준 비 서 면

사 건 2016가합680254 손해배상(기)
원 고 1. E
2. F
3. G
위 원고들 소송대리인 법무법인 정통, 담당변호사 정보호

피 고 주식회사 A
서울특별시 서초구 서초중앙로8길 OOO
대표이사
위 피고 소송대리인 법무법인 옳음, 담당변호사 나승소

피고 소송대리인은 이 사건에 관하여 다음과 같이 변론을 준비합니다.

다 음

1. 원고들의 주장요지

예상되는 원고들의 주장 요지는 다음과 같습니다.

가. 피고 주식회사 A(이하 '피고')는 고의 또는 중과실로 이 사건 개인정보를 유출하여 원고들에게 손해를 발생시켰으므로 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법"이라 한다) 제32조 제2항 위반에 해당하여 원고들은 주위적 청구로서 이에 대한 손해배상을 구한다. 원인되는 사실은 다음과 같다.

1) 피고는 개인정보의 유출을 방지할 주의의무를 다 하지 아니하였다.

이 사건 피고는 정보통신서비스 제공자로서 정보통신망법 제28조 및 동법 시행령 제15조에따라 위임된 방송통신위원회 고시 제2015-03호 '개인정보의 기술적·관리적 보호조치 기준'(이하 "방통위고시"라 한다) 제4항 제4조에 의거하여 망분리 의무대상자에 해당하지만, 피고는 망분리 조치를 다 하지 아니하였다. 또한 이 사건 피고는 정보통신망법 제45조의 위임규정인 미래창조과학부고시 제2013-196호 '정보보호조치에 관한 지침'을 위반하였다. 피고회사가 정보보호를 위하여 집행한 예산은 미래창조과학부고시 제2013-196호 '정보보호조치에 관한 지침'(이하 "미래부고시"라 한다) 별표1의 규정과는 달리 정보기술부문 예산의 2%였다. 그리고 실제 피고가 사용하던 솔루션을 활용할 경우 피고는 위 미래부고시 별표1에 규정된 바와 같이 '네트워크 모니터링 도구를 이용하여 백본망, 주요 노드 및 외부망과 연계되는 주요 회선의 트래픽 소통량을 24시간 모니터링'(이하 "트래픽 모니터링"이라 한다)할 수 있음에도, 피고는 이 사건 분석용 DB의 다운로드와 관련하여 트래픽 모니터링을 하지 아니하였다. 이처럼 피고는 기술적 관리적 보호조치를 다 하지 아니하였다. 또한 피고는 충분한 예산

이 확보되었거나 트래픽 모니터링을 사용하였다면 이 사건 침해사고를 충분히 회피할 수 있었다. 그러므로 피고에게는 개인정보 유출에 중대한 과실이 있다.

2) 피고의 개인정보 유출로 인하여 원고들에게 손해가 발생하였다.

원고들은 피고의 개인정보 유출로 인하여 자신의 개인정보가 거래될 수 있다는 불쾌감과 앞으로도 계속적으로 신분도용 등에 따른 추가 피해발생에 대한 불안감 등의 심리적 정신적 고통으로 인한 정신적 손해가 발생하였다.

나. 피고는 이용계약관계에 있는 원고들의 정보를 개인정보유출로부터 보호해야 할 계약상 의무를 지는데, 이러한 이용계약상의 의무위반 행위로 손해가 발생하였으므로 원고들은 예비적 청구로서 채무불이행에 따른 손해배상을 구한다.

다. 피고는 정보통신망법 제4장에 관한 법령상 의무를 지는바, 그 의무이행을 위반하여 그에 따른 손해가 발생하였으므로 원고들은 피고에 대하여 정보통신망법 제32조 제1항 및 제32조의2에 의거하여 손해배상을 구한다. 구체적 법령위반 사실은 다음과 같다.

1) 피고는 위암 환자의 위암 관련 서적 구매내역, 출산자의 유아 용품 구매 내역 등 원고들의 권리 및 이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하였으므로 정보통신망법 제23조 제1항 상의 법령상 의무를 위반하였다.

2) 피고는 위탁업체인 C에 개인정보 취급위탁하는 경우 정보통신망법 제25조제1항에 따라 정보통신망법 제22조에 따른 개인정보의 수집·이용에 대한 동의와 별도로 개인정보 취급위탁에 관한 사항에 관한 동의를 받아야 하는 바, 위 법령상 의무를 위반하였다.

