2. 연구의 한계 및 향후 연구 방향

본 연구는 기존의 개인정보 보호에 대한 연구가 각각 법적 관점과 기술적 관점을 중심으로 전개된다는 문제의식에 기반하여, 권력 불균등과 정보 불균형이라는 사회과학적 관점을 반영하려고 노력했다. 그러나 이러한 측면에 대한 연구는 이론적 논의에 그쳤을 뿐, 실태 조사에서는 그다지 많이 반영되지 못했다는 점에서 한계가 나타났다. 향후 연구에서는 이런 측면을 확인할 수 있는 지표들을 개발하여 더욱 입체적인 실태 조사를 진행할 필요가 있다.

기술적 측면에 대한 조사 역시 일반 현황을 검토하는 이상으로 나아가지 못했다는 점에서 아쉬움이 남는다. 이는 연구진의 역량 부족도 있지만, 기본적으로 자료를 입수하기에 매우 어려운 문제가 있다. 특히 금융기관의 경우 해킹 등에 대한 우려로 보안과 관련된 기술적 조치를 외부에 공개하지 않았으며, 감독기관인 금융감독원만이 이 정보를 얻을 수 있었다. 그러나 금융감독원 역시 이 정보가 공개되면 상대적으로 취약한 금융 기관에 해킹이 집중되는 우려를 표하며, 비공개의 정책을 펴고 있다. 기업명을 익명 처리를 하더라도 최소

한의 기업별 보안 현황을 확인할 수 있는 정보를 제공하는 것이 관련 연구를 발전시키는 데 보탬이 될 것이다.

참고문헌

1. 국내 자료

강달천,「프라이버시 보호를 위한 감독기구의 사전적 권한」, 함께하는 시민행동 외 8개 시민사회단체 공동 주최,『연속 워크숍 : 프라이버시 보호법제 개선의 쟁점들 - 제2회 워크숍 : 프라이버시 감독 체계의 개선 방안을 모색한다』자료집.

고영삼,『전자감시사회와 프라이버시』, 서울 : 한울아카데미, 1998.

공정거래위원회 표준약관 00028호.

곽홍희,『금융정보망 정보보호 현황 및 표준화 동향』, 금융결제원, 1999.4.

광주인권운동센터 외,「정보사회 기본권 보장을 위한 33대 공약 - "국민의 권리는 정보사회에서도 지켜져야 한다"」기자회견 자료집, 2002.11.14.

교육인적자원부 자료,『교육행정정보시스템 설명자료 - 교무/학사 등 5개 업무영역 중심으로』, 2003.

권선경,「미국과 한국의 개인정보보호법제도 비교 연구」, 한국정보보호진흥원,『2002 개인정보보호백서』, 서울: 한국정보보호진흥원, 2003.

권영성,『헌법학원론』, 서울 : 법문사, 2000.

금융감독원,『2002년도 금융사고 현황과 대책』, 2003.2.

금융결제원,『금융결제원 연차보고서』, 2003. 6.

금융정보화추진분과위원회 사무국,『2002년도 금융정보화 추진현황』, 2003.

기술과 법 연구소,『전문가 집단의 개인정보보호 마인드에 관한 설문조사 결과보고서』, 서울 : 한국정보보호진흥원, 2001.

김연수,『개인정보보호』, 서울 : 사이버출판사, 2001.

김종철,「헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론」, 법무부,『인터넷 법률』제4호, 2001. 1.

김주환, 「디지털 시대의 프라이버시 권리」, 김주환 외, 『디지털시대와 인간존엄성』, 서울 : 나남출판, 2001.
노순규, 『정보관련 법제화와 정보보호』, 한국정보통신진흥협회, 『정보화사회』 123호, 1998.
릭 휘태커, 『개인의 죽음』, 노명현·이명균 역, 서울 : 생각의 나무, 2001.
박광진, 「디지털 시대의 개인정보 활용과 오용 대책」, 김주환 외, 『디지털시대와 인간존엄성』, 서울 : 나남출판, 2001.
박영우 외, 『2001년 주요 민간부문 정보보호 실태조사』, 서울 : 한국정보보호진흥원, 2001.
박인우, 「지식 정보 사회와 우리 교육의 방향」, 함께하는 시민행동 엮음, 『인터넷 한국의 10가지 쟁점』, 서울 : 역사넷, 2002.
방석호, 「전자상거래에서의 프라이버시와 소비자 보호」, 『한국정보법학회 국내학술세미나』, 1998.
백의선 외, 『국가간 개인정보 유통에 관한 정책 연구』, 한국정보보호센터 정책연구, 2000.
이지윤, 「인터넷 개인정보보호 정책 분석-유럽연합(EU)과 미국의 정책비교」, 이화여자대학교 석사논문, 2002.
서근우, 『신용정보관리제도의 현황과 과제』, 서울 : 한국금융연구원, 1996.
『시사저널』, 제 651호, 2002. 4.18.
신종철, 「프라이버시 보호를 위한 규제에 대한 연구」, 성균관대학교 석사논문, 2001.
신종철, 「프라이버시 보호의 사회적 과제」, 함께하는 시민행동 엮음, 함께하는 시민행동 엮음, 『인터넷 한국의 10가지 쟁점』, 서울 : 역사넷, 2002.
심슨 가핀켈, 『데이터베이스 제국』, 한국데이터베이스진흥센터 역, 서울 : 한빛미디어, 2001.
안쏘니 기든스, 『민족국가와 폭력』, 진덕규 역, 서울 : 삼지원, 1991.
윤현식, 「개인정보의 국가등록제도와 프라이버시권과의 관계에 관한 연구 -

감시와 통제의 기제로서 주민등록법을 중심으로』, 건국대학교 석사논문, 2002.
이덕구,「민간이 보유하는 개인정보의 보호』, 인천대학교 평화통일연구소,『통일문제와 국제관계』제8호, 1997.
이은우,『정보화에 따른 프라이버시권 침해법령 조사 연구』, 국가인권위원회 2002년도 인권상황 실태조사 연구용역사업보고서, 2002.
이인호,「한국의 개인정보보호법제의 문제점과 정비방안』, 한국정보보호진흥원 2003년 제2회 개인정보보호 심포지움,『각국 개인정보보호 법제도의 비교법적 접근』, 2003.
이인호,「토론 : 프라이버시보호 감독기구의 독립성 확보의 필요성』,『함께하는 시민행동 연속 워크숍, 제2회 프라이버시 감독체계의 개선방안 모색』자료집, 2003. 8.21.
이창범,「현행 프라이버시 보호 담당기구의 성과와 한계』, 함께하는 시민행동 외 8개 시민사회단체 공동 주최,『연속 워크숍 : 프라이버시 보호법제 개선의 쟁점들 - 제2회 워크숍 : 프라이버시 감독 체계의 개선 방안을 모색한다』자료집.
이형규,「독일 정보보호법의 현대화 추진방안』, 한국정보보호진흥원 2003년 제2회 개인정보보호 심포지움,『각국 개인정보보호 법제도의 비교법적 접근』, 2003.
정보사회세계정상회의(WSIS)를 위한 시민사회네트워크,『정보사회에 대한 한국 시민사회 선언문』(http://www.wsis.or.kr'principle.html), 2003. 5.
정보통신부,『개인정보보호지침 해설서』, 2002. 4.
정영화 외,『개인정보보호 감독기구 도입을 위한 법제도 개선방안연구』, 서울 : 한국정보보호센터, 2000.
정영화,「정보사회의 프라이버시 보호를 위한 정책과제 - 개인정보보호법률(Privacy Act)의 실현을 중심으로』, 프라이버시보호네트워크『1차 토론회 자료집』, 2001.

정재훈, 「민간부문에서의 정보프라이버시 보호」, 한국정보법학회 『제7회 세미나』, 1997.
정찬모, 『개인정보보호에 관한 국제적 입법동향 및 우리의 대응』, 서울 : 정보통신정책연구원, 1997.
제정 금융감독위원회 공고 제2000-117호, 2000.12.29.
조양호, 「OECD의 개인정보 보호 8가지 원칙」, 함께하는 시민행동 부설 인터넷 시민학교 굿시티즌 온라인 강좌 『프라이버시 - 빅브라더를 막아라』 (http://www.goodcitizen.or.kr/lecture/list.asp?b_number=195&b code=code)
진보네트워크센터 성명, 「인터넷 게시판 실명제가 노무현 정부식 '참여 민주주의'인가」, 2003. 9.18.
진보네트워크 보도자료, 「행정자치부, "현재로서는 인터넷 실명제 계획 없다"」, 2003.10. 9.
참여연대 의견서, 「정보통신망이용촉진및정보보호등에관한법률 개정안에 대한 의견서」, 2003. 7.31.
참여연대 보도자료, 「개인정보보호심의위원회, 지난 5년간 단 1차례 회의」, 2003. 8. 5.
한겨레신문
한국소비자단체협의회, 『개인정보 침해관련 실태조사 및 제도개선방안 연구』, 재정경제부 용역사업, 2002.
한국소비자단체협의회, 『개인정보 침해관련 실태조사 및 제도개선방안 연구』, 재정경제부 용역사업, 2002.
한국은행, 『2003. 6월말 현재 국내 인터넷뱅킹서비스 이용현황』, 2003. 6.
한국은행 금융결제부, 『전자금융의 발달과 은행산업의 미래』, 1996.
한국정보보호진흥원, 『2002 개인정보보호백서』, 서울: 한국정보보호진흥원, 2003.
한국표준협회, 『정보 기술 - 정보 보안 경영 실무 지침』, 2002. 8.26.
한상희, 「국가감시와 민주주의 - 공공영역의 창출을 위한 헌법해석」, 프라이버

시보호네트워크 제2차 공동토론회『개인정보의 국가 등록/관리제도의 문제점 자료집』, 2001.
함께하는 시민행동 보도자료,「국가보안법에 버금가는 '네트워크 보안법' 제정 시도 중단하라』, 2003. 6.11.
함께하는 시민행동 보도자료,「국내 대표적 인터넷 사이트 개인정보보호실태 조사 결과』, 2000. 4. 6.
함께하는 시민행동 보도자료,「시민행동, 역감시 카메라 설치 캠페인 시작』
함께하는 시민행동 보도자료,「50여개 인터넷 사이트 개인정보보호규정 수용도 조사결과』, 2001.11.16.
함께하는 시민행동 보도자료,「인터넷시대 개인정보보호를 위한 발상의 전환 - '주민등록번호를 바꾸자'』 2003.10. 6.
함께하는 시민행동 외 7개 단체,「독립적 개인정보 보호기구 설치를 촉구하는 정당·시민사회 기자회견 자료집』
홍석만·이준구,「역감시 권리로서의 프라이버시권에 대한 재구성』, 민주사회를 위한 변호사모임 편,『역감시의 권리로서 프라이버시권에 대한 재구성』, 서울: 민주사회를 위한 변호사모임, 1999.
홍인수,『개인정보보호 및 스팸메일에 대한 이용자 의식 조사』, 서울 : 한국소비자보호원, 2001.
홍창수 외,「PKI에 잠재된 개인정보의 모호성』, 한국정보보호진흥원,『개인정보연구』 2002년 제1호.
Cyberlaw Institute of Korea,『국내 인터넷 사이트의 개인정보 보호에 관한 실태조사』, 1999. 8.16.

2. 국외 자료

Basel Committee Publications, Risk Management Principles for Electronic

Banking, May 2001. (http://www.bis.org/publ/bcbs82.pdf)
David Lyon & Elia Zureik, “Surveillance, Privacy and the New Technology,” Computers, Surveillance, and Privacy, Minneapolis: Univ. of Minnesota Press,
Lawrence Lessig, Code and Other Laws of Cyberspace, New York : BASIC BOOKS, 1999.
Margaret Jane Radin, Contested Commodities, Cambridge, Mass. : Harvard Univ. Press, 1996.
Margaret Jane Radin, “Property Evolving in Cyberspace,” Journal of Law and Communications, 15, 1996.

3. 웹사이트

http://www.bccard.co.kr
http://www.iaisweb.org/content/02pas/02internet.pdf
http://www.iosco.org/pubdocs/pdf/IOSCOPD120.pdf
http://www.truste.org

부 록

1. 기업의 고객 자기정보 통제권 보장 실태

2. 개인정보 보호에 관한 이용자들의 의식과 태도 설문 문항

3. 개인정보 보호에 관한 이용자들의 의식과 태도 설문 결과

1. 기업의 고객 자기정보 통제권 보장 실태

1. 수집하는 정보의 구체적 항목과 목적을 밝히고 있는가?

① 개별 항목별로 구체적인 수집 목적을 설명하고 있다.

② 구체적인 수집목적을 설명하되, 개별항목과 직결시켜 설명하지는 않고있다.

③ 추상적인 형태의 수집 목적만을 제시하고 있다.

④ 제시하지 않고 있다.

	①	②	③	④
보험사	보험사 A, 보험사 B 보험사 C, 보험사 D	보험사 E 보험사 F	보험사 G 보험사 H 보험사 I	보험사 J
쇼핑몰	쇼핑몰 A, 쇼핑몰 B 쇼핑몰 C, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 F 쇼핑몰 G	쇼핑몰 H 쇼핑몰 I	쇼핑몰 J	
언론사		언론사 A, 언론사 B 언론사 C, 언론사 D 언론사 E, 언론사 F	언론사 G 언론사 H 언론사 I 언론사 J	
은행		은행 A, 은행 B 은행 C, 은행 D	은행 E, 은행 F 은행 G, 은행 H 은행 I, 은행 J 은행 K	
증권사		증권사 A, 증권사 B 증권사 C, 증권사 D	증권사 E, 증권사 F 증권사 G	
카드사	카드사 A, 카드사 B 카드사 C, 카드사 D 카드사 E, 카드사 F	카드사 G 카드사 H	카드사 I	
포털	포털 A 포털 B	포털 C, 포털 E 포털 D, 포털 F 포털 G	포털 H 포털 I 포털 J	

2. 개인정보의 보유 기간을 제시하고 있는가?

① 구체적 설명이 없다.

② 탈퇴하면 삭제한다는 식의 일반적 수준으로만 제시되고 있다.

③ 각각의 항목별로 구체적인 보존 연한을 명시하고 있다.

④ 각각의 항목별로 구체적인 보존 연한을 명시하고, 그 근거도 구체적으로 제시한다.

	①	②	③	④
보험사	보험사 J	보험사 G, 보험사 E 보험사 H, 보험사 F, 보험사 I	보험사 D	보험사 A 보험사 B 보험사 C
쇼핑몰		쇼핑몰 H, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 I	쇼핑몰 J	쇼핑몰 A, 쇼핑몰 B 쇼핑몰 C, 쇼핑몰 F 쇼핑몰 G
언론사		언론사 A, 언론사 G 언론사 B, 언론사 I 언론사 J, 언론사 C, 언론사 E	언론사 H 언론사 D 언론사 F	
은행	은행 J	은행 E, 은행 A 은행 B, 은행 F 은행 G, 은행 H 은행 I, 은행 C 은행 K, 은행 D		
증권사		증권사 A, 증권사 B 증권사 E, 증권사 F 증권사 C, 증권사 G 증권사 D		
카드사		카드사 D, 카드사 G 카드사 H, 카드사 I		카드사 A, 카드사 B 카드사 C, 카드사 E 카드사 F
포털	포털 J	포털 H, 포털 C, 포털 I 포털 E, 포털 D, 포털 B 포털 F, 포털 G		포털 A

3. 회원의 자기정보통제권을 어떻게 보장하고 있는가? (모두 표시)

① 열람 ② 정정 ③ 삭제

	①②③	언급없음
보험사	보험사 A, 보험사 B, 보험사 C, 보험사 G 보험사 E, 보험사 H, 보험사 F, 보험사 I 보험사 D	보험사 J
쇼핑몰	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 C, 쇼핑몰 H 쇼핑몰 D, 쇼핑몰 E, 쇼핑몰 I, 쇼핑몰 F 쇼핑몰 J, 쇼핑몰 G	
언론사	언론사 A, 언론사 G, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F	
은행	은행 E, 은행 A, 은행 B, 은행 F 은행 G, 은행 H, 은행 I, 은행 C 은행 J, 은행 K, 은행 D	
증권사	증권사 A, 증권사 B, 증권사 E, 증권사 F 증권사 C, 증권사 G, 증권사 D	
카드사	카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 F 카드사 G, 카드사 H, 카드사 I	
포털	포털 H, 포털 C, 포털 A, 포털 I, 포털 E 포털 D, 포털 J, 포털 B, 포털 F, 포털 G	

4. 쿠키 운용에 관한 정책이 존재하는가?