3) 피고는 이 사건 침해사고에 대하여 원인을 제공한 D에 대한 관리, 감독 의무를 다 하지 아니하였으므로, 정보통신망법 제25조 4항 상의 관리감독의무를 위반하였다. 주어진 사실관계에 의하면 피고는 해당 문서 또는 별도의 계약으로 개인정보처리 위탁업체인 C와 위 개인정보의 기술적• 관리적 보호조치에 관한 사항 등 개인정보의 안전한 관리에 관한 특별한 약정을 하지 않았으므로 피고로서는 위 사안 개인정보유출에 대하여 면책될 여지가 없다. 더구나 피고는 보안교육 이외에 C사 직원들의 업무행위를 구체적으로 교육 및 감독하지는 않았다.

4) 피고는 정보통신망법 제27조의3에 따라 침해사고와 관련된 사실을 24시간 이내 이용자에게 통지하고 방통위 또는 한국인터넷진흥원에 통지 및 신고해야 할 의무를 지는데, 해킹사실을 안 지 1주일 후에야 피고가 각 대상자에게 통지 및 신고를 한 바 위 법령상 의무를 위반하였다.

5) 피고는 방통위고시 상의 망분리 의무, 미래부고시 상의 트래픽 모니터링, 예산 확보 의무를 다 하지 못하였는 바 정보통신망법 제28조 상 개인정보 보호조치에 따르는 법령상 의무를 위반하였다.

다. 원고들은 정보통신망법 제32조에 대신하여 정보통신망법 제32조의2에 따라 피고에게 손해배상을 청구한다.

2. 주위적 청구인 정보통신망법 제32조 제2항 위반에 대한 항변

가. 피고의 개인정보 유출에 대한 중과실 여부

원고들은 피고가 개인정보 유출을 방지할 의무가 있음을 근거로, 피고가 방통위고시 상 망분리 의무를 성실히 이행하지 아니하였고, 미래부고시에 따른 트래픽 모니터링 및 일정 비율 이상 예산 지출 의무의 위반이 있으므로, 기술적 관리적 보호조치를 다 하지 않았음을 주장할 것입니다. 그리고 피고가 이 사건 침해사고를 충분히 인식·회피할 수 있었음에도 그렇게 하지 아니하였으므로 개인정보 유출에 대한 과실이 있다고 주장할 것입니다. 하지만 피고가 망분리 조치를 함에 있어 일정한 조치를 취한 점, 그리고 망분리 의무를 제외한 개인정보의 기술적·관리적 보호조치를 다 한 점, 이 사건 해킹의 경위를 고려해볼 때 피고가 해킹사고를 인식하거나 회피할 수는 없었다는 점에서 원고들의 과실이 없고, 있다 하여도 중과실에 이르지는 않는다고 보기 힘듭니다. 아래에서 각각을 검토하겠습니다.

1) 개인정보 유출을 방지할 주의의무의 위반 여부

가) 방통위고시상 망분리 조치 의무를 위반하였는지 여부에 대한 항변

(1) 확인된 사실관계에 따르면 피고는 빅데이터 분석 알고리즘 개발 DB를 개발이 완료되지 않은 관계로 개인정보처리시스템으로 분류하지 않았고, 이에 따라 이에 접속하여 개발을 진행하던 업무용 컴퓨터는 망분리 대상에 해당하지 아니하였습니다. 원고들은 이를 이유로 피고 회사가 망분리 의무를 다 하지 아니하였다고 주장할 것입니다.

그러나 피고 회사 내부 개발실에 있던 업무용 컴퓨터는 내부 방침상 모두 망분리되어 있는 상태였고, C사의 직원들은 계약기간 동안 피고 회사에 상주하며 개발작업을 진행하였습니다. 또한 C사 개발담당자 D에게는 전항에서 작성한 피고의 DB시스템에 접근할 수 있는 망분리된 업무용 컴퓨터가 배정되었습니다. 방통위고시 제4조 제4항에 따른 망분리 의무는 개인정보취급자가 본 정보를 처리하는 "컴퓨터" 등을 물리적 또는 논리적으로 망분리 하여야 한다고 규정하고 있습니다. 피고는 위 조항에 따라 망분리된 컴퓨터를 사용하였는 바, 형식적으로 본 고시 문언에 따르는 망분리 의무를 다 하였다고 보아야 합니다.

한편 피고는 가설사설망(VPN)을 통해 외부로부터의 접속을 막고 D로 하여금 개인정보관리시스템에 접근하게 하도록 한 사실이 있습니다. 방통위고시 제4조는 망분리에 대해 물리적, 논리적으로만 구분할 뿐 망분리 수준 등에 대해 구체적 기준에 대해 제시하고 있지 않으며, VPN을 토대로 한 방식도 기술적·관리적 보호조치 기준에 따른 논리적 망분리에 해당한다는 점을 생각해볼 때 피고는 망분리 조치를 다 하였다고 보아야 합니다.

(2) 기타 방통위고시에 따른 개인정보 보호조치 여부

앞서 살펴본 조치들에 있어 피고의 과실이 인정된다고 하여도 피고는 현저히 그 주의의무를 위반했다고 볼 수는 없습니다. 피고는 방통위고시에 따라 정보통신망법 제28조 제1항에서 요구하는 조치들, 즉 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립・시행, 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치・운영, 접속기록의 위조・변조 방지를 위한 조치, 개인정보를 안전하게 저장・전송할 수 있는 암호화기술 등을 이용한 보안조치, 백신 소프트웨어의 설치・운영 등 컴퓨터바이러스에 의한 침해 방지조치, 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치를 하였습니다. 설령 피고가 기술적・관리적 보호조치 일부를 해태하였다는 것이 인정되는 경우라도 피고가 개인정보 보호에 관한 대부분의 조치를 하였으므로, 현저하게 그 주의의무를 위반한 것으로 볼 수는 없습니다.

나) 미래부고시에 따른 조치 준수 의무에 대한 항변

확인된 사실관계와 같이, 실제 피고가 사용하던 솔루션을 활용할 경우 피고는 트래픽 모니터링을 할 수 있었음에도 피고는 이 사건 분석용 DB의 다운로드와 관련하여 트래픽 모니터링을 하지 아니하였습니다. 한편 또한 피고가 정보보호를 위하여 집행한 예산은 미래부 규정과는 달리 정보기술부문 예산의 2%였습니다. 원고들은 이에 대하여 위 솔루션을 활용했더라면 이 사건 정보유출을 막음으로써 충분한 개인정보보호가 이루어지지 않았다는 주장을 할 것으로 예상됩니다.

(1) 우선 예산에 대한 원고들의 주장에 대해서는, 회사의 규모와 성격에 따라 정보기술부문의 총 예산이 달라 그 적정한 비율을 일괄적으로 규제할 수는 없어 이 예산이 과소하다고 보기는 힘듭니다. 뿐만 아니라 피고는 본사의 정보기술부문 예산의 2%를 편성, 집행하여 법령상 의무인 방통위고시를 모두 준수하였는 바, 피고의 예산은 충분했다고 할 것입니다.

(2) 트래픽 모니터링과 관련하여 원고들은 특정 솔루션을 활용함으로써 정보유출을 막는 것이 가능함에도 이를 제대로 활용하지 아니한 잘못이 있다고 할 것입니다. 그러나 위와 같은 기능을 구현할 수 있다는 것과 그 기능을 구현해야 할 정보통신망 관련 법령상 또는 계약상 의무가 있다는 것은 서로 다른 차원의 문제라고 항변할 수 있습니다. 정보통신망법은 제4장 '개인정보의 보호' 부분에서 제28조를 두어 정보통신서비스 제공자 등의 개인정보 보호를 위한 기술적・관리적 조치를 규정하고 이에 따라 정보통신망법시행령 제15조 및 이 사건 고시를 통하여 개인정보 보호를 위한 구체적인 기술적・관리적 보호조치 기준을 규정하고 있는 바, 정보통신서비스 제공자는 정보통신망 관련 법령상의 기술적・관리적 보호조치를 이행함으로써 개인정보 보호조치를 다했다고 볼 수 있습니다. 판례에 따르면 방통위고시에서 정하고 있는 기술적・관리적 보호조치를 다한 경우, 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 원칙적으로 위반하였다고 볼 수 없다고 보았습니다.(대법원 2015. 2. 12. 선고 2013다43994 판결)

한편 정보통신망법 제45조는 제6장 '정보통신망의 안정성 확보 등' 부분에 규정되어 있고

그 보호조치의 목적이 '정보통신망의 안정성 및 정보의 신뢰성'을 확보하기 위한 것에 있을 뿐만 아니라 정보보호지침을 정하여 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다고만 규정하고 있는 점 등을 미루어볼 때, 피고가 준수해야 할 정보통신망법상의 개인정보 보호를 위한 기술적·관리적 보호조치에 개인정보 처리 시스템에서 대량으로 유출되는 정보를 실시간으로 모니터링 하는 보호조치가 포함되어 있다고 보기는 어렵습니다. (서울고등법원 2015. 3. 20. 선고 2013나20047, 2013나20054(병합), 2013나20061(병합), 2013나20078(병합))