① 정책이 없다.

② 정책이 존재하지만, 추상적 설명에 그치고 있다.

③ 쿠키에 담기는 정보의 내용을 상세히 소개하고 있다.

④ 쿠키에 담기는 정보의 내용을 소개하고, 쿠키 거부 방안을 제시하고 있다.

⑤ 개인식별정보와 통합하여 사용되지 않음을 밝히고 있다.

⑥ 기타 (Session방식 - 쿠키 저장 없음)

	①	②	③	④	④⑤	⑥
보험사	보험사 J			보험사 G	보험사 A, 보험사 B 보험사 C, 보험사 E 보험사 F, 보험사 D	보험사 H 보험사 I
쇼핑몰	쇼핑몰 D	쇼핑몰 F		쇼핑몰 C 쇼핑몰 H 쇼핑몰 E	쇼핑몰 A, 쇼핑몰 B 쇼핑몰 I, 쇼핑몰 J, 쇼핑몰 G	
언론사		언론사 I 언론사 J		언론사 A 언론사 G 언론사 B 언론사 H	언론사 C, 언론사 D 언론사 E, 언론사 F	
은행	은행 F 은행 J			은행 E 은행 G 은행 H 은행 I 은행 K 은행 D	은행 A 은행 B 은행 C	
증권사	증권사 F			증권사 D	증권사 A, 증권사 B 증권사 E, 증권사 C 증권사 G	
카드사					카드사 A, 카드사 B 카드사 C, 카드사 D 카드사 E, 카드사 F 카드사 G, 카드사 H 카드사 I	
포털	포털 C	포털 I 포털 J	포털 E	포털 H 포털 D 포털 B 포털 G	포털 A 포털 F	

5. 기술적 대책을 상세히 제시하고 있는가?

① 정책이 없다.

② 추상적인 내용이 제시되고 있다.

③ 어떠한 방식을 사용하는지 정도의 비교적 구체적인 내용이 제시되어 있다.

④ 해당 시스템마다 회사, 기종, 모델명 등 매우 자세하게 설명하고 있다.

	①	②	③
보험사	보험사 J		보험사 A, 보험사 B, 보험사 C 보험사 G, 보험사 E, 보험사 H 보험사 F, 보험사 I, 보험사 D
쇼핑몰			쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 C 쇼핑몰 H, 쇼핑몰 D, 쇼핑몰 E, 쇼핑몰 I, 쇼핑몰 F, 쇼핑몰 J, 쇼핑몰 G
언론사	언론사 G	언론사 H 언론사 I 언론사 J	언론사 A, 언론사 B 언론사 C, 언론사 D, 언론사 E, 언론사 F
은행	은행 E, 은행 F, 은행 H 은행 I, 은행 J	은행 K	은행 A, 은행 B 은행 G, 은행 C, 은행 D
증권사	증권사 B	증권사 G	증권사 A, 증권사 E, 증권사 F 증권사 C, 증권사 D
카드사	카드사 H		카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 F 카드사 G, 카드사 I
포털		포털 I, 포털 J 포털 B, 포털 G	포털 H, 포털 C, 포털 A 포털 E, 포털 D, 포털 F

6. 아동의 개인정보를 보호하기 위한 부모의 동의권을 명시하고 있는가?

① 명시한다.　② 명시하지 않고 있다.　③ 수집하지 않는다　④ 기타

	①	②	③	④
보험사	보험사 A, 보험사 B 보험사 G, 보험사 H 보험사 F, 보험사 I 보험사 D	보험사 J	보험사 C	보험사 E
쇼핑몰	쇼핑몰 C, 쇼핑몰 H 쇼핑몰 E	쇼핑몰 I	쇼핑몰 A, 쇼핑몰 B 쇼핑몰 D, 쇼핑몰 F, 쇼핑몰 J 쇼핑몰 G	
언론사	언론사 A, 언론사 B 언론사 H, 언론사 I 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F	언론사 G		
은행	은행 E 은행 C	은행 F, 은행 G 은행 H, 은행 I 은행 J, 은행 K		은행 A 은행 B 은행 D
증권사	증권사 A, 증권사 B 증권사 G, 증권사 D	증권사 E, 증권사 F 증권사 C		
카드사	카드사 B, 카드사 E 카드사 G, 카드사 H	카드사 I	카드사 A, 카드사 C 카드사 D, 카드사 F	
포털	포털 H, 포털 C, 포털 A 포털 I, 포털 E, 포털 D 포털 J, 포털 B 포털 F, 포털 G			

7. 비회원 거래자에 대한 개인정보 보호 정책이 적절한가?

① 개별 항목별로 구체적인 수집 목적을 설명하고 있다.

② 구체적인 수집목적을 설명하되, 개별항목과 직결시켜 설명하지는 않고있다.

③ 추상적인 형태의 수집 목적만을 제시하고 있다.

④ 제시하지 않고 있다.　　⑤ 해당사항 없음

	②	④	⑤
보험사			보험사 A, 보험사 B, 보험사 C, 보험사 G 보험사 E, 보험사 H, 보험사 J 보험사 F, 보험사 I, 보험사 D
쇼핑몰	쇼핑몰 A 쇼핑몰 C 쇼핑몰 H 쇼핑몰 G	쇼핑몰 B, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 I 쇼핑몰 F	쇼핑몰 J
언론사			언론사 A, 언론사 G, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F
은행			은행 E, 은행 A, 은행 B, 은행 F 은행 G, 은행 H, 은행 I, 은행 C 은행 J, 은행 K, 은행 D
증권사			증권사 A, 증권사 B, 증권사 E, 증권사 F 증권사 C, 증권사 G, 증권사 D
카드사			카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 F 카드사 G, 카드사 H, 카드사 I
포털	포털 D	포털 H, 포털 C 포털 I	포털 A, 포털 E, 포털 J 포털 B, 포털 F, 포털 G

7-1. 비회원 거래자의 개인정보 보존 연한을 제시하고 있는가?

① 구체적 설명이 없다.

② 거래가 끝나면 삭제한다는 식의 일반적 수준으로만 제시되고 있다.

③ 각각의 항목별로 구체적인 보존 연한을 명시하고 있다.

④ 각각의 항목별로 구체적인 보존 연한을 명시하고, 그 근거도 구체적으로 제시한다.

⑤ 비회원 거래의 해당사항이 없다.

	①	⑤
보험사		보험사 A, 보험사 B, 보험사 C, 보험사 G 보험사 E, 보험사 H, 보험사 J, 보험사 F, 보험사 I, 보험사 D
쇼핑몰	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 C 쇼핑몰 H, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 I 쇼핑몰 F, 쇼핑몰 G	쇼핑몰 J
언론사		언론사 A, 언론사 G, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F
은행		은행 E, 은행 A, 은행 B, 은행 F 은행 G, 은행 H, 은행 I, 은행 C 은행 J, 은행 K, 은행 D
증권사		증권사 A, 증권사 B, 증권사 E, 증권사 F 증권사 C, 증권사 G, 증권사 D
카드사		카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 F 카드사 G, 카드사 H, 카드사 I
포털	포털 H, 포털 C, 포털 I, 포털 D	포털 A, 포털 E, 포털 J 포털 B, 포털 F, 포털 G

8. 개인정보 관리 책임자를 지정하고 있는가?

① 지정한다　　② 지정하지 않는다

	①	②
보험사	보험사 A, 보험사 B, 보험사 C 보험사 G, 보험사 E, 보험사 H 보험사 F, 보험사 I, 보험사 D	보험사 J
쇼핑몰	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 C, 쇼핑몰 H 쇼핑몰 D, 쇼핑몰 E, 쇼핑몰 I, 쇼핑몰 F 쇼핑몰 J, 쇼핑몰 G	
언론사	언론사 A, 언론사 G, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F	
은행	은행 E, 은행 A, 은행 B, 은행 F 은행 G, 은행 H, 은행 I, 은행 C 은행 K, 은행 D	은행 J
증권사	증권사 A, 증권사 B, 증권사 E 증권사 C, 증권사 G, 증권사 D	증권사 F
카드사	카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 F 카드사 G, 카드사 H, 카드사 I	
포털	포털 H, 포털 C, 포털 A, 포털 I, 포털 E 포털 D, 포털 J, 포털 B, 포털 F, 포털 G	

8-1. 개인정보관리책임자의 정보를 어느 정도 공개하고 있는가?

① 성명 ② 직위 ③ 주소 ④ 전화 ⑤ e-mail

	①④	①②④	①④⑤	①~④	①②④⑤	①~⑤	
보험사			보험사 G	보험사 F	보험사 A, 보험사 B 보험사 C, 보험사 E 보험사 H, 보험사 I 보험사 D		
쇼핑몰					쇼핑몰 A, 쇼핑몰 C 쇼핑몰 H, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 F 쇼핑몰 J, 쇼핑몰 G		①②⑤ 쇼핑몰 B 쇼핑몰 I
언론사	언론사 E				언론사 A, 언론사 G 언론사 B, 언론사 H 언론사 I, 언론사 J 언론사 C, 언론사 D, 언론사 F		
은행		은행 K	은행 H 은행 C	은행 I	은행 E, 은행 A 은행 B, 은행 D		①② 은행 F ③⑤ 은행 G
증권사		증권사 B			증권사 A, 증권사 E 증권사 C, 증권사 G 증권사 D		
카드사		카드사 D			카드사 A, 카드사 B 카드사 C, 카드사 D 카드사 E, 카드사 F 카드사 G, 카드사 H 카드사 I	카드사 F	
포털		포털 G			포털 H, 포털 C, 포털 A 포털 I, 포털 E, 포털 D 포털 J, 포털 B, 포털 F		

8-2. 개인정보관리책임자의 직위는 무엇인가?

	부사장	상무/이사	부장	차장	과장	대리	팀장	기타
보험사		보험사 D	보험사 A 보험사 B		보험사 E 보험사 F		보험사 C 보험사 I	보험사 A (선임)
쇼핑몰		쇼핑몰 G	쇼핑몰 E 쇼핑몰 J	쇼핑몰 I			쇼핑몰 A 쇼핑몰 B 쇼핑몰 C 쇼핑몰 D 쇼핑몰 F	쇼핑몰 H (기획총괄)
언론사			언론사 G 언론사 I 언론사 C 언론사 D				언론사 A 언론사 B 언론사 J 언론사 F	언론사 H (본부장)
은행			은행 A 은행 D	은행 B 은행 F	은행 E	은행 I	은행 K	
증권사			증권사 G			증권사 E	증권사 A 증권사 B 증권사 C	증권사 D (보안담당)
카드사		카드사 F	카드사 C 카드사 G		카드사 I		카드사 A 카드사 B 카드사 D 카드사 E 카드사 H	
포털	포털 J	포털 A	포털 I 포털 B				포털 C 포털 E 포털 F 포털 G	포털 H (본부장) 포털 D (실장)

9. 개인정보 유출에 따른 손해 배상에 대비한 보험에 가입해있는가?

① 가입되어 있다　　② 가입되어있지 않다　　③ 미확인

	①	②	③
보험사	보험사 C, 보험사 G	보험사 A, 보험사 H 보험사 D	보험사 B, 보험사 E 보험사 J, 보험사 F 보험사 I
쇼핑몰	쇼핑몰 A, 쇼핑몰 H 쇼핑몰 G	쇼핑몰 B, 쇼핑몰 D 쇼핑몰 I, 쇼핑몰 F, 쇼핑몰 J	쇼핑몰 C 쇼핑몰 E
언론사		언론사 A, 언론사 G 언론사 B, 언론사 H 언론사 I, 언론사 J 언론사 C, 언론사 E, 언론사 F	언론사 D
은행	은행 E, 은행 I	은행 A, 은행 B 은행 H, 은행 C 은행 K	은행 F, 은행 G 은행 J, 은행 D
증권사	증권사 B	증권사 A, 증권사 E 증권사 F, 증권사 C 증권사 G, 증권사 D	
카드사		카드사 A, 카드사 B 카드사 C, 카드사 D 카드사 G, 카드사 H 카드사 I	카드사 E, 카드사 F
포털		포털 C, 포털 H, 포털 D 포털 J, 포털 G	포털 A, 포털 I, 포털 E 포털 B, 포털 F

10. 주민등록번호를 어떻게 수집·관리하는가?

① 회원 가입 때 수집한다

② 주민등록번호가 필요한 서비스를 이용할 때 수집한다

③ 수집하지 않는다

	①	②	③
보험사	보험사 A, 보험사 B, 보험사 C, 보험사 G 보험사 E, 보험사 H, 보험사 J, 보험사 F, 보험사 I, 보험사 D		
쇼핑몰	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 C, 쇼핑몰 H 쇼핑몰 D, 쇼핑몰 E, 쇼핑몰 I, 쇼핑몰 F 쇼핑몰 J, 쇼핑몰 G		
언론사	언론사 A, 언론사 G, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F		
은행	은행 E, 은행 A, 은행 B, 은행 F 은행 H, 은행 I 은행 K, 은행 D		은행 G 은행 C 은행 J
증권사	증권사 A, 증권사 B, 증권사 E, 증권사 F 증권사 C, 증권사 G		증권사 D
카드사	카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 F 카드사 G, 카드사 H, 카드사 I		
포털	포털 C, 포털 A, 포털 I, 포털 E, 포털 D 포털 J, 포털 B, 포털 F, 포털 G	포털 H	

10-1. 주민등록번호와 실명을 통한 인터넷 실명제를 실시하고 있는가?

① 실시한다　　② 실시하지 않는다

	①	②
보험사	보험사 C, 보험사 G, 보험사 E 보험사 H, 보험사 J, 보험사 F 보험사 I, 보험사 D	보험사 A 보험사 B
쇼핑몰	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 H 쇼핑몰 D, 쇼핑몰 E, 쇼핑몰 I 쇼핑몰 F, 쇼핑몰 G	쇼핑몰 C 쇼핑몰 J
언론사	언론사 A, 언론사 G, 언론사 B 언론사 H, 언론사 I, 언론사 J 언론사 D, 언론사 E, 언론사 F	언론사 C
은행	은행 A, 은행 B 은행 F, 은행 D	은행 E, 은행 G, 은행 H, 은행 I 은행 C, 은행 J, 은행 K
증권사		증권사 A, 증권사 B, 증권사 E 증권사 F, 증권사 C, 증권사 G 증권사 D
카드사	카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 G 카드사 I	카드사 F 카드사 H
포털	포털 H, 포털 C, 포털 A, 포털 I 포털 E, 포털 D, 포털 J, 포털 B 포털 F, 포털 G	

10-2. 언제 실명을 확인하는가? (모두 선택)

① 회원 가입 때 ② 게시판에 글쓰기를 할 때

③ 물품 구매를 할 때 ④ 성인용 컨텐츠를 이용할 때

⑤ 기타

	①	②⑤
보험사	보험사 C, 보험사 G, 보험사 E, 보험사 H 보험사 J, 보험사 F, 보험사 I, 보험사 D	
쇼핑몰	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 H, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 I, 쇼핑몰 F, 쇼핑몰 G	
언론사	언론사 A, 언론사 G, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 D, 언론사 E, 언론사 F	
은행	은행 A, 은행 B, 은행 F, 은행 D	
증권사	*	
카드사	카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 G, 카드사 I	
포털	포털 C, 포털 A, 포털 I, 포털 E, 포털 D 포털 J, 포털 B, 포털 F, 포털 G	포털 H (커뮤니티 개설, 금융서비스)

10-3. 실명제를 실시하는 경우 어떤 실명확인 방식을 사용하고 있는가?