다) 수탁자 C를 관리, 감독할 의무를 위반하였는지 여부에 대한 항변

피고는 개인정보보호법 제28조 및 정보통신망법 제25조 4항에 따라 수탁업자인 C에 대한 관리, 감독 의무가 있는 바, C의 직원 D의 과실로 이 사건 개인정보 유출이 있었고 C와의 보안에 관한 특별한 약정이 없었다는 이유로 원고들에게 정보통신망법 제32조 제2항에 따른 책임을 물을 것으로 보입니다. 그러나 피고는 수탁자인 C에 대하여 보안서약서 징구 및 1회 보안교육을 한 것만으로도 충분한 관리 감독이 이루어졌다고 볼 수 있습니다.

우선 C사가 업무를 수행한 환경의 특수성을 고려해야 합니다. C사의 직원들은 계약기간 동안 피고에 상주하며 개발작업을 진행하였습니다. 그리고 C사 개발담당자 D에게만 피고의 DB시스템에 접근할 수 있는 망분리된 업무용 컴퓨터가 배정되었습니다. 피고 내에서는 방통위고시에 따른 보호조치가 이루어졌다는 점을 고려할 때, 마지막으로 C업체의 개발 과정을 구체적으로 감독하는 것은 개발 과정에서 C와 피고 모두에게 업무 및 비용 상 부담되는 일이었으므로 할 수 없었다고 보아야 합니다.

원고들의 주장대로 방통위고시는 필요한 교육을 정기적으로 하는 것을 의무로 하고 있는데, 이 사건과 같이 3개월에 걸쳐 이루어진 단기의 개발 과정에 있어서 사안과 같이 1회의 보안교육만 해도 충분하다고 할 수 있습니다. 또한 DB에 대한 접근권한이 있는 D를 제외한 나머지에게 보안교육을 강화할 의무가 없었고, 특히 D에 대하여는 동종업무를 수 차례 하면서 전문가로서 보안의 중요성을 충분히 인지하고 있던 자라 할 것이어서 추가적인 교육을 할 필요가 없었다고 할 것입니다.

추가적으로 통상의 개인정보 위탁자에 대한 보안서약서 안에는 수탁자로 하여금 비상업용 프로그램을 설치하지 않는 등의 보안조치를 취해야 할 의무를 부과하고 있습니다. 예를 들자면 수탁자는 사전 승인을 받지 못한 프로그램 및 정보기기는 위탁자의 업무와 관련하여 사용하지 않는다는 내용이 포함되어 있으며, 이를 위반할 시 정보통신망법 위반에 따른 책임 등을 지는 것으로 명시하고 있습니다. 요컨대 D는 피고에 대하여 비상업용 프로그램을 설치하지 않을 의무를 가지고 있음에도 이를 이행하지 않은 것이므로, 피고는 감독 의무를 다 하였다고 보아야 합니다.

2) 피고의 침해사고에 대한 인식 및 회피가능성에 대한 항변

(가) 이 사건 침해사고 해킹의 경위를 살펴보면, 우선 D의 개인용 노트북은 이 사건 해킹의 대상이 된 개인정보 DB에 대해 VPN을 통한 접근 권한이 있었고, D의 개인용 노트북을 백도어 프로그램을 이용하여 해킹하였으며, 해커는 위의 접근 권한을 토대로 개인정보 DB에

접근하여 이뤄졌습니다. 요컨대 D는 기술적 관리적 보호조치 하에서 유효하게 DB에 접근할 수 있는 자였고, 해커는 D로 가장하는 등 고도의 기술을 사용하여 해킹을 시도하였으므로, 망분리 의무를 포함하여 어떠한 기술적·관리적 보호조치를 통해서도 침해사고를 회피하거나 인식할 수는 없었다고 보아야 합니다.