① 외부 기관(신용평가 회사 등)의 DB와 연계

② 주민등록번호 알고리즘 확인

	①	②
보험사	보험사 C, 보험사 G, 보험사 E, 보험사 H 보험사 J, 보험사 F, 보험사 D	보험사 I
쇼핑몰	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 H, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 I, 쇼핑몰 F, 쇼핑몰 G	
언론사	언론사 A, 언론사 G, 언론사 B 언론사 H, 언론사 I, 언론사 J 언론사 D, 언론사 E, 언론사 F	
은행	은행 A, 은행 B, 은행 F, 은행 D	
증권사	*	
카드사	카드사 A, 카드사 B, 카드사 C, 카드사 D 카드사 E, 카드사 G, 카드사 I	
포털	포털 H, 포털 C, 포털 A, 포털 I 포털 E, 포털 D, 포털 J 포털 B, 포털 F, 포털 G	

11. 연락처 정보 중 필수적으로 수집하고 있는 정보는? (모두 선택)

① 주소 ② e-mail ③ 전화 ④ 휴대폰

	②	①③	①, ③or④	①②③	①③④	①②, ③or④	①②③④	
보험사				보험사 B 보험사 C 보험사 J 보험사 F 보험사 I			보험사 G 보험사 H 보험사 D	②③ 보험사 A ②④ 보험사 E
쇼핑몰				쇼핑몰 A 쇼핑몰 B 쇼핑몰 C 쇼핑몰 H 쇼핑몰 E 쇼핑몰 I 쇼핑몰 F		쇼핑몰 D	쇼핑몰 J 쇼핑몰 G	
언론사				언론사 A 언론사 G 언론사 B 언론사 C 언론사 D 언론사 E 언론사 F		언론사 I 언론사 J	언론사 H	
은행		은행 E		은행 A 은행 I 은행 D			은행 K	①②은행 C **없음** 은행 F 은행 G 은행 H 은행 C 은행 J
증권사	증권사 D	증권사 A		증권사 F 증권사 C 증권사 G	증권사 E	증권사 B		
카드사		카드사 G		카드사 D 카드사 E 카드사 H 카드사 I		카드사 A 카드사 C	카드사 B 카드사 F	
포털	포털 A	포털 J	포털 H	포털 I 포털 E 포털 D		포털 F	포털 G	①②④ 포털 C **없음** 포털 B

11-1. 각각의 연락처에 수집해야 할 타당한 목적이 제시되고 있는가?

① 제시하고 있지 않다

② 개인정보보호정책(약관)에서 포괄적으로 제시하고 있다.

③ 실제 수집단계에서 구체적 목적을 제시하고 있다.

④ 수집하지 않는다.

	①	②	③	④
보험사	보험사 G, 보험사 H 보험사 J, 보험사 F, 보험사 I	보험사 B 보험사 C 보험사 D	보험사 A 보험사 E	
쇼핑몰	쇼핑몰 H, 쇼핑몰 I, 쇼핑몰 J	쇼핑몰 A, 쇼핑몰 B 쇼핑몰 C, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 F 쇼핑몰 G		
언론사	언론사 A, 언론사 G, 언론사 B 언론사 H, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F		언론사 I	
은행	은행 E, 은행 A, 은행 B 은행 I, 은행 K, 은행 D			은행 F 은행 G 은행 H 은행 C 은행 J
증권사	증권사 A, 증권사 B, 증권사 E 증권사 F, 증권사 C 증권사 G 증권사 D			
카드사	카드사 D 카드사 G 카드사 I	카드사 A, 카드사 B 카드사 C, 카드사 E 카드사 F, 카드사 H		
포털	포털 H, 포털 I, 포털 E 포털 D, 포털 G	포털 A 포털 B	포털 C 포털 J 포털 F	

12. 광고성 메일이나 우편물의 수신에 대한 동의 절차를 밟고 있는가?

① (별도의 동의 절차를 마련하고 있으나)모든 우편물에 대해 하나의 동의를 받고 있다

② 우편물의 종류에 따라 개별적 동의를 받고 있다

③ 약관에 대한 동의로 대체된다. ④ 안내가 없다. ⑤ 해당사항 없다.

	①	②	③	④	⑤
보험사	보험사 B 보험사 G, 보험사 I	보험사 E, 보험사 D	보험사 C 보험사 H 보험사 J 보험사 F	보험사 A	
쇼핑몰	쇼핑몰 A, 쇼핑몰 B 쇼핑몰 H, 쇼핑몰 D 쇼핑몰 E, 쇼핑몰 I 쇼핑몰 F, 쇼핑몰 J	쇼핑몰 C 쇼핑몰 G			
언론사	언론사 J, 언론사 C 언론사 D, 언론사 E	언론사 A, 언론사 G 언론사 B, 언론사 H 언론사 I, 언론사 F			
은행	은행 E, 은행 A 은행 B, 은행 I	은행 K	은행 D		은행 F 은행 G 은행 H 은행 C 은행 J
증권사	증권사 C 증권사 D	증권사 G		증권사 A 증권사 B 증권사 E 증권사 F	
카드사	카드사 A, 카드사 C 카드사 E, 카드사 F 카드사 G	카드사 B 카드사 D		은행 F 은행 A	
포털	포털 A, 포털 E 포털 D	포털 H, 포털 C 포털 B, 포털 G	포털 I 포털 J 포털 F		

13. 현재 개인정보를 공유하고 있는 대상을 구체적으로 명시하고 있는가?

① 공유 대상 기업의 명칭과 제공 목적, 제공 항목을 구체적으로 명시

② 공유 대상 기업의 명칭과 제공 목적만을 구체적으로 명시

③ 공유 대상 기업의 명칭만을 구체적으로 명시

④ 공유 대상과 목적을 모두 추상적으로 표현

⑤ 공유 여부를 명확히 알 수 없다.　　⑥ 기타

	①	③	④	⑤	⑥
보험사			보험사 B, 보험사 C 보험사 E, 보험사 H 보험사 J, 보험사 F 보험사 I, 보험사 D	보험사 A 보험사 G	
쇼핑몰		쇼핑몰 C 쇼핑몰 D 쇼핑몰 F		쇼핑몰 A, 쇼핑몰 B 쇼핑몰 E, 쇼핑몰 I 쇼핑몰 J, 쇼핑몰 G	쇼핑몰 H (명칭/항목)
언론사	언론사 H	언론사 G 언론사 F	언론사 A, 언론사 B 언론사 I, 언론사 J 언론사 D, 언론사 E	언론사 C	
은행		은행 C 은행 K		은행 E, 은행 A, 은행 B, 은행 F 은행 G, 은행 H, 은행 I, 은행 J, 은행 D	
증권사			증권사 A, 증권사 B	증권사 E, 증권사 F 증권사 C,증권사 G 증권사 D	
카드사	카드사 E	카드사 I	카드사 B, 카드사 C	카드사 A, 카드사 D 카드사 F, 카드사 G 카드사 H	
포털	포털 G		포털 C, 포털 I 포털 E, 포털 D 포털 F	포털 H, 포털 A 포털 J, 포털 B	

13-1. 현재 공유하는 개인정보 대한 동의 절차를 분리하고 있는가?

① 공유 대상 기업 각각에 대해 따로 동의 절차를 마련한다

② 공유 대상 기업에 대한 동의 절차가 따로 마련되어 있으나, 전체 공유 대상 기업에 대해 한꺼번에 동의하도록 되어 있다

③ 약관에 대한 동의로 대체된다

④ 명확한 안내가 없다. ⑤ 해당사항 없음

	②	③	④	⑤
보험사		보험사 A, 보험사 B 보험사 C, 보험사 G 보험사 E, 보험사 H 보험사 J, 보험사 F 보험사 I, 보험사 D		
쇼핑몰	쇼핑몰 C 쇼핑몰 E 쇼핑몰 F	쇼핑몰 A, 쇼핑몰 H 쇼핑몰 D	쇼핑몰 B 쇼핑몰 I 쇼핑몰 J 쇼핑몰 G	
언론사		언론사 A, 언론사 G 언론사 B, 언론사 H 언론사 I, 언론사 J 언론사 D, 언론사 E, 언론사 F	언론사 C	
은행		은행 F	은행 E, 은행 A 은행 B, 은행 G 은행 H, 은행 I 은행 C, 은행 J 은행 K, 은행 D	
증권사		증권사 A, 증권사 B 증권사 G	증권사 E, 증권사 F 증권사 C, 증권사 D	
카드사		카드사 B, 카드사 C 카드사 D, 카드사 E	카드사 A, 카드사 F 카드사 G, 카드사 H 카드사 I	
포털		포털 C, 포털 I 포털 E, 포털 D 포털 F, 포털 G	포털 H, 포털 A 포털 J, 포털 B	

14. 약관 및 개인정보 정책의 변경시, 어떤 안내방식을 택하고 있는가?

① 홈페이지 안내 ② e-mail 고지 ③ 기타(우편/영업장게시) ④ 안내없음

	①	④	①~③택1	①②	①③	①②③
보험사	보험사 A, 보험사 B 보험사 C, 보험사 G 보험사 E, 보험사 H 보험사 F, 보험사 D	보험사 J				보험사 I
쇼핑몰	쇼핑몰 A, 쇼핑몰 B 쇼핑몰 C, 쇼핑몰 H 쇼핑몰 D, 쇼핑몰 I 쇼핑몰 F, 쇼핑몰 J 쇼핑몰 G		쇼핑몰 E			
언론사	언론사 G 언론사 B			언론사 A,언론사 H 언론사 I, 언론사 J 언론사 C, 언론사 D 언론사 E, 언론사 F		
은행	은행 E 은행 K 은행 D				은행 F 은행 J	은행 A 은행 B 은행 G 은행 H 은행 I 은행 C
증권사	증권사 B			증권사 G	증권사 A 증권사 E 증권사 C 증권사 D	증권사 F
카드사	카드사 A, 카드사 C 카드사 E, 카드사 F 카드사 G, 카드사 H 카드사 I			카드사 D	카드사 B	
포털	포털 H, 포털 C 포털 A, 포털 I 포털 E, 포털 D 포털 J, 포털 B 포털 F, 포털 G					

14-1. 약관 및 개인정보 정책 변경시, 어떤 방식으로 동의를 받는가?

① 안내 절차 없음

② 일정기간 안내한 후, 탈퇴하지 않은 사람을 모두 동의한 것으로 간주한다

③ 일정기간 안내한 후, 동의한다고 명시적으로 밝힌 사람들만 동의한 것으로 간주하고, 그 외의 사람들의 정보는 폐기한다.

④ 일정기간 안내한 후, 동의한다고 명시적으로 밝힌 사람들만 동의한 것으로 간주한다. 그러나, 그 외의 사람들의 정보는 폐기하지도 사용하지도 않고 보관한다.

	①	②
보험사	보험사 G 보험사 J	보험사 A, 보험사 B, 보험사 C 보험사 E, 보험사 H, 보험사 F 보험사 I, 보험사 D
쇼핑몰	쇼핑몰 J	쇼핑몰 A, 쇼핑몰 B, 쇼핑몰 C 쇼핑몰 H, 쇼핑몰 D, 쇼핑몰 E 쇼핑몰 I, 쇼핑몰 F, 쇼핑몰 G
언론사	언론사 G	언론사 A, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F
은행	은행 J	은행 E, 은행 A, 은행 B, 은행 F 은행 G, 은행 H, 은행 I, 은행 C 은행 K, 은행 D
증권사	증권사 A 증권사 G 증권사 D	증권사 B, 증권사 E 증권사 F, 증권사 C
카드사		카드사 A, 카드사 B, 카드사 C 카드사 D, 카드사 E, 카드사 F 카드사 G, 카드사 H, 카드사 I
포털	포털 I 포털 B	포털 H, 포털 C, 포털 A, 포털 E 포털 D, 포털 J, 포털 F, 포털 G

15. 영업의 양수 / 양도가 일어날 때, 어떤 안내 방식을 택하는가?

① 홈페이지 안내 ② e-mail 고지 ③ 기타(우편/영업장게시) ④ 안내없음

	④	①②	①②③
보험사	보험사 G, 보험사 E, 보험사 H, 보험사 J 보험사 F, 보험사 I, 보험사 D	보험사 B 보험사 C	보험사 A
쇼핑몰	쇼핑몰 H, 쇼핑몰 D, 쇼핑몰 E 쇼핑몰 I, 쇼핑몰 F, 쇼핑몰 J	쇼핑몰 A 쇼핑몰 B 쇼핑몰 C 쇼핑몰 G	
언론사	언론사 A, 언론사 G, 언론사 B 언론사 H, 언론사 I, 언론사 J 언론사 C, 언론사 D, 언론사 E, 언론사 F		
은행	은행 E, 은행 A, 은행 B 은행 F, 은행 G, 은행 H 은행 I 은행 C, 은행 J 은행 K, 은행 D		
증권사	증권사 A, 증권사 B, 증권사 E 증권사 F, 증권사 C, 증권사 G 증권사 D		
카드사	카드사 B, 카드사 D, 카드사 E 카드사 G, 카드사 H, 카드사 I	카드사 A 카드사 C 카드사 F	
포털	포털 H, 포털 C, 포털 A, 포털 I, 포털 E 포털 D, 포털 J, 포털 B, 포털 F, 포털 G		

15-1. 영업의 양수 / 양도시, 어떤 방식으로 동의를 받는가?

① 안내 절차조차 없다

② 일정기간 안내한 후, 탈퇴하지 않은 사람을 모두 동의한 것으로 간주한다

③ 일정기간 안내한 후, 동의한다고 명시적으로 밝힌 사람들만 동의한 것으로 간주하고, 그 외의 사람들의 정보는 폐기한다.

④ 일정기간 안내한 후, 동의한다고 명시적으로 밝힌 사람들만 동의한 것으로 간주한다. 그러나, 그 외의 사람들의 정보는 폐기하지도 사용하지도 않고 보관한다.

⑤ 추상적으로 동의를 받겠다고만 나와있다.

	①	②	③	⑤
보험사	보험사 G, 보험사 E, 보험사 H 보험사 J, 보험사 F, 보험사 I	보험사 A 보험사 B 보험사 C 보험사 D		
쇼핑몰	쇼핑몰 H, 쇼핑몰 D, 쇼핑몰 E 쇼핑몰 I, 쇼핑몰 F, 쇼핑몰 J	쇼핑몰 A 쇼핑몰 G	쇼핑몰 B 쇼핑몰 C	
언론사	언론사 A, 언론사 G, 언론사 B, 언론사 H 언론사 I, 언론사 J, 언론사 C 언론사 D, 언론사 E, 언론사 F			
은행	은행 E, 은행 A, 은행 B, 은행 F 은행 G, 은행 H, 은행 I, 은행 C 은행 J, 은행 K, 은행 D			
증권사	증권사 A, 증권사 B, 증권사 E, 증권사 F 증권사 C, 증권사 G, 증권사 D			
카드사	카드사 B, 카드사 D, 카드사 E 카드사 G, 카드사 H, 카드사 I	카드사 A	카드사 C	카드사 F
포털	포털 H, 포털 C, 포털 A, 포털 I, 포털 E 포털 D, 포털 J, 포털 B, 포털 F, 포털 G			

2. 개인정보 보호에 관한 이용자들의 의식과 태도 설문 문항

< 이용약관 >

1. 인터넷 서비스를 이용하기 위해 회원 가입을 할 때, 이용약관을 읽어보십니까?
① 꼼꼼히 읽어보는 편이다 ② 부분적으로 읽어보는 편이다
③ 거의 읽지 않는 편이다

1-1. (1번 문항에 대해 ②라고 대답한 사람에게) 주로 읽는 내용은 어떤 부분입니까? (복수 응답 가능)
① 요금 관련 사항 ② 개인정보 관련 사항 ③ 이용자 권리 관련 사항
④ 물품 구매 관련 사항 ⑤ 기타

1-2. (1번 문항에 대해 ③이라고 대답한 사람에게) 읽어보지 않는 이유는 무엇입니까?
① 어느 사이트나 내용이 거의 같다 ② 구체적인 정보를 주지 않고 있다
③ 양이 지나치게 많다 ④ 안 읽어도 별다른 문제가 발생하지 않는다
⑤ 기타

< 개인정보보호정책 >

2. 인터넷 서비스를 이용하기 위해 회원 가입을 할 때, 개인정보 보호정책을 읽어보십니까?
① 꼼꼼히 읽어보는 편이다 ② 부분적으로 읽어보는 편이다
③ 거의 읽지 않는 편이다

2-1. (2번 문항에 대해 ②라고 대답한 사람에게) 주로 읽는 내용은 어떤 부분입니까? (복수 응답 가능)
① 제3자 공유 관련 사항 ② 가입·탈퇴에 관한 사항
③ 이용자 권리 관련 사항 ④ 쿠키 관련 사항 ⑤ 기타

2-2. (2번 문항에 대해 ③이라고 대답한 사람에게) 읽어보지 않는 이유는 무엇입니까?
① 어느 사이트나 내용이 거의 같다 ② 구체적인 정보를 주지 않고 있다
③ 양이 지나치게 많다 ④ 안 읽어도 별다른 문제가 발생하지 않는다

< 텔레마케팅 >

3. 텔레마케팅 전화가 걸려올 경우, 개인정보 취득 경위에 대해 질문을 한 경험이 있습니까?
① 있다 ② 없다

3-1. (3번 문항에 대해 ①이라고 대답한 사람에게) 질문에 대한 답변을 듣는 경우는 몇 %정도인가요?
① 0%(한 번도 답변을 듣지 못함) ② 0% 이상~25% 미만
③ 25% 이상~50% 미만 ④ 50% 이상~75% 미만
⑤ 75% 이상 100% 미만 ⑥ 100%(모두 답변을 들음)

< 인터넷 쇼핑몰 >

4. 다음 중 주로 이용하는 쇼핑몰을 하나만 선택해주십시오.
① 쇼핑몰 A ② 쇼핑몰 B ③ 쇼핑몰 C ④ 쇼핑몰 D ⑤ 쇼핑몰 E
⑥ 쇼핑몰 F ⑦ 쇼핑몰 G ⑧ 쇼핑몰 H ⑨ 쇼핑몰 I ⑩ 쇼핑몰 J

4-1. 해당 쇼핑몰 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는지에 대해 안내를 받으셨습니까?
① 받았다 ② 받지 못했다.

4-2. 해당 사이트가 몇 개의 다른 회사와 개인정보를 공유하는지 알고 계십니까?
① 알고 있다 ② 모르고 있다.

4-3. (해당 사이트 이외의 다른 사이트도 포함하여) 쇼핑몰에서 물건을 구매하신 경험이 어느 정도입니까?
① 없다 ② 1~3회 ③ 4~10회 ④ 11~30회 ⑤ 30~99회 ⑥ 100회 이상

< 인터넷 포털사이트 >

5. 다음 중 주로 이용하는 포털 사이트를 하나만 선택해주십시오.
① 포털 A ② 포털 B ③ 포털 C ④ 포털 D ⑤ 포털 E
⑥ 포털 F ⑦ 포털 G ⑧ 포털 H ⑨ 포털 I ⑩ 포털 J

5-1. 해당 포털 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는지에 대해 안내를 받으셨습니까?
① 받았다 ② 받지 못했다.

5-2. 선택한 사이트가 몇 개의 다른 회사와 개인정보를 공유하는지 알고 계십니까?
① 알고 있다 ② 모르고 있다.

5-3. 귀하는 위의 사이트 중 몇 개의 사이트에 가입하셨습니까? _____개

< 언론사 사이트 >

6. 다음 중 주로 이용하는 언론사 사이트를 하나만 선택해주십시오.
① 언론사 A ② 언론사 B ③ 언론사 C ④ 언론사 D ⑤ 언론사 E
⑥ 언론사 F ⑦ 언론사 G ⑧ 언론사 H ⑨ 언론사 I ⑩ 언론사 J

6-1. 해당 언론사 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는지에 대해 안내를 받으셨습니까?
① 받았다 ② 받지 못했다.

6-2. 선택한 사이트가 몇 개의 다른 회사와 개인정보를 공유하는지 알고 계십니까?
① 알고 있다 ② 모르고 있다.

< 카드회사 >

7. 다음 중 주로 이용하는 카드회사를 하나만 선택해주십시오.
① 카드사 A ② 카드사 B ③ 카드사 C ④ 카드사 D ⑤ 카드사 E
⑥ 카드사 F ⑦ 카드사 G ⑧ 카드사 H ⑨ 카드사 I

7-1. 해당 카드회사 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는 지에 대해 안내를 받으셨습니까?
① 받았다 ② 받지 못했다.

7-2. 선택한 카드사가 몇 개의 다른 회사와 개인정보를 공유하는지 알고 계십

니까?
① 알고 있다　　② 모르고 있다.

< 인터넷 사이트의 개인정보 문의/상담 처리 >

8. 개인정보 관련 불만이나 질문을 전화를 통해 사이트 운영자 혹은 개인정보 관리책임자에 제기한 적이 있습니까?
① 없다　　② 있다

8-1. (9번 문항에 대해 ②라고 대답한 사람에게) 개인정보관리책임자가 전화를 받은 경우는 몇 %정도입니까?
① 0%(한 번도 전화를 받지 않음)　② 0% 이상~25% 미만
③ 25% 이상~50% 미만　　④ 50% 이상~75% 미만
⑤ 75% 이상 100% 미만　　⑥ 100%(모두 전화를 받음)

8-2. (9번 문항에 대해 ②라고 대답한 사람에게) 문제 해결에 얼마나 도움이 되었습니까?
① 전혀 도움이 되지 않음　② 별로 도움이 되지 않음　③ 그저 그렇다
④ 약간 도움이 됨　　⑤ 매우 도움이 됨

9. 개인정보 관련 불만이나 문의를 처리하기 위해, 사이트 운영자나 개인정보 관리책임자에게 e-mail을 보낸 적이 있습니까?
① 없다　　② 있다

9-1. (10번 문항에 대해 ②라고 대답한 사람에게) 개인정보관리책임자로부터

e-mail 회신을 받은 경우는 몇 %정도입니까?
① 0%(한 번도 회신을 받지 못함) ② 0% 이상~25% 미만
③ 25% 이상~50% 미만 ④ 50% 이상~75% 미만
⑤ 75% 이상 100% 미만 ⑥ 100%(모두 회신을 받음)

9-2. (10번 문항에 대해 ②라고 대답한 사람에게) e-mail 회신이 문제 해결에 얼마나 도움이 되었습니까?
① 전혀 도움이 되지 않음 ② 별로 도움이 되지 않음 ③ 그저 그렇다
④ 약간 도움이 됨 ⑤ 매우 도움이 됨

10. 개인정보 관련 불만이나 문의를 처리하기 위해, 사이트 게시판에 글을 올린 적이 있습니까?
① 없다 ② 있다

10-1. (11번 문항에 대해 ②라고 대답한 사람에게) 개인정보관리책임자가 답변을 한 경우는 몇 %정도입니까?
① 0%(한번도 답변 받지 못함) ② 0% 이상~25% 미만
③ 25% 이상~50% 미만 ④ 50% 이상~75% 미만
⑤ 75% 이상 100% 미만 ⑥ 100%(모두 답변 받음)

10-2. (11번 문항에 대해 ②라고 대답한 사람에게) 답변이 문제 해결에 얼마나 도움이 되었습니까?
① 전혀 도움이 되지 않음 ② 별로 도움이 되지 않음 ③ 그저 그렇다
④ 약간 도움이 됨 ⑤ 매우 도움이 됨

< 개인 정보 유출 >

11. 인터넷 사이트에 회원 가입을 할 때, 여러 가지 개인정보를 입력해야 합니다. 다음 개인정보 중 입력이 가장 꺼려지는 정보는 어떤 정보입니까?
① 이름 ② 주민등록번호 ③ 전화번호 ④ 핸드폰 번호
⑤ e-mail 주소 ⑥ 직장 ⑦ 학교 ⑧ 주소 ⑨ 기타 _____

12. 회원 가입시 주민등록번호를 요구하고 있습니다. 기업들이 회원 가입시 주민등록번호를 요구하는 것에 대해 어떻게 생각하십니까?
① 유출되지 않는다는 것만 보장된다면 수집해도 좋다
② 유출되지 않는다는 보장이 있다 하더라도, 실명 확인이 필요한 경우에만 수집해야 한다
③ 실명 확인이 필요하다 하더라도 대체할 만한 방법이 있는 한 수집하지 않아야 한다

13. 주민등록번호가 도용되어 회원 가입에 실패한 경험이 있습니까?
① 없다 ② 1회 ③ 2~4회 ④ 5~9회 ⑤ 10회 이상

14. 가입한 적이 없는 회사로부터 스팸메일을 받는 경우가 몇 회 정도입니까?
① 1일 20건 이상 ② 1일 10건~1일 20건 미만 ③ 1일 2건~1일 10건 미만
④ 주 3건 이상~1일 2건 미만 ⑤ 주 1건~주 3건 미만 ⑥ 없다

14-1. 원치 않는 메일을 받았을 경우 어떻게 대처하십니까?
① 읽지 않고 삭제한다 ② 발신자에게 수신거부 신청을 한다
③ 발신자 메일 주소를 내 메일 프로그램(혹은 서비스)의 차단 목록에 올려놓는다

14-2. (15-1 문항에 대해 ②라고 대답한 사람에게) 수신거부 신청의 효과가 어느 정도입니까?

① 수신거부 신청이 비교적 잘 받아들여지는 편이다.
② 여러 차례 수신거부 신청을 해야만 받아들여진다.
③ 아무리 수신거부 신청을 하더라도 계속 메일이 온다.
④ 수신거부 신청을 하고 나서 오히려 다른 스팸메일들이 더 늘어났다.

15. 회원 탈퇴시 신분증 사본이나 주민등록등본을 제출할 것을 요구하는 사이트를 만난 적이 몇 번 정도입니까?
① 없다 ② 1개 사이트 ③ 2~4개 ④ 5~10개 ⑤ 10개 이상

< 인구통계 특성 >

1. 귀하의 나이는?
① 10대 ② 20대 ③ 30대 ④ 40대 ⑤ 50대 이상

2. 귀하의 성별은?
① 남 ② 여

3. 귀하의 학력은?
① 초등졸 이하 ② 중졸 이하 ③ 고졸 이하 ④ 대졸 이하 ⑤ 대학원생 이상

3. 개인정보 보호에 관한 이용자들의 의식과 태도 설문 결과

문1. 인터넷 서비스를 이용하기 위해 회원 가입을 할 때, 이용약관을 읽어보십니까?

			꼼꼼히 읽어보는 편이다	부분적으로 읽어보는 편이다	거의 읽지 않는 편이다	Total
Total		빈도	86	362	594	1042
		(%)	8.3	34.7	57.0	100.0
연령별	10대	빈도	2	3	4	9
		(%)	22.2	33.3	44.4	100.0
	20대	빈도	26	111	223	360
		(%)	7.2	30.8	61.9	100.0
	30대	빈도	45	178	276	499
		(%)	9.0	35.7	55.3	100.0
	40대	빈도	7	59	46	112
		(%)	6.3	52.7	41.1	100.0
	50대 이상	빈도	6	11	45	62
		(%)	9.7	17.7	72.6	100.0
성별	남	빈도	48	197	291	536
		(%)	9.0	36.8	54.3	100.0
	여	빈도	38	165	303	506
		(%)	7.5	32.6	59.9	100.0
학력별	초등졸 이하	빈도	0	0	6	6
		(%)	0.0	0.0	100.0	100.0
	중졸 이하	빈도	0	4	3	7
		(%)	0.0	57.1	42.9	100.0
	고졸 이하	빈도	31	131	194	356
		(%)	8.7	36.8	54.5	100.0
	대졸 이하	빈도	50	217	378	645
		(%)	7.8	33.6	58.6	100.0
	대학원생 이상	빈도	5	10	13	28
		(%)	17.9	35.7	46.4	100.0

문1-1. 주로 읽는 내용은 어떤 부분입니까?(복수응답 가능)

			요금 관련 사항	개인정보 관련 사항	이용자 권리 관련 사항	물품 구매 관련 사항	기타	Total
Total		빈도	227	165	133	29	17	362
		(%)	62.7	45.6	36.7	8.0	4.7	100.0
연령별	10대	빈도	3	1	0	0	0	3
		(%)	100.0	33.3	0.0	0.0	0.0	100.0
	20대	빈도	68	53	31	6	10	111
		(%)	61.3	47.7	27.9	5.4	9.0	100.0
	30대	빈도	111	78	70	18	5	178
		(%)	62.4	43.8	39.3	10.1	2.8	100.0
	40대	빈도	38	29	26	5	2	59
		(%)	64.4	49.2	44.1	8.5	3.4	100.0
	50대 이상	빈도	7	4	6	0	0	11
		(%)	63.6	36.4	54.5	0.0	0.0	100.0
성별	남	빈도	114	92	76	12	10	197
		(%)	57.9	46.7	38.6	6.1	5.1	100.0
	여	빈도	113	73	57	17	7	165
		(%)	68.5	44.2	34.5	10.3	4.2	100.0
학력별	중졸 이하	빈도	3	3	0	0	0	4
		(%)	75.0	75.0	0.0	0.0	0.0	100.0
	고졸 이하	빈도	74	56	50	12	4	131
		(%)	56.5	42.7	38.2	9.2	3.1	100.0
	대졸 이하	빈도	145	101	78	16	12	217
		(%)	66.8	46.5	35.9	7.4	5.5	100.0
	대학원생 이상	빈도	5	5	5	1	1	10
		(%)	50.0	50.0	50.0	10.0	10.0	100.0

문1-2. 읽어보지 않는 이유는 무엇입니까?