(나) 원고들은 미래부고시에 따라 트래픽 모니터링을 하였더라면 피고가 침해사고를 인식할 수 있었을 것이라고 항변할 것으로 보입니다. 하지만 주어진 사실관계로는 피고가 침입탐지시스템과 솔루션을 통하여 트래픽과 파일전송을 실시간 모니터링하여 이상징후를 탐지할 수 없었으므로 이 사건 침해사고를 인식하거나 회피하였을 것이라고 볼 수 없습니다. 참고로 앞서 본 판례에서는 평소 트래픽에 비하여 이사건 해커가 2GB, 2GB, 6GB 등 세 차례로 나누어 외부로 유출한 파일로 인하여 발생한 트래픽이 이상 징후로 판단하여야 할 정도의 대용량이라고 보기 어렵다고 판시하였습니다. 결론적으로 이 사건에서 트래픽 모니터링을 하였다고 하더라도 단 1회에 불과한 3GB의 파일 유출을 탐지할 수는 없었다고 보아야 할 것입니다.

또한 피고는 동일 예산으로 정보통신망법 제28조에 따른 기술적·관리적 보호조치 기준에 따른 항목을 모두 준수하고 있었습니다. 그러므로 개인정보보호에 책정된 예산이 충분했더라면 이 사건 침해사고를 인식 또는 회피할 수 있었을 것이라고 주장할 수는 없습니다.

나. 손해의 발생여부에 관한 항변

원고들은 피고의 개인정보 유출로 인하여 유출된 자신의 개인정보가 거래되거나 전파되고 있을 수 있다는 불쾌감은 물론 앞으로도 계속적으로 신분도용 등에 따른 추가 피해발생에 대한 불안감 등의 심리적, 정신적 고통으로 인한 정신적 손해가 발생하였다고 주장할 것입니다. 또한 피고에게 기술적, 관리적 보호조치(제28조) 위반으로 인한 과징금이 발생할 것으로 보이는 점, 피고에 의한 침해사고의 규모, 피고의 태도, 피고의 사회적 책임 등의 제반 사정을 미루어 정보통신망법 제32조 제2항에 따른 손해배상을 청구할 것입니다.

그러나 원고에게 어떠한 손해도 발생하지 아니하였으며, 피고는 기술적, 관리적 보호조치를 다 하였을 뿐 아니라 그에 따라 과징금이 없을 것이라는 점, 그리고 피고 역시 정확한 사실관계를 파악하여 침해사고를 이용자에게 통지하고 한국인터넷진흥원 등에 신고하였고 그 결과 해커가 검거되었는바, 피고는 원고에 대하여 본 조항에 따른 손해배상책임이 없다고 할 것입니다.

정신적 손해에 관하여 판례는 개인정보 이용자에게 위자료로 배상할 만한 정신적 손해가 발생하였는지 여부를 판단할 기준으로, "유출된 개인정보의 종류와 성격이 무엇인지, 개인정보의 유출로 정보주체를 식별할 가능성이 발생하였는지, 제3자가 유출된 개인정보를 열람하였는지 또는 제3자의 열람 여부가 밝혀지지 않았다면 제3자의 열람 가능성이 있었거나 앞으로 그 열람 가능성이 있는지, 유출된 개인정보가 어느 범위까지 확산되었는지, 개인정보의 유출로 추가적인 법익침해의 가능성이 발생하였는지, 개인정보를 처리하는 자가 개인정보를 관리해온 실태와 개인정보가 유출된 구체적인 경위는 어떠한지, 개인정보의 유출로 인한 피해의 발생 및 확산을 방지하기 위하여 어떠한 조치가 취하여졌는지 등 여러 사정을 종합적으로 고려하여 구체적 사건에 따라 개별적으로 판단하여야 한다."고 보았습니다. (대법원

2012. 12. 26. 선고 2011다59834,59858,59841 판결)

위 판례 기준에 따라 주어진 사실관계를 살펴보면, 현재 사건 해커가 다운로드 받은 정보는 이미 삭제된 상태입니다. 해커는 정보의 사용 여부, 추가 복제 여부, 공범의 존재, 제3자에 대한 전달 여부에 관하여도 부인하였습니다. 그러므로 이 사건 개인정보는 유출된 흔적도 없고, 다운로드 받은 정보는 이미 삭제되었으며, 비록 해커가 그러한 정보를 열람하였다고 가정하더라도 3GB에 달하는 개인정보를 열람만으로 식별하거나 알아내기는 어려우며, 후속 피해 상황이 발견되지 아니하였습니다. 이와 유사한 사례에서 판례는 원고들의 위자료가 발생하지 아니하였다고 판시한 바 있습니다. (대법원 2012. 12. 26. 선고 2011다59834,59858,59841 판결 참조) 한편 개인정보 유출에 대해 원고들의 위자료 배상을 인용한 대구지방법원 2014. 2. 13. 선고 2012나9865 판결에서의 개인정보는 성명, 주민등록번호, 아이디, 비밀번호, 주소, 전화번호 등과 같이 기본적이면서 보호가 필요한 성격의 정보라 볼 수 있으나, 본 사건에서 유출된 정보는 ID, 성별, 나이, 거주지('동'까지 기재), 최근 3개월간의 구매 내역으로 앞서 살펴본 판례의 보호가 필요한 기본정보와 보호이익 상 차이가 있다 할 것입니다. 그러므로 판례의 태도에 비추어볼 때 , 이 사건 침해사고로 인하여 원고들에게 정신적 손해가 발생하지 아니하였다고 할 수 있습니다.