			어느 사이트나 내용이 거의 같다	구체적인 정보를 주지 않고 있다	양이 지나치게 많다	안 읽어도 별다른 문제가 발생하지 않는다	기타	Total
Total		빈도	130	30	316	114	4	594
		(%)	21.9	5.1	53.2	19.2	0.7	100.0
연령별	10대	빈도	0	0	4	0	0	4
		(%)	0.0	0.0	100.0	0.0	0.0	100.0
	20대	빈도	43	7	139	33	1	223
		(%)	19.3	3.1	62.3	14.8	0.4	100.0
	30대	빈도	67	16	128	63	2	276
		(%)	24.3	5.8	46.4	22.8	0.7	100.0
	40대	빈도	9	6	22	8	1	46
		(%)	19.6	13.0	47.8	17.4	2.2	100.0
	50대 이상	빈도	11	1	23	10	0	45
		(%)	24.4	2.2	51.1	22.2	0.0	100.0
성별	남	빈도	75	19	134	62	1	291
		(%)	25.8	6.5	46.0	21.3	0.3	100.0
	여	빈도	55	11	182	52	3	303
		(%)	18.2	3.6	60.1	17.2	1.0	100.0
학력별	초등졸 이하	빈도	0	0	6	0	0	6
		(%)	0.0	0.0	100.0	0.0	0.0	100.0
	중졸 이하	빈도	1	0	1	1	0	3
		(%)	33.3	0.0	33.3	33.3	0.0	100.0
	고졸 이하	빈도	39	11	112	31	1	194
		(%)	20.1	5.7	57.7	16.0	0.5	100.0
	대졸 이하	빈도	86	18	192	79	3	378
		(%)	22.8	4.8	50.8	20.9	0.8	100.0
	대학원생 이상	빈도	4	1	5	3	0	13
		(%)	30.8	7.7	38.5	23.1	0.0	100.0

문2. 인터넷 서비스를 이용하기 위해 회원 가입을 할 때, 개인정보 보호정책을 읽어보십니까?

			꼼꼼히 읽어보는 편이다	부분적으로 읽어보는 편이다	거의 읽지 않는 편이다	Total
Total		빈도	118	342	582	1042
		(%)	11.3	32.8	55.9	100.0
연령별	10대	빈도	3	2	4	9
		(%)	33.3	22.2	44.4	100.0
	20대	빈도	33	102	225	360
		(%)	9.2	28.3	62.5	100.0
	30대	빈도	59	181	259	499
		(%)	11.8	36.3	51.9	100.0
	40대	빈도	15	50	47	112
		(%)	13.4	44.6	42.0	100.0
	50대 이상	빈도	8	7	47	62
		(%)	12.9	11.3	75.8	100.0
성별	남	빈도	65	184	287	536
		(%)	12.1	34.3	53.5	100.0
	여	빈도	53	158	295	506
		(%)	10.5	31.2	58.3	100.0
학력별	초등졸 이하	빈도	0	1	5	6
		(%)	0.0	16.7	83.3	100.0
	중졸 이하	빈도	1	1	5	7
		(%)	14.3	14.3	71.4	100.0
	고졸 이하	빈도	50	124	182	356
		(%)	14.0	34.8	51.1	100.0
	대졸 이하	빈도	63	206	376	645
		(%)	9.8	31.9	58.3	100.0
	대학원생 이상	빈도	4	10	14	28
		(%)	14.3	35.7	50.0	100.0

문2-1. 주로 읽는 내용은 어떤 부분입니까?(복수응답 가능)

			제3자의 공유 관련 사항	가입,탈퇴에 관한 사항	이용자 권리 관련 사항	쿠키 관련 사항	기타	Total
Total		빈도	53	195	193	20	12	342
		(%)	15.5	57.0	56.4	5.8	3.5	100.0
연령별	10대	빈도	0	1	0	0	1	2
		(%)	0.0	50.0	0.0	0.0	50.0	100.0
	20대	빈도	10	55	58	10	4	102
		(%)	9.8	53.9	56.9	9.8	3.9	100.0
	30대	빈도	31	102	101	5	4	181
		(%)	17.1	56.4	55.8	2.8	2.2	100.0
	40대	빈도	11	32	29	4	3	50
		(%)	22.0	64.0	58.0	8.0	6.0	100.0
	50대 이상	빈도	1	5	5	1	0	7
		(%)	14.3	71.4	71.4	14.3	0.0	100.0
성별	남	빈도	27	104	103	14	8	184
		(%)	14.7	56.5	56.0	7.6	4.3	100.0
	여	빈도	26	91	90	6	4	158
		(%)	16.5	57.6	57.0	3.8	2.5	100.0
학력별	초등졸 이하	빈도	0	1	0	0	0	1
		(%)	0.0	100.0	0.0	0.0	0.0	100.0
	중졸 이하	빈도	0	1	0	0	0	1
		(%)	0.0	100.0	0.0	0.0	0.0	100.0
	고졸 이하	빈도	22	66	78	3	4	124
		(%)	17.7	53.2	62.9	2.4	3.2	100.0
	대졸 이하	빈도	31	121	112	16	8	206
		(%)	15.0	58.7	54.4	7.8	3.9	100.0
	대학원생 이상	빈도	0	6	3	1	0	10
		(%)	0.0	60.0	30.0	10.0	0.0	100.0

문2-2. 읽어보지 않는 이유는 무엇입니까?

			어느 사이트나 내용이 거의 같다	구체적인 정보를 주지 않고 있다	양이 지나치게 많다	안 읽어도 별다른 문제가 발생하지 않는다	Total
Total		빈도	130	43	278	131	582
		(%)	22.3	7.4	47.8	22.5	100.0
연령별	10대	빈도	0	0	3	1	4
		(%)	0.0	0.0	75.0	25.0	100.0
	20대	빈도	44	16	113	52	225
		(%)	19.6	7.1	50.2	23.1	100.0
	30대	빈도	64	22	115	58	259
		(%)	24.7	8.5	44.4	22.4	100.0
	40대	빈도	13	2	23	9	47
		(%)	27.7	4.3	48.9	19.1	100.0
	50대 이상	빈도	9	3	24	11	47
		(%)	19.1	6.4	51.1	23.4	100.0
성별	남	빈도	69	24	126	68	287
		(%)	24.0	8.4	43.9	23.7	100.0
	여	빈도	61	19	152	63	295
		(%)	20.7	6.4	51.5	21.4	100.0
학력별	초등졸 이하	빈도	1	1	3	0	5
		(%)	20.0	20.0	60.0	0.0	100.0
	중졸 이하	빈도	1	1	1	2	5
		(%)	20.0	20.0	20.0	40.0	100.0
	고졸 이하	빈도	33	15	96	38	182
		(%)	18.1	8.2	52.7	20.9	100.0
	대졸 이하	빈도	91	26	172	87	376
		(%)	24.2	6.9	45.7	23.1	100.0
	대학원생 이상	빈도	4	0	6	4	14
		(%)	28.6	0.0	42.9	28.6	100.0

문3. 텔레마케팅 전화가 결려올 경우, 개인정보 취득경위에 대해 질문을 한 경험이 있습니까?

			있다	없다	Total
Total		빈도	242	800	1042
		(%)	23.2	76.8	100.0
연령별	10대	빈도	2	7	9
		(%)	22.2	77.8	100.0
	20대	빈도	76	284	360
		(%)	21.1	78.9	100.0
	30대	빈도	121	378	499
		(%)	24.2	75.8	100.0
	40대	빈도	35	77	112
		(%)	31.3	68.8	100.0
	50대 이상	빈도	8	54	62
		(%)	12.9	87.1	100.0
성별	남	빈도	141	395	536
		(%)	26.3	73.7	100.0
	여	빈도	101	405	506
		(%)	20.0	80.0	100.0
학력별	초등졸 이하	빈도	1	5	6
		(%)	16.7	83.3	100.0
	중졸 이하	빈도	1	6	7
		(%)	14.3	85.7	100.0
	고졸 이하	빈도	75	281	356
		(%)	21.1	78.9	100.0
	대졸 이하	빈도	160	485	645
		(%)	24.8	75.2	100.0
	대학원생 이상	빈도	5	23	28
		(%)	17.9	82.1	100.0

문3-1. 질문에 대한 답변을 듣는 경우는 몇 % 정도인가요?

			0%(한번도 답변을 듣지 못함)	0% 이상 ~25% 미만	25% 이상 ~50% 미만	50% 이상 ~75% 미만	75% 이상 ~100% 미만	100%(모두 답변을 들음)	Total
Total		빈도	69	80	61	16	10	6	242
		(%)	28.5	33.1	25.2	6.6	4.1	2.5	100.0
연령별	10대	빈도	2	0	0	0	0	0	2
		(%)	100.0	0.0	0.0	0.0	0.0	0.0	100.0
	20대	빈도	23	20	18	8	5	2	76
		(%)	30.3	26.3	23.7	10.5	6.6	2.6	100.0
	30대	빈도	33	45	29	6	4	4	121
		(%)	27.3	37.2	24.0	5.0	3.3	3.3	100.0
	40대	빈도	7	12	14	2	0	0	35
		(%)	20.0	34.3	40.0	5.7	0.0	0.0	100.0
	50대 이상	빈도	4	3	0	0	1	0	8
		(%)	50.0	37.5	0.0	0.0	12.5	0.0	100.0
성별	남	빈도	43	42	41	9	4	2	141
		(%)	30.5	29.8	29.1	6.4	2.8	1.4	100.0
	여	빈도	26	38	20	7	6	4	101
		(%)	25.7	37.6	19.8	6.9	5.9	4.0	100.0
학력별	초등졸 이하	빈도	1	0	0	0	0	0	1
		(%)	100.0	0.0	0.0	0.0	0.0	0.0	100.0
	중졸 이하	빈도	1	0	0	0	0	0	1
		(%)	100.0	0.0	0.0	0.0	0.0	0.0	100.0
	고졸 이하	빈도	22	24	18	5	3	3	75
		(%)	29.3	32.0	24.0	6.7	4.0	4.0	100.0
	대졸 이하	빈도	42	55	42	11	7	3	160
		(%)	26.3	34.4	26.3	6.9	4.4	1.9	100.0
	대학원생 이상	빈도	3	1	1	0	0	0	5
		(%)	60.0	20.0	20.0	0.0	0.0	0.0	100.0

문4. 다음 중 주로 이용하는 쇼핑몰 사이트를 하나만 선택해 주십시오.

			쇼핑몰 A	쇼핑몰 B	쇼핑몰 C	쇼핑몰 D	쇼핑몰 E	쇼핑몰 F	쇼핑몰 G	쇼핑몰 H	쇼핑몰 I	쇼핑몰 J	Total
Total		빈도	107	198	58	22	147	12	81	62	178	177	1042
		(%)	10.3	19.0	5.6	2.1	14.1	1.2	7.8	6.0	17.1	17.0	100.0
연령별	10대	빈도	1	1	1	0	3	0	2	0	0	1	9
		(%)	11.1	11.1	11.1	0.0	33.3	0.0	22.2	0.0	0.0	11.1	100.0
	20대	빈도	33	59	18	8	50	4	32	17	61	78	360
		(%)	9.2	16.4	5.0	2.2	13.9	1.1	8.9	4.7	16.9	21.7	100.0
	30대	빈도	50	98	28	9	75	5	35	33	83	83	499
		(%)	10.0	19.6	5.6	1.8	15.0	1.0	7.0	6.6	16.6	16.6	100.0
	40대	빈도	13	24	6	2	11	2	10	8	23	13	112
		(%)	11.6	21.4	5.4	1.8	9.8	1.8	8.9	7.1	20.5	11.6	100.0
	50대 이상	빈도	10	16	5	3	8	1	2	4	11	2	62
		(%)	16.1	25.8	8.1	4.8	12.9	1.6	3.2	6.5	17.7	3.2	100.0
성별	남	빈도	65	78	30	12	94	2	40	28	95	92	536
		(%)	12.1	14.6	5.6	2.2	17.5	0.4	7.5	5.2	17.7	17.2	100.0
	여	빈도	42	120	28	10	53	10	41	34	83	85	506
		(%)	8.3	23.7	5.5	2.0	10.5	2.0	8.1	6.7	16.4	16.8	100.0
학력별	초등졸 이하	빈도	1	3	1	0	1	0	0	0	0	0	6
		(%)	16.7	50.0	16.7	0.0	16.7	0.0	0.0	0.0	0.0	0.0	100.0
	중졸 이하	빈도	1	0	0	0	0	0	0	1	3	2	7
		(%)	14.3	0.0	0.0	0.0	0.0	0.0	0.0	14.3	42.9	28.6	100.0
	고졸 이하	빈도	37	75	22	9	59	3	22	21	60	48	356
		(%)	10.4	21.1	6.2	2.5	16.6	0.8	6.2	5.9	16.9	13.5	100.0
	대졸 이하	빈도	66	116	34	12	83	9	52	37	114	122	645
		(%)	10.2	18.0	5.3	1.9	12.9	1.4	8.1	5.7	17.7	18.9	100.0
	대학원생 이상	빈도	2	4	1	1	4	0	7	3	1	5	28
		(%)	7.1	14.3	3.6	3.6	14.3	0.0	25.0	10.7	3.6	17.9	100.0

문4-1. 해당 쇼핑몰 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는 지에 대한 안내를 받으셨습니까?

		받았다	받지 못했다	Total
쇼핑몰 A	빈도	29	78	107
	(%)	27.1	72.9	100.0
쇼핑몰 B	빈도	23	175	198
	(%)	11.6	88.4	100.0
쇼핑몰 C	빈도	17	41	58
	(%)	29.3	70.7	100.0
쇼핑몰 D	빈도	6	16	22
	(%)	27.3	72.7	100.0
쇼핑몰 E	빈도	27	120	147
	(%)	18.4	81.6	100.0
쇼핑몰 F	빈도	0	12	12
	(%)	0.0	100.0	100.0
쇼핑몰 G	빈도	6	75	81
	(%)	7.4	92.6	100.0
쇼핑몰 H	빈도	9	53	62
	(%)	14.5	85.5	100.0
쇼핑몰 I	빈도	34	144	178
	(%)	19.1	80.9	100.0
쇼핑몰 J	빈도	28	149	177
	(%)	15.8	84.2	100.0
Total	빈도	179	863	1042
	(%)	17.2	82.8	100.0

문4-2. 해당 사이트가 몇 개의 다른 회사와 개인정보를 공유하는지 알고 계십니까?

		알고 있다	모르고 있다	Total
쇼핑몰 A	빈도	15	92	107
	(%)	14.0	86.0	100.0
쇼핑몰 B	빈도	8	190	198
	(%)	4.0	96.0	100.0
쇼핑몰 C	빈도	15	43	58
	(%)	25.9	74.1	100.0
쇼핑몰 D	빈도	7	15	22
	(%)	31.8	68.2	100.0
쇼핑몰 E	빈도	17	130	147
	(%)	11.6	88.4	100.0
쇼핑몰 F	빈도	0	12	12
	(%)	0.0	100.0	100.0
쇼핑몰 G	빈도	1	80	81
	(%)	1.2	98.8	100.0
쇼핑몰 H	빈도	9	53	62
	(%)	14.5	85.5	100.0
쇼핑몰 I	빈도	20	158	178
	(%)	11.2	88.8	100.0
쇼핑몰 J	빈도	16	161	177
	(%)	9.0	91.0	100.0
Total	빈도	108	934	1042
	(%)	10.4	89.6	100.0

문4-3. (해당 사이트 외에 다른 사이트도 포함하여) 쇼핑몰에서 물건을 구매하신 경험이 어느 정도 입니까?