참고로 미국 판례에서 나타난 손해배상의 요건 상 정신적 고통의 경우 의학적으로 진단된 질병을 앓고 있고 그것이 피고의 과실로 인하여 야기된 것임을 주장, 입증하여야 한다고 손해배상책임을 부인한 바 있습니다. 이는 일반적 손해배상책임의 법리에 따라 개인정보가 위태롭게 되었다는 것만으로는 실제 손해가 발생하지 않았기에 손해배상책임을 부인한 것입니다. 이에 따르면 원고 역시 정신적 손해를 입었다고 하기 위해서는 이에 대한 입증이 필요하지만, 그러한 입증은 불가능합니다.

다. 소결

피고는 본 방통위고시에 따라 기술적·관리적 보호조치 의무를 다 하였습니다. 방통위고시에 따른 망분리 의무에 있어서도, 피고는 업무상 본 고시가 요구하는 "컴퓨터 등"에 대한 망분리 조치를 다 하였는바 과실이 없다고 할 것입니다. 한편 미래부고시에 따른 정보보호조치 지침은 피고의 의무라 할 수 없으며 그러한 의무를 지켰다고 하여도 이 사건 개인정보 유출을 피할 수 있었다고 단정할 수 없습니다. 그러므로 피고에게는 과실조차 인정될 수 없다고 할 것이고, 비록 인정된다고 하여도 나머지 기술적·관리적 보호조치를 다 하였으므로 중과실에는 이르지 아니하였습니다.

마지막으로 원고들에게 개인정보 유출로 인하여 손해가 발생하지 않았으며, 원고들은 개인정보 유출로 인하여 원고들에게 손해가 발생하였다는 사실을 입증할 수 없으므로, 피고는 정보통신망법 제32조 제2항에 따르는 책임을 지지 않습니다.

3. 예비적 청구 중 이용계약상 의무 위반에 관한 항변

원고들은 정보통신망법의 취지 및 개인정보보호법의 조항, 피고의 업무 등을 고려해볼 때 원고들이 피고에게 개인정보를 제공하는 것은 계약상 핵심적인 부분이므로 피고에게는 개인정보에 대한 보호의무 내지 안전의무로서의 계약상 부수의무가 있다고 주장할 것입니다. 그

리고 피고가 개인정보보호에 실패하여 개인정보유출사고가 발생하였으므로 원고들은 피고에 대하여 채무불이행에 따른 손해배상책임을 물을 것으로 보입니다. 이에 대해 피고가 계약상 책임을 지는지 여부에 관해 계약상 의무를 다 하였는지 여부를 판례의 기준에 따라 검토한 후 손해발생사실이 없음을 검토하겠습니다.

가. 피고가 이용계약상 의무를 다 하였는지 여부

1) 계약상 의무를 다 하였는지를 판단하기 위하여 판례에서 제시하는 기준

판례는 정보통신망법 제28조 제1항이나 정보통신서비스 이용계약에 따른 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였는지 여부를 판단함에 있어서 "해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, 정보통신서비스제공자의 업종·영업규모와 정보통신서비스제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피 가능성, 정보통신서비스제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 정보통신서비스제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다."고 보았습니다. 더 나아가 당시 정보통신부 장관 고시였던 「개인정보의 기술적·관리적 보호조치 기준」은 "해킹 등 침해사고 당시의 기술수준 등을 고려하여 정보통신서비스제공자가 구 정보통신망법 제28조 제1항에 따라 준수해야 할 기술적·관리적 보호조치를 구체적으로 규정하고 있으므로, 정보통신서비스제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한, 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다."고 판시하였습니다. (대법원 2015. 2. 12. 선고 2013다43994 판결)

2) 피고가 고시에 따른 개인정보의 기술적・관리적 보호조치를 다 하였는지 여부

정보통신부장관이 마련한 위 판례의 고시는 현재 이 사건 방통위고시로 승계되었으며, 피고는 주위적 청구에서 살펴본 대로 방통위고시를 준수하였습니다. 그러므로 피고는 원고들에 대하여 개인정보 유출에 따른 계약상 책임을 지지 않습니다. 그러나 원고들은 피고가 망분리 의무에 따른 조치를 하지 않은 점을 토대로 방통위고시에 따른 조치를 다 하지 아니하였으므로 피고의 원고에 대한 계약상 의무를 다하지 아니하였다고 항변할 것입니다. 뿐만 아니라, 비록 피고가 방통위고시를 준수하였다고 하더라도 이 사건에서는 피고가 방통위고시 외에 추가적인 보호조치를 취해야하는 특별한 사정이 있다고 항변할 것입니다. 그러나 주위적 청구에서 살펴본 바와 같이 실제 업무상 망분리 조치가 이루어졌으므로, 피고는 망분리 의무를 포함한 방통위고시 사항을 모두 준수하였으므로 계약상 의무를 다 하였다고 할 것입니다.

또한 피고와 유사한 업종, 규모를 지닌 ㈜이베이코리아는 2008년 당시 개인정보유출 사고가 있었는데, 당시 방통위고시에 따른 기술적・관리적 보호조치를 다 하였음을 이유로 계약

상, 법령 상 의무를 다 하였다고 보았습니다. (대법원 2015. 2. 12. 선고 2013다43994 판결) 이에 따르면 피고는 방통위고시에 따른 기술적·관리적 보호조치를 다 하였으므로 계약상 의무를 다 한 것으로 보아야 합니다. 한편 보편적인 정보보안의 기술 수준은 2015년 개정된 방통위고시에 따른 기술적·관리적 보호조치를 토대로 파악될 수 있습니다. 피고는 주위적 청구에서 살펴본 바와 같이 망분리 조치에 있어서 방통위고시에서 요구되는 망분리 조치를 실제 업무 현장에서 수행하였습니다. 또한 피고는 그 외에 2015년 개정된 방통위고시에 따른 기술적·관리적 보호조치를 준수하였습니다. 피고는 예산 내에서 본 조치를 준수하였으므로 정보보안에 충분한 비용을 들였고 그 효용도 충분했다고 볼 것입니다. 그리고 주위적 청구에서 살펴본 바와 같이 피고는 위 해킹사고에 대한 회피 가능성이 없었고, 손해가 발생하지 아니하였고 그 손해 발생이 입증될 수 없으므로, 방통위고시 외의 조치가 고려되어야 할 특별한 사정에 해당한다고 볼 수 없습니다.

원고들은 이에 대하여, 미래부고시를 근거로 충분한 예산이 확보되지 못하였으며 트래픽 모니터링을 제대로 수행하지 아니하였으므로 그 효용도 부족했다고 항변할 것입니다. 그러나 법령 상 의무가 아님에도 트래픽 모니터링에 필요한 솔루션을 갖추고 있었던 점, 방통위고시에 따라 업무상의 망분리 조치를 하였던 점을 고려해볼 때 피고는 정보보안에 필요한 예산이 충분했고 효용도 충분하였다고 보입니다. 요컨대 피고는 기술적·관리적 보호조치를 다 하였으므로 원고들에 대한 계약상 의무를 다 하였다고 할 것입니다.

결론적으로 피고는 방통위고시를 준수하는 것 외에 다른 개인정보 보호조치를 고려해야 할 특별한 사정이 있다고 보기 힘듭니다. 이에 따라 피고는 계약상 의무를 다 하였다고 보아야 합니다.

나. 손해 발생 여부

설령 피고가 원고들에 대하여 손해배상책임을 진다고 하여도, 주위적 청구에서 살펴본 바와 같이, 원고들에게 손해발생의 사실이 없으며, 손해 발생의 입증책임은 피고에게 있으나 원고들은 그 손해를 입증하지 못하는바 원고들에 대하여 배상할 손해가 존재하지 않습니다.

다. 소결

피고는 방통위고시에 따른 의무를 준수하였으므로 판례에 따르면 원고들에 대한 개인정보 유출을 방지할 계약상 의무가 없습니다. 설령 그 의무를 일부 준수하지 아니하였다거나 이 사건 피고에 대하여 특별한 사정이 인정되어 피고에게 원고들에 대한 과실이 있다고 하여도, 원고에 대하여 배상할 손해가 존재하지 않습니다.