			없다	1~3회	4~10회	11~30회	30~99회	100회 이상	Total
Total		빈도	319	409	169	102	36	7	1042
		(%)	30.6	39.3	16.2	9.8	3.5	0.7	100.0
연령별	10대	빈도	6	1	2	0	0	0	9
		(%)	66.7	11.1	22.2	0.0	0.0	0.0	100.0
	20대	빈도	110	134	52	44	17	3	360
		(%)	30.6	37.2	14.4	12.2	4.7	0.8	100.0
	30대	빈도	149	203	85	45	14	3	499
		(%)	29.9	40.7	17.0	9.0	2.8	0.6	100.0
	40대	빈도	28	47	24	8	4	1	112
		(%)	25.0	42.0	21.4	7.1	3.6	0.9	100.0
	50대 이상	빈도	26	24	6	5	1	0	62
		(%)	41.9	38.7	9.7	8.1	1.6	0.0	100.0
성별	남	빈도	196	206	84	35	11	4	536
		(%)	36.6	38.4	15.7	6.5	2.1	0.7	100.0
	여	빈도	123	203	85	67	25	3	506
		(%)	24.3	40.1	16.8	13.2	4.9	0.6	100.0
학력별	초등졸 이하	빈도	5	1	0	0	0	0	6
		(%)	83.3	16.7	0.0	0.0	0.0	0.0	100.0
	중졸 이하	빈도	2	4	1	0	0	0	7
		(%)	28.6	57.1	14.3	0.0	0.0	0.0	100.0
	고졸 이하	빈도	145	134	45	20	11	1	356
		(%)	40.7	37.6	12.6	5.6	3.1	0.3	100.0
	대졸 이하	빈도	157	264	115	80	24	5	645
		(%)	24.3	40.9	17.8	12.4	3.7	0.8	100.0
	대학원생 이상	빈도	10	6	8	2	1	1	28
		(%)	35.7	21.4	28.6	7.1	3.6	3.6	100.0

문5. 다음 중 주로 이용하는 포털 사이트를 하나만 선택해 주십시오.

			포털 A	포털 B	포털 C	포털 D	포털 E	포털 F	포털 G	포털 H	포털 I	포털 J	Total
Total		빈도	469	23	27	8	43	13	23	407	14	15	1042
		(%)	45.0	2.2	2.6	0.8	4.1	1.2	2.2	39.1	1.3	1.4	100.0
연령별	10대	빈도	5	0	1	0	0	0	0	3	0	0	9
		(%)	55.6	0.0	11.1	0.0	0.0	0.0	0.0	33.3	0.0	0.0	100.0
	20대	빈도	125	7	12	2	12	5	5	184	2	6	360
		(%)	34.7	1.9	3.3	0.6	3.3	1.4	1.4	51.1	0.6	1.7	100.0
	30대	빈도	237	14	13	6	22	7	10	171	12	7	499
		(%)	47.5	2.8	2.6	1.2	4.4	1.4	2.0	34.3	2.4	1.4	100.0
	40대	빈도	65	2	0	0	4	1	6	32	0	2	112
		(%)	58.0	1.8	0.0	0.0	3.6	0.9	5.4	28.6	0.0	1.8	100.0
	50대 이상	빈도	37	0	1	0	5	0	2	17	0	0	62
		(%)	59.7	0.0	1.6	0.0	8.1	0.0	3.2	27.4	0.0	0.0	100.0
성별	남	빈도	242	12	13	6	26	6	13	200	8	10	536
		(%)	45.1	2.2	2.4	1.1	4.9	1.1	2.4	37.3	1.5	1.9	100.0
	여	빈도	227	11	14	2	17	7	10	207	6	5	506
		(%)	44.9	2.2	2.8	0.4	3.4	1.4	2.0	40.9	1.2	1.0	100.0
학력별	초등졸 이하	빈도	4	0	1	0	0	0	0	1	0	0	6
		(%)	66.7	0.0	16.7	0.0	0.0	0.0	0.0	16.7	0.0	0.0	100.0
	중졸 이하	빈도	5	0	0	0	0	0	0	2	0	0	7
		(%)	71.4	0.0	0.0	0.0	0.0	0.0	0.0	28.6	0.0	0.0	100.0
	고졸 이하	빈도	167	5	9	0	18	7	6	132	5	7	356
		(%)	46.9	1.4	2.5	0.0	5.1	2.0	1.7	37.1	1.4	2.0	100.0
	대졸 이하	빈도	280	18	16	7	25	6	17	259	9	8	645
		(%)	43.4	2.8	2.5	1.1	3.9	0.9	2.6	40.2	1.4	1.2	100
	대학원생 이상	빈도	13	0	1	1	0	0	0	13	0	0	28
		(%)	46.4	0.0	3.6	3.6	0.0	0.0	0.0	46.4	0.0	0.0	100.0

문5-1. 해당 포털 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는지에 대해 안내를 받으셨습니까?

		받았다	받지 못했다	Total
포털 A	빈도	75	394	469
	(%)	16.0	84.0	100.0
포털 B	빈도	0	23	23
	(%)	0.0	100.0	100.0
포털 C	빈도	1	26	27
	(%)	3.7	96.3	100.0
포털 D	빈도	1	7	8
	(%)	12.5	87.5	100.0
포털 E	빈도	11	32	43
	(%)	25.6	74.4	100.0
포털 F	빈도	2	11	13
	(%)	15.4	84.6	100.0
포털 G	빈도	0	23	23
	(%)	0.0	100.0	100.0
포털 H	빈도	60	347	407
	(%)	14.7	85.3	100.0
포털 I	빈도	1	13	14
	(%)	7.1	92.9	100.0
포털 J	빈도	2	13	15
	(%)	13.3	86.7	100.0
Total	빈도	153	889	1042
	(%)	14.7	85.3	100.0

문5-2. 선택한 사이트가 몇 개의 다른 회사와 개인정보를 공유하는 지 알고 계십니까?

		알고 있다	모르고 있다	Total
포털 A	빈도	51	418	469
	(%)	10.9	89.1	100.0
포털 B	빈도	0	23	23
	(%)	0.0	100.0	100.0
포털 C	빈도	2	25	27
	(%)	7.4	92.6	100.0
포털 D	빈도	1	7	8
	(%)	12.5	87.5	100.0
포털 E	빈도	6	37	43
	(%)	14.0	86.0	100.0
포털 F	빈도	1	12	13
	(%)	7.7	92.3	100.0
포털 G	빈도	0	23	23
	(%)	0.0	100.0	100.0
포털 H	빈도	42	365	407
	(%)	10.3	89.7	100.0
포털 I	빈도	0	14	14
	(%)	0.0	100.0	100.0
포털 J	빈도	3	12	15
	(%)	20.0	80.0	100.0
Total	빈도	106	936	1042
	(%)	10.2	89.8	100.0

문5-3. 귀하는 위의 사이트 중 몇 개의 사이트에 가입하셨습니까?

			0개	1개	2개	3개	4개	5개	6개	7개	8개	9개	10개	Total
Total		빈도	27	227	308	203	78	65	43	19	16	2	54	1042
		(%)	2.6	21.8	29.6	19.5	7.5	6.2	4.1	1.8	1.5	0.2	5.2	100.0
연령별	10대	빈도	1	2	1	2	0	0	0	1	1	0	1	9
		(%)	11.1	22.2	11.1	22.2	0.0	0.0	0.0	11.1	11.1	0.0	11.1	100
	20대	빈도	4	40	91	102	36	25	23	9	9	1	20	360
		(%)	1.1	11.1	25.3	28.3	10.0	6.9	6.4	2.5	2.5	0.3	5.6	100.0
	30대	빈도	19	150	185	57	28	15	7	4	3	0	31	499
		(%)	3.8	30.1	37.1	11.4	5.6	3.0	1.4	0.8	0.6	0.0	6.2	100.0
	40대	빈도	2	10	14	28	13	22	13	5	3	1	1	112
		(%)	1.8	8.9	12.5	25.0	11.6	19.6	11.6	4.5	2.7	0.9	0.9	100.0
	50대 이상	빈도	1	25	17	14	1	3	0	0	0	0	1	62
		(%)	1.6	40.3	27.4	22.6	1.6	4.8	0.0	0.0	0.0	0.0	1.6	100.0
성별	남	빈도	16	136	178	91	26	20	12	5	4	1	47	536
		(%)	3.0	25.4	33.2	17.0	4.9	3.7	2.2	0.9	0.7	0.2	8.8	100.0
	여	빈도	11	91	130	112	52	45	31	14	12	1	7	506
		(%)	2.2	18.0	25.7	22.1	10.3	8.9	6.1	2.8	2.4	0.2	1.4	100.0
학력별	초등졸 이하	빈도	0	2	3	1	0	0	0	0	0	0	0	6
		(%)	0.0	33.3	50.0	16.7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
	중졸 이하	빈도	0	2	0	2	1	0	0	0	2	0	0	7
		(%)	0.0	28.6	0.0	28.6	14.3	0.0	0.0	0.0	28.6	0.0	0.0	100.0
	고졸 이하	빈도	10	92	101	75	32	18	8	6	0	1	13	356
		(%)	2.8	25.8	28.4	21.1	9.0	5.1	2.2	1.7	0.0	0.3	3.7	100.0
	대졸 이하	빈도	17	126	193	119	44	45	35	13	13	1	39	645
		(%)	2.6	19.5	29.9	18.4	6.8	7.0	5.4	2.0	2.0	0.2	6.0	100
	대학원생 이상	빈도	0	5	11	6	1	2	0	0	1	0	2	28
		(%)	0.0	17.9	39.3	21.4	3.6	7.1	0.0	0.0	3.6	0.0	7.1	100.0

문6. 다음 중 주로 이용하는 언론사 사이트를 하나만 선택해 주십시오.

			언론사 A	언론사 B	언론사 C	언론사 D	언론사 E	언론사 F	언론사 G	언론사 H	언론사 I	언론사 J	Total
Total		빈도	192	154	44	174	114	84	70	71	131	8	1042
		(%)	18.4	14.8	4.2	16.7	10.9	8.1	6.7	6.8	12.6	0.8	100.0
연령별	10대	빈도	1	2	0	0	2	1	2	1	0	0	9
		(%)	11.1	22.2	0.0	0.0	22.2	11.1	22.2	11.1	0.0	0.0	100.0
	20대	빈도	64	47	13	68	48	34	24	15	46	1	360
		(%)	17.8	13.1	3.6	18.9	13.3	9.4	6.7	4.2	12.8	0.3	100.0
	30대	빈도	92	75	21	90	45	38	32	38	62	6	499
		(%)	18.4	15.0	4.2	18.0	9.0	7.6	6.4	7.6	12.4	1.2	100.0
	40대	빈도	16	19	7	9	14	10	5	13	19	0	112
		(%)	14.3	17.0	6.3	8.0	12.5	8.9	4.5	11.6	17.0	0.0	100.0
	50대 이상	빈도	19	11	3	7	5	1	7	4	4	1	62
		(%)	30.6	17.7	4.8	11.3	8.1	1.6	11.3	6.5	6.5	1.6	100
성별	남	빈도	117	80	33	69	48	28	37	37	83	4	536
		(%)	21.8	14.9	6.2	12.9	9.0	5.2	6.9	6.9	15.5	0.7	100.0
	여	빈도	75	74	11	105	66	56	33	34	48	4	506
		(%)	14.8	14.6	2.2	20.8	13.0	11.1	6.5	6.7	9.5	0.8	100.0
학력별	초등졸 이하	빈도	0	1	0	0	0	1	2	2	0	0	6
		(%)	0.0	16.7	0.0	0.0	0.0	16.7	33.3	33.3	0.0	0.0	100.0
	중졸 이하	빈도	1	1	0	1	1	1	1	1	0	0	7
		(%)	14.3	14.3	0.0	14.3	14.3	14.3	14.3	14.3	0.0	0.0	100.0
	고졸 이하	빈도	46	49	7	71	55	30	25	15	57	1	356
		(%)	12.9	13.8	2.0	19.9	15.4	8.4	7.0	4.2	16.0	0.3	100.0
	대졸 이하	빈도	138	97	35	99	55	50	40	51	73	7	645
		(%)	21.4	15.0	5.4	15.3	8.5	7.8	6.2	7.9	11.3	1.1	100.0
	대학원생 이상	빈도	7	6	2	3	3	2	2	2	1	0	28
		(%)	25.0	21.4	7.1	10.7	10.7	7.1	7.1	7.1	3.6	0.0	100.0

문6-1. 해당 언론사 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는 지에 대해 안내를 받으셨습니까?

		받았다	받지 못했다	Total
언론사 A	빈도	28	164	192
	(%)	14.6	85.4	100.0
언론사 B	빈도	28	126	154
	(%)	18.2	81.8	100.0
언론사 C	빈도	5	39	44
	(%)	11.4	88.6	100.0
언론사 D	빈도	6	168	174
	(%)	3.4	96.6	100.0
언론사 E	빈도	6	108	114
	(%)	5.3	94.7	100.0
언론사 F	빈도	5	79	84
	(%)	6.0	94.0	100.0
언론사 G	빈도	5	65	70
	(%)	7.1	92.9	100.0
언론사 H	빈도	10	61	71
	(%)	14.1	85.9	100.0
언론사 I	빈도	19	112	131
	(%)	14.5	85.5	100.0
언론사 J	빈도	0	8	8
	(%)	0.0	100.0	100.0
Total	빈도	112	930	1042
	(%)	10.7	89.3	100.0

문6-2. 선택한 사이트가 몇 개의 다른 회사와 개인정보를 공유하는 지 알고 계십니까?

		알고 있다	모르고 있다	Total
언론사 A	빈도	23	169	192
	(%)	12.0	88.0	100.0
언론사 B	빈도	19	135	154
	(%)	12.3	87.7	100.0
언론사 C	빈도	3	41	44
	(%)	6.8	93.2	100.0
언론사 D	빈도	7	167	174
	(%)	4.0	96.0	100.0
언론사 E	빈도	4	110	114
	(%)	3.5	96.5	100.0
언론사 F	빈도	3	81	84
	(%)	3.6	96.4	100.0
언론사 G	빈도	3	67	70
	(%)	4.3	95.7	100.0
언론사 H	빈도	7	64	71
	(%)	9.9	90.1	100.0
언론사 I	빈도	14	117	131
	(%)	10.7	89.3	100.0
언론사 J	빈도	0	8	8
	(%)	0.0	100.0	100.0
Total	빈도	83	959	1042
	(%)	8.0	92.0	100.0

문7. 다음 중 주로 이용하는 카드회사를 하나만 선택해 주십시오.

			카드사 A	카드사 B	카드사 C	카드사 D	카드사 E	카드사 F	카드사 G	카드사 H	카드사 I	Total
Total		빈도	294	198	181	62	221	23	12	29	22	1042
		(%)	28.2	19.0	17.4	6.0	21.2	2.2	1.2	2.8	2.1	100.0
연령별	10대	빈도	3	1	1	0	1	0	0	2	1	9
		(%)	33.3	11.1	11.1	0.0	11.1	0.0	0.0	22.2	11.1	100.0
	20대	빈도	105	78	59	26	67	3	3	12	7	360
		(%)	29.2	21.7	16.4	7.2	18.6	0.8	0.8	3.3	1.9	100.0
	30대	빈도	142	89	88	27	110	15	6	10	12	499
		(%)	28.5	17.8	17.6	5.4	22.0	3.0	1.2	2.0	2.4	100.0
	40대	빈도	29	22	23	7	21	4	2	2	2	112
		(%)	25.9	19.6	20.5	6.3	18.8	3.6	1.8	1.8	1.8	100.0
	50대 이상	빈도	15	8	10	2	22	1	1	3	0	62
		(%)	24.2	12.9	16.1	3.2	35.5	1.6	1.6	4.8	0.0	100.0
성별	남	빈도	155	104	85	32	107	14	6	19	14	536
		(%)	28.9	19.4	15.9	6.0	20.0	2.6	1.1	3.5	2.6	100.0
	여	빈도	139	94	96	30	114	9	6	10	8	506
		(%)	27.5	18.6	19.0	5.9	22.5	1.8	1.2	2.0	1.6	100.0
학력별	초등졸 이하	빈도	2	1	0	0	1	0	1	0	1	6
		(%)	33.3	16.7	0.0	0.0	16.7	0.0	16.7	0.0	16.7	100.0
	중졸 이하	빈도	3	0	1	0	3	0	0	0	0	7
		(%)	42.9	0.0	14.3	0.0	42.9	0.0	0.0	0.0	0.0	100.0
	고졸 이하	빈도	116	60	67	23	69	7	1	8	5	356
		(%)	32.6	16.9	18.8	6.5	19.4	2.0	0.3	2.2	1.4	100.0
	대졸 이하	빈도	164	136	108	38	139	16	9	20	15	645
		(%)	25.4	21.1	16.7	5.9	21.6	2.5	1.4	3.1	2.3	100.0
	대학원생 이상	빈도	9	1	5	1	9	0	1	1	1	28
		(%)	32.1	3.6	17.9	3.6	32.1	0.0	3.6	3.6	3.6	100.0

문7-1. 해당 카드회사 사이트에 가입하실 때, 개인정보를 몇 개의 회사와 공유하는 지에 대해 안내를 받으셨습니까?

		받았다	받지 못했다	Total
카드사 A	빈도	44	250	294
	(%)	15.0	85.0	100.0
카드사 B	빈도	28	170	198
	(%)	14.1	85.9	100.0
카드사 C	빈도	32	149	181
	(%)	17.7	82.3	100.0
카드사 D	빈도	2	60	62
	(%)	3.2	96.8	100.0
카드사 E	빈도	24	197	221
	(%)	10.9	89.1	100.0
카드사 F	빈도	1	22	23
	(%)	4.3	95.7	100.0
카드사 G	빈도	4	8	12
	(%)	33.3	66.7	100.0
카드사 H	빈도	1	28	29
	(%)	3.4	96.6	100.0
카드사 I	빈도	4	18	22
	(%)	18.2	81.8	100.0
Total	빈도	140	902	1042
	(%)	13.4	86.6	100.0

문7-2. 선택한 카드사가 몇 개의 다른 회사와 개인정보를 공유하는 지 알고 계십니까?

		알고 있다	모르고 있다	Total
카드사 A	빈도	29	265	294
	(%)	9.9	90.1	100.0
카드사 B	빈도	18	180	198
	(%)	9.1	90.9	100.0
카드사 C	빈도	27	154	181
	(%)	14.9	85.1	100.0
카드사 D	빈도	3	59	62
	(%)	4.8	95.2	100.0
카드사 E	빈도	17	204	221
	(%)	7.7	92.3	100.0
카드사 F	빈도	0	23	23
	(%)	0.0	100.0	100.0
카드사 G	빈도	4	8	12
	(%)	33.3	66.7	100.0
카드사 H	빈도	1	28	29
	(%)	3.4	96.6	100.0
카드사 I	빈도	2	20	22
	(%)	9.1	90.9	100.0
Total	빈도	101	941	1042
	(%)	9.7	90.3	100.0

문8. 개인정보 관련 불만이나 질문을 전화를 통해 사이트 운영자 혹은 개인정보 관리 책임자에게 제기한 적이 있습니까?

			없다	있다	Total
Total		빈도	921	121	1042
		(%)	88.4	11.6	100.0
연령별	10대	빈도	7	2	9
		(%)	77.8	22.2	100.0
	20대	빈도	315	45	360
		(%)	87.5	12.5	100.0
	30대	빈도	446	53	499
		(%)	89.4	10.6	100.0
	40대	빈도	96	16	112
		(%)	85.7	14.3	100.0
	50대 이상	빈도	57	5	62
		(%)	91.9	8.1	100.0
성별	남	빈도	466	70	536
		(%)	86.9	13.1	100.0
	여	빈도	455	51	506
		(%)	89.9	10.1	100.0
학력별	초등졸 이하	빈도	5	1	6
		(%)	83.3	16.7	100.0
	중졸 이하	빈도	6	1	7
		(%)	85.7	14.3	100.0
	고졸 이하	빈도	315	41	356
		(%)	88.5	11.5	100.0
	대졸 이하	빈도	569	76	645
		(%)	88.2	11.8	100.0
	대학원생 이상	빈도	26	2	28
		(%)	92.9	7.1	100.0

문8-1. 개인정보 관리 책임자가 전화를 받은 경우는 몇 % 정도입니까?

			0%(한번도 전화를 받지 않음)	0% 이상 ~25% 미만	25% 이상 ~50% 미만	50% 이상 ~75% 미만	75% 이상 ~100% 미만	100%(모두 전화를 받음)	Total
Total		빈도	37	42	15	14	4	9	121
		(%)	30.6	34.7	12.4	11.6	3.3	7.4	100.0
연령별	10대	빈도	1	0	1	0	0	0	2
		(%)	50.0	0.0	50.0	0.0	0.0	0.0	100.0
	20대	빈도	10	17	4	8	2	4	45
		(%)	22.2	37.8	8.9	17.8	4.4	8.9	100.0
	30대	빈도	20	17	6	4	1	5	53
		(%)	37.7	32.1	11.3	7.5	1.9	9.4	100.0
	40대	빈도	5	6	3	2	0	0	16
		(%)	31.3	37.5	18.8	12.5	0.0	0.0	100.0
	50대 이상	빈도	1	2	1	0	1	0	5
		(%)	20.0	40.0	20.0	0.0	20.0	0.0	100.0
성별	남	빈도	23	21	9	9	3	5	70
		(%)	32.9	30.0	12.9	12.9	4.3	7.1	100.0
	여	빈도	14	21	6	5	1	4	51
		(%)	27.5	41.2	11.8	9.8	2.0	7.8	100.0
학력별	초등졸 이하	빈도	0	0	1	0	0	0	1
		(%)	0.0	0.0	100.0	0.0	0.0	0.0	100.0
	중졸 이하	빈도	0	1	0	0	0	0	1
		(%)	0.0	100.0	0.0	0.0	0.0	0.0	100.0
	고졸 이하	빈도	16	14	5	5	0	1	41
		(%)	39.0	34.1	12.2	12.2	0.0	2.4	100.0
	대졸 이하	빈도	20	27	8	9	4	8	76
		(%)	26.3	35.5	10.5	11.8	5.3	10.5	100.0
	대학원생 이상	빈도	1	0	1	0	0	0	2
		(%)	50.0	0.0	50.0	0.0	0.0	0.0	100.0

문8-2. 문제 해결에 얼마나 도움이 되었습니까?

			전혀 도움이 되지 않음	별로 도움이 되지 않음	그저 그렇다	약간 도움이 됨	매우 도움이 됨	Total	평균
Total		빈도	37	42	15	22	5	121	2.31
		(%)	30.6	34.7	12.4	18.2	4.1	100.0	
연령별	10대	빈도	1	0	1	0	0	2	2.00
		(%)	50.0	0.0	50.0	0.0	0.0	100.0	
	20대	빈도	10	15	7	13	0	45	2.51
		(%)	22.2	33.3	15.6	28.9	0.0	100.0	
	30대	빈도	19	21	4	6	3	53	2.11
		(%)	35.8	39.6	7.5	11.3	5.7	100.0	
	40대	빈도	5	4	3	2	2	16	2.50
		(%)	31.3	25.0	18.8	12.5	12.5	100.0	
	50대 이상	빈도	2	2	0	1	0	5	2.00
		(%)	40.0	40.0	0.0	20.0	0.0	100.0	
성별	남	빈도	20	22	8	17	3	70	2.44
		(%)	28.6	31.4	11.4	24.3	4.3	100.0	
	여	빈도	17	20	7	5	2	51	2.12
		(%)	33.3	39.2	13.7	9.8	3.9	100.0	
학력별	초등졸 이하	빈도	1	0	0	0	0	1	1.00
		(%)	100.0	0.0	0.0	0.0	0.0	100.0	
	중졸 이하	빈도	0	1	0	0	0	1	2.00
		(%)	0.0	100.0	0.0	0.0	0.0	100.0	
	고졸 이하	빈도	14	12	8	6	1	41	2.22
		(%)	34.1	29.3	19.5	14.6	2.4	100.0	
	대졸 이하	빈도	20	29	7	16	4	76	2.41
		(%)	26.3	38.2	9.2	21.1	5.3	100.0	
	대학원생 이상	빈도	2	0	0	0	0	2	1.00
		(%)	100.0	0.0	0.0	0.0	0.0	100.0	

문9. 개인정보 관련 불만이나 문의를 처리하기 위해, 사이트운영자나 개인정보 관리 책임자에게 e-mail을 보낸 적이 있습니까?

			없다	있다	Total
Total		빈도	889	153	1042
		(%)	85.3	14.7	100.0
연령별	10대	빈도	8	1	9
		(%)	88.9	11.1	100.0
	20대	빈도	287	73	360
		(%)	79.7	20.3	100.0
	30대	빈도	448	51	499
		(%)	89.8	10.2	100.0
	40대	빈도	90	22	112
		(%)	80.4	19.6	100.0
	50대 이상	빈도	56	6	62
		(%)	90.3	9.7	100.0
성별	남	빈도	461	75	536
		(%)	86.0	14.0	100.0
	여	빈도	428	78	506
		(%)	84.6	15.4	100.0
학력별	초등졸 이하	빈도	6	0	6
		(%)	100.0	0.0	100.0
	중졸 이하	빈도	6	1	7
		(%)	85.7	14.3	100.0
	고졸 이하	빈도	299	57	356
		(%)	84.0	16.0	100.0
	대졸 이하	빈도	552	93	645
		(%)	85.6	14.4	100.0
	대학원생 이상	빈도	26	2	28
		(%)	92.9	7.1	100.0

문9-1. 개인정보 관리 책임자로부터 e-mail 회신을 받은 경우는 몇 % 정도입니까?

			0%(한번도 회신을 받지 못함)	0% 이상 ~25% 미만	25% 이상 ~50% 미만	50% 이상 ~75% 미만	75% 이상 ~100% 미만	100%(모두 회신을 받음)	Total
Total		빈도	17	46	18	30	12	30	153
		(%)	11.1	30.1	11.8	19.6	7.8	19.6	100.0
연령별	10대	빈도	0	1	0	0	0	0	1
		(%)	0.0	100.0	0.0	0.0	0.0	0.0	100.0
	20대	빈도	7	21	8	14	6	17	73
		(%)	9.6	28.8	11.0	19.2	8.2	23.3	100.0
	30대	빈도	6	15	5	9	6	10	51
		(%)	11.8	29.4	9.8	17.6	11.8	19.6	100.0
	40대	빈도	3	7	5	4	0	3	22
		(%)	13.6	31.8	22.7	18.2	0.0	13.6	100.0
	50대 이상	빈도	1	2	0	3	0	0	6
		(%)	16.7	33.3	0.0	50.0	0.0	0.0	100.0
성별	남	빈도	9	17	10	21	3	15	75
		(%)	12.0	22.7	13.3	28.0	4.0	20.0	100.0
	여	빈도	8	29	8	9	9	15	78
		(%)	10.3	37.2	10.3	11.5	11.5	19.2	100.0
학력별	중졸 이하	빈도	0	1	0	0	0	0	1
		(%)	0.0	100.0	0.0	0.0	0.0	0.0	100.0
	고졸 이하	빈도	8	20	5	10	2	12	57
		(%)	14.0	35.1	8.8	17.5	3.5	21.1	100.0
	대졸 이하	빈도	9	23	13	20	10	18	93
		(%)	9.7	24.7	14.0	21.5	10.8	19.4	100.0
	대학원생 이상	빈도	0	2	0	0	0	0	2
		(%)	0.0	100.0	0.0	0.0	0.0	0.0	100.0

문9-2. e-mail 회신이 문제 해결에 얼마나 도움이 되었습니까?

			전혀 도움이 되지 않음	별로 도움이 되지 않음	그러 그렇다	약간 도움이 됨	매우 도움이 됨	Total	평균
Total		빈도	25	49	22	46	11	153	2.80
		(%)	16.3	32.0	14.4	30.1	7.2	100.0	
연령별	10대	빈도	0	0	0	1	0	1	4.00
		(%)	0.0	0.0	0.0	100.0	0.0	100.0	
	20대	빈도	13	24	13	18	5	73	2.70
		(%)	17.8	32.9	17.8	24.7	6.8	100.0	
	30대	빈도	7	18	4	17	5	51	2.90
		(%)	13.7	35.3	7.8	33.3	9.8	100.0	
	40대	빈도	5	4	5	8	0	22	2.73
		(%)	22.7	18.2	22.7	36.4	0.0	100.0	
	50대 이상	빈도	0	3	0	2	1	6	3.17
		(%)	0.0	50.0	0.0	33.3	16.7	100.0	
성별	남	빈도	14	24	10	21	6	75	2.75
		(%)	18.7	32.0	13.3	28.0	8.0	100.0	
	여	빈도	11	25	12	25	5	78	2.85
		(%)	14.1	32.1	15.4	32.1	6.4	100.0	
학력별	중졸 이하	빈도	0	1	0	0	0	1	2.00
		(%)	0.0	100.0	0.0	0.0	0.0	100.0	
	고졸 이하	빈도	9	15	10	19	4	57	2.89
		(%)	15.8	26.3	17.5	33.3	7.0	100.0	
	대졸 이하	빈도	16	32	11	27	7	93	2.75
		(%)	17.2	34.4	11.8	29.0	7.5	100.0	
	대학원생 이상	빈도	0	1	1	0	0	2	2.50
		(%)	0.0	50.0	50.0	0.0	0.0	100.0	

문10. 개인정보 관련 불만이나 문의를 처리하기 위해 사이트 게시판에 글을 올린 적이 있습니까?

			없다	있다	Total
Total		빈도	902	140	1042
		(%)	86.6	13.4	100.0
연령별	10대	빈도	7	2	9
		(%)	77.8	22.2	100.0
	20대	빈도	295	65	360
		(%)	81.9	18.1	100.0
	30대	빈도	451	48	499
		(%)	90.4	9.6	100.0
	40대	빈도	91	21	112
		(%)	81.3	18.8	100.0
	50대 이상	빈도	58	4	62
		(%)	93.5	6.5	100.0
성별	남	빈도	463	73	536
		(%)	86.4	13.6	100.0
	여	빈도	439	67	506
		(%)	86.8	13.2	100.0
학력별	초등졸 이하	빈도	6	0	6
		(%)	100.0	0.0	100.0
	중졸 이하	빈도	5	2	7
		(%)	71.4	28.6	100.0
	고졸 이하	빈도	308	48	356
		(%)	86.5	13.5	100.0
	대졸 이하	빈도	558	87	645
		(%)	86.5	13.5	100.0
	대학원생 이상	빈도	25	3	28
		(%)	89.3	10.7	100.0

문10-1. 개인정보 관리 책임자가 답변을 한 경우는 몇 % 정도입니까?

			0%(한번도 답변을 받지 못함)	0% 이상 ~25% 미만	25% 이상 ~50% 미만	50% 이상 ~75% 미만	75% 이상 ~100% 미만	100%(모두 답변을 받음)	Total
Total		빈도	21	41	16	31	16	15	140
		(%)	15.0	29.3	11.4	22.1	11.4	10.7	100.0
연령별	10대	빈도	0	1	0	1	0	0	2
		(%)	0.0	50.0	0.0	50.0	0.0	0.0	100.0
	20대	빈도	8	14	8	16	10	9	65
		(%)	12.3	21.5	12.3	24.6	15.4	13.8	100.0
	30대	빈도	8	15	6	11	4	4	48
		(%)	16.7	31.3	12.5	22.9	8.3	8.3	100.0
	40대	빈도	5	8	2	3	2	1	21
		(%)	23.8	38.1	9.5	14.3	9.5	4.8	100.0
	50대 이상	빈도	0	3	0	0	0	1	4
		(%)	0.0	75.0	0.0	0.0	0.0	25.0	100.0
성별	남	빈도	15	19	7	19	6	7	73
		(%)	20.5	26.0	9.6	26.0	8.2	9.6	100.0
	여	빈도	6	22	9	12	10	8	67
		(%)	9.0	32.8	13.4	17.9	14.9	11.9	100.0
학력별	중졸 이하	빈도	0	1	0	1	0	0	2
		(%)	0.0	50.0	0.0	50.0	0.0	0.0	100.0
	고졸 이하	빈도	5	13	6	13	5	6	48
		(%)	10.4	27.1	12.5	27.1	10.4	12.5	100.0
	대졸 이하	빈도	14	26	10	17	11	9	87
		(%)	16.1	29.9	11.5	19.5	12.6	10.3	100.0
	대학원생 이상	빈도	2	1	0	0	0	0	3
		(%)	66.7	33.3	0.0	0.0	0.0	0.0	100.0

문10-2. 답변이 문제 해결에 얼마나 도움이 되었습니까?

			전혀 도움이 되지 않음	별로 도움이 되지 않음	그저 그렇다	약간 도움이 됨	매우 도움이 됨	Total	평균
Total		빈도	29	45	21	39	6	140	2.63
		(%)	20.7	32.1	15.0	27.9	4.3	100.0	
연령별	10대	빈도	0	0	0	1	1	2	4.50
		(%)	0.0	0.0	0.0	50.0	50.0	100.0	
	20대	빈도	12	18	13	22	0	65	2.69
		(%)	18.5	27.7	20.0	33.8	0.0	100.0	
	30대	빈도	11	18	4	12	3	48	2.54
		(%)	22.9	37.5	8.3	25.0	6.3	100.0	
	40대	빈도	6	7	4	3	1	21	2.33
		(%)	28.6	33.3	19.0	14.3	4.8	100.0	
	50대 이상	빈도	0	2	0	1	1	4	3.25
		(%)	0.0	50.0	0.0	25.0	25.0	100.0	
성별	남	빈도	16	27	9	16	5	73	2.55
		(%)	21.9	37.0	12.3	21.9	6.8	100.0	
	여	빈도	13	18	12	23	1	67	2.72
		(%)	19.4	26.9	17.9	34.3	1.5	100.0	
학력별	중졸 이하	빈도	0	1	0	0	1	2	3.50
		(%)	0.0	50.0	0.0	0.0	50.0	100.0	
	고졸 이하	빈도	11	12	6	17	2	48	2.73
		(%)	22.9	25.0	12.5	35.4	4.2	100.0	
	대졸 이하	빈도	15	32	15	22	3	87	2.61
		(%)	17.2	36.8	17.2	25.3	3.4	100.0	
	대학원생 이상	빈도	3	0	0	0	0	3	1.00
		(%)	100.0	0.0	0.0	0.0	0.0	100.0	

문11. 인터넷 사이트에 회원 가입을 할 때, 여러 가지 개인정보를 입력해야 합니다. 다음 개인 정보 중 입력이 가장 꺼려지는 정보는 어떤 정보입니까?

			이름	주민등록번호	전화번호	핸드폰 번호	e-mail 주소	직장	학교	주소	기타	Total
Total		빈도	46	781	47	85	29	20	9	21	4	1042
		(%)	4.4	75.0	4.5	8.2	2.8	1.9	0.9	2.0	0.4	100.0
연령별	10대	빈도	1	8	0	0	0	0	0	0	0	9
		(%)	11.1	88.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
	20대	빈도	18	261	17	29	8	11	2	11	3	360
		(%)	5.0	72.5	4.7	8.1	2.2	3.1	0.6	3.1	0.8	100.0
	30대	빈도	24	372	24	39	18	6	7	8	1	499
		(%)	4.8	74.5	4.8	7.8	3.6	1.2	1.4	1.6	0.2	100.0
	40대	빈도	3	87	6	11	2	2	0	1	0	112
		(%)	2.7	77.7	5.4	9.8	1.8	1.8	0.0	0.9	0.0	100.0
	50대 이상	빈도	0	53	0	6	1	1	0	1	0	62
		(%)	0.0	85.5	0.0	9.7	1.6	1.6	0.0	1.6	0.0	100.0
성별	남	빈도	31	381	24	44	21	14	9	11	1	536
		(%)	5.8	71.1	4.5	8.2	3.9	2.6	1.7	2.1	0.2	100.0
	여	빈도	15	400	23	41	8	6	0	10	3	506
		(%)	3.0	79.1	4.5	8.1	1.6	1.2	0.0	2.0	0.6	100.0
학력별	초등졸 이하	빈도	0	5	0	1	0	0	0	0	0	6
		(%)	0.0	83.3	0.0	16.7	0.0	0.0	0.0	0.0		100.0
	중졸 이하	빈도	1	5	0	1	0	0	0	0	0	7
		(%)	14.3	71.4	0.0	14.3	0.0	0.0	0.0	0.0	0.0	100.0
	고졸 이하	빈도	20	263	19	24	9	8	3	7	3	356
		(%)	5.6	73.9	5.3	6.7	2.5	2.2	0.8	2.0	0.8	100.0
	대졸 이하	빈도	24	489	27	55	19	12	5	13	1	645
		(%)	3.7	75.8	4.2	8.5	2.9	1.9	0.8	2.0	0.2	100.0
	대학원생 이상	빈도	1	19	1	4	1	0	1	1	0	28
		(%)	3.6	67.9	3.6	14.3	3.6	0.0	3.6	3.6	0.0	100.0

문12. 회원 가입 시 주민등록 번호를 요구하고 있습니다. 기업들이 회원 가입 시 주민등록 번호를 요구하는 것에 대해 어떻게 생각하십니까?

			유출되지 않는다는 것만 보장된다면 수집해도 좋다	유출되지 않는다는 보장이 있다 하더라도 실명 확인이 필요한 경우에만 수집해야한다	실명확인이 필요하다 하더라도 대체할 만한 방법이 있는한 수집하지 않아야 한다	Total
Total		빈도	163	447	432	1042
		(%)	15.6	42.9	41.5	100.0
연령별	10대	빈도	1	4	4	9
		(%)	11.1	44.4	44.4	100.0
	20대	빈도	60	155	145	360
		(%)	16.7	43.1	40.3	100.0
	30대	빈도	76	212	211	499
		(%)	15.2	42.5	42.3	100.0
	40대	빈도	18	48	46	112
		(%)	16.1	42.9	41.1	100.0
	50대 이상	빈도	8	28	26	62
		(%)	12.9	45.2	41.9	100.0
성별	남	빈도	100	230	206	536
		(%)	18.7	42.9	38.4	100.0
	여	빈도	63	217	226	506
		(%)	12.5	42.9	44.7	100.0
학력별	초등졸 이하	빈도	0	4	2	6
		(%)	0.0	66.7	33.3	100.0
	중졸 이하	빈도	1	3	3	7
		(%)	14.3	42.9	42.9	100.0
	고졸 이하	빈도	58	148	150	356
		(%)	16.3	41.6	42.1	100.0
	대졸 이하	빈도	101	279	265	645
		(%)	15.7	43.3	41.1	100.0
	대학원생 이상	빈도	3	13	12	28
		(%)	10.7	46.4	42.9	100.0

문13. 주민등록번호가 도용되어 회원 가입에 실패한 경험이 있습니까?

			없다	1회	2~4회	5~9회	10회 이상	Total
Total		빈도	765	133	119	12	13	1042
		(%)	73.4	12.8	11.4	1.2	1.2	100.0
연령별	10대	빈도	7	1	1	0	0	9
		(%)	77.8	11.1	11.1	0.0	0.0	100.0
	20대	빈도	233	61	49	8	9	360
		(%)	64.7	16.9	13.6	2.2	2.5	100.0
	30대	빈도	385	56	51	3	4	499
		(%)	77.2	11.2	10.2	0.6	0.8	100.0
	40대	빈도	84	12	15	1	0	112
		(%)	75.0	10.7	13.4	0.9	0.0	100.0
	50대 이상	빈도	56	3	3	0	0	62
		(%)	90.3	4.8	4.8	0.0	0.0	100.0
성별	남	빈도	379	74	65	7	11	536
		(%)	70.7	13.8	12.1	1.3	2.1	100.0
	여	빈도	386	59	54	5	2	506
		(%)	76.3	11.7	10.7	1.0	0.4	100.0
학력별	초등졸 이하	빈도	6	0	0	0	0	6
		(%)	100.0	0.0	0.0	0.0	0.0	100.0
	중졸 이하	빈도	6	1	0	0	0	7
		(%)	85.7	14.3	0.0	0.0	0.0	100.0
	고졸 이하	빈도	268	44	39	2	3	356
		(%)	75.3	12.4	11.0	0.6	0.8	100.0
	대졸 이하	빈도	465	85	76	10	9	645
		(%)	72.1	13.2	11.8	1.6	1.4	100.0
	대학원생 이상	빈도	20	3	4	0	1	28
		(%)	71.4	10.7	14.3	0.0	3.6	100.0

문14. 가입한적이 없는 회사로부터 스팸메일을 받는 경우가 몇회 정도입니까?

			1일 20건 이상	1일 10건~1일 20건 미만	1일 2건~1일 10건 미만	주3건 이상~1일 2건 미만	주1건~주3건 미만	없다	Total
Total		빈도	233	238	294	98	115	64	1042
		(%)	22.4	22.8	28.2	9.4	11.0	6.1	100.0
연령별	10대	빈도	4	1	1	1	0	2	9
		(%)	44.4	11.1	11.1	11.1	0.0	22.2	100.0
	20대	빈도	98	104	82	29	32	15	360
		(%)	27.2	28.9	22.8	8.1	8.9	4.2	100.0
	30대	빈도	102	103	151	50	53	40	499
		(%)	20.4	20.6	30.3	10.0	10.6	8.0	100.0
	40대	빈도	20	21	43	8	15	5	112
		(%)	17.9	18.8	38.4	7.1	13.4	4.5	100.0
	50대 이상	빈도	9	9	17	10	15	2	62
		(%)	14.5	14.5	27.4	16.1	24.2	3.2	100.0
성별	남	빈도	129	127	151	48	47	34	536
		(%)	24.1	23.7	28.2	9.0	8.8	6.3	100.0
	여	빈도	104	111	143	50	68	30	506
		(%)	20.6	21.9	28.3	9.9	13.4	5.9	100.0
학력별	초등졸 이하	빈도	2	0	0	1	3	0	6
		(%)	33.3	0.0	0.0	16.7	50.0	0.0	100.0
	중졸 이하	빈도	1	2	1	1	1	1	7
		(%)	14.3	28.6	14.3	14.3	14.3	14.3	100.0
	고졸 이하	빈도	78	66	103	38	41	30	356
		(%)	21.9	18.5	28.9	10.7	11.5	8.4	100.0
	대졸 이하	빈도	144	166	179	57	69	30	645
		(%)	22.3	25.7	27.8	8.8	10.7	4.7	100.0
	대학원생 이상	빈도	8	4	11	1	1	3	28
		(%)	28.6	14.3	39.3	3.6	3.6	10.7	100.0

문14-1. 원치 않는 메일을 받았을 경우 어떻게 대처하십니까?

			읽지 않고 삭제한다	발신자에게 수신거부 신청을 한다	발신자 메일 주소를 내 메일 프로그램의 차단목록에 올려 놓는다	Total
Total		빈도	839	99	104	1042
		(%)	80.5	9.5	10.0	100.0
연령별	10대	빈도	6	1	2	9
		(%)	66.7	11.1	22.2	100.0
	20대	빈도	281	40	39	360
		(%)	78.1	11.1	10.8	100.0
	30대	빈도	413	45	41	499
		(%)	82.8	9.0	8.2	100.0
	40대	빈도	84	12	16	112
		(%)	75.0	10.7	14.3	100.0
	50대 이상	빈도	55	1	6	62
		(%)	88.7	1.6	9.7	100.0
성별	남	빈도	430	57	49	536
		(%)	80.2	10.6	9.1	100.0
	여	빈도	409	42	55	506
		(%)	80.8	8.3	10.9	100.0
학력별	초등졸 이하	빈도	5	0	1	6
		(%)	83.3	0.0	16.7	100.0
	중졸 이하	빈도	6	0	1	7
		(%)	85.7	0.0	14.3	100.0
	고졸 이하	빈도	297	21	38	356
		(%)	83.4	5.9	10.7	100.0
	대졸 이하	빈도	506	78	61	645
		(%)	78.4	12.1	9.5	100.0
	대학원생 이상	빈도	25	0	3	28
		(%)	89.3	0.0	10.7	100.0

문14-2. 수신거부 신청의 효과가 어느 정도입니까?

			수신거부 신청이 비교적 잘 받아들여지는 편이다	여러 차례 수신거부 신청을 해야한 받아들여진다	아무리 수신거부 신청을 하더라도 계속 메일이 온다	수신거부 신청을 하고 나서 오히려 다른 스팸메일들이 더 늘어났다	Total
Total		빈도	24	36	37	2	99
		(%)	24.2	36.4	37.4	2.0	100.0
연령별	10대	빈도	1	0	0	0	1
		(%)	100.0	0.0	0.0	0.0	100.0
	20대	빈도	8	13	18	1	40
		(%)	20.0	32.5	45.0	2.5	100.0
	30대	빈도	12	16	16	1	45
		(%)	26.7	35.6	35.6	2.2	100.0
	40대	빈도	2	7	3	0	12
		(%)	16.7	58.3	25.0	0.0	100.0
	50대 이상	빈도	1	0	0	0	1
		(%)	100.0	0.0	0.0	0.0	100.0
성별	남	빈도	15	22	18	2	57
		(%)	26.3	38.6	31.6	3.5	100.0
	여	빈도	9	14	19	0	42
		(%)	21.4	33.3	45.2	0.0	100.0
학력별	고졸 이하	빈도	5	8	8	0	21
		(%)	23.8	38.1	38.1	0.0	100.0
	대졸 이하	빈도	19	28	29	2	78
		(%)	24.4	35.9	37.2	2.6	100.0

문15. 회원 탈퇴 시 신분증 사본이나 주민등록증을 제출할 것을 요구하는 사이트를 만난 적이 있습니까?

			없다	1개 사이트	2~4개	5~10개	11개 이상	Total
Total		빈도	820	136	67	15	4	1042
		(%)	78.7	13.1	6.4	1.4	0.4	100.0
연령별	10대	빈도	8	1	0	0	0	9
		(%)	88.9	11.1	0.0	0.0	0.0	100.0
	20대	빈도	276	49	26	8	1	360
		(%)	76.7	13.6	7.2	2.2	0.3	100.0
	30대	빈도	389	73	28	6	3	499
		(%)	78.0	14.6	5.6	1.2	0.6	100.0
	40대	빈도	90	8	13	1	0	112
		(%)	80.4	7.1	11.6	0.9	0.0	100.0
	50대 이상	빈도	57	5	0	0	0	62
		(%)	91.9	8.1	0.0	0.0	0.0	100.0
성별	남	빈도	405	78	42	9	2	536
		(%)	75.6	14.6	7.8	1.7	0.4	100.0
	여	빈도	415	58	25	6	2	506
		(%)	82.0	11.5	4.9	1.2	0.4	100.0
학력별	초등졸 이하	빈도	5	1	0	0	0	6
		(%)	83.3	16.7	0.0	0.0	0.0	100.0
	중졸 이하	빈도	5	2	0	0	0	7
		(%)	71.4	28.6	0.0	0.0	0.0	100.0
	고졸 이하	빈도	287	46	20	2	1	356
		(%)	80.6	12.9	5.6	0.6	0.3	100.0
	대졸 이하	빈도	498	85	47	13	2	645
		(%)	77.2	13.2	7.3	2.0	0.3	100.0
	대학원생 이상	빈도	25	2	0	0	1	28
		(%)	89.3	7.1	0.0	0.0	3.6	100.0