4. 예비적 청구 중 정보통신망법 제32조 제1항 위반 및 제32조의2 위반에 대한 항변

원고들은 정보통신망법 제4장의 규정에 해당하는 정보통신망법 상 개인정보의 수집 제한(제23조), 개인정보의 취급위탁(제25조), 개인정보 누출 등의 통지, 신고(제27조의3), 개인정보 보호조치(제28조) 위반을 이유로 피고에 대하여 정보통신망법 제32조 제1항 및 정보통신망법 제32조2에 따라 손해배상을 청구할 것으로 보입니다. 그러나 피고는 기술적·관리적 보

호조치에 관한 법령상 의무를 다 하였으며, 나머지 규정은 정보통신망법 제32조의 손해배상의 요건에 해당하지 아니하고 설령 해당한다고 하여도 그 위반이 없고, 위반이 있다고 하여도 그 과실은 없다고 항변하는 바입니다.

가. 피고의 정보통신망법 제32조상 "이 장의 위반" 여부

1) 개인정보 보호조치에 관한 정보통신망법 제28조의 위반 여부

판례는 정보통신서비스제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한, 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다."고 판시하였습니다. (대법원 2015. 2. 12. 선고 2013다43994 판결) 판례는 기술적·관리적 보호조치를 취하여야 할 계약상 의무 위반 여부와 법령상 의무 위반 여부를 동일한 기준으로 판단하고 있습니다. 앞서 살펴본 것처럼 또한 피고는 방통위고시를 준수하는 것 외에 다른 개인정보 보호조치를 고려해야 할 특별한 사정이 있다고 보기 힘듭니다. 피고는 방통위고시에 따른 의무를 준수하였으므로, 판례에 따르면 원고들에 대한 개인정보 유출을 방지할 법령상 의무를 다 하였습니다.

2) 정보통신망법 제32조 제1항 "이 장의 규정" 중 개인정보 보호조치를 제외한 규정의 위반 여부

원고들은 또한 피고의 정보통신망법 상 개인정보의 수집 제한(제23조), 개인정보의 취급위탁(제25조), 개인정보 누출 등의 통지, 신고(제27조의3) 위반을 이유로 정보통신망법 제32조 제1항 및 제32조의2에 따라 손해배상을 청구할 것으로 보입니다. 그러나 정보통신망법 제32조 제1항 상 "이 장의 위반"에는 위의 규정들을 포함하지는 않는다고 봐야 하며, 그렇지 않다고 하여도 피고가 각각의 법령을 위반한 사실이 없거나 위반이 있어도 과실이 없다고 보아야 합니다. 이에 대하여 검토하겠습니다.

(가) 정보통신망법 상 개인정보의 수집 제한(제23조), 개인정보의 취급위탁(제25조), 개인정보 누출 등의 통지, 신고(제27조의3) 등이 정보통신망법 제32조 제1항 상의 "이 장의 위반"에 해당하는지 여부

정보통신망법 제32조 제1항 상 "이 장의 위반"에는 동법 제28조 개인정보 보호조치 규정 외에 규정은 포함되지 않는다고 봐야 합니다. 의무위반과 개인정보의 누출 사이에는 사실적 인과관계와 규범의 보호목적 관련성이 있어야 하는 바, 개인정보 누출등과 무관한 위 규정은 이러한 관련성을 갖고 있지 않습니다. 누출의 통지·신고는 개인정보가 누출된 이후의 책무로, 확대손해와 관련한 과실 상계는 별론으로 하더라도 책임성립과 사이의 관련성은 인정할 수 없습니다.

(나) 정보통신망법 상 개인정보의 수집 제한(제23조), 개인정보의 취급위탁 시 동의(제25조 제1항), 수탁자에 대한 관리, 감독의무(제25조 제4항) 개인정보 누출 등의 통지, 신고(제27조

의3) 규정 위반 여부

설령 "이 장의 위반"에는 동법 제28조 개인정보 보호조치 규정 외의 위 규정들이 포함된다고 하여도, 각 규정의 위반한 사실이 없거나 위반이 있어도 과실이 없다고 보아야 합니다. 이에 대하여 검토하겠습니다.

(1) 개인정보의 수집 제한(제23조) 위반 여부

피고가 B쇼핑몰을 통해 원고 E가 "위암을 이겨낸 사람들", "위암 수술 후 식사 가이드", "암 치료 후 건강관리 가이드" 등의 서적을 구매하였다는 사실, 원고 F가 아기 출산 후 남아용 기저귀, 젖병세정제, 물티슈 등의 아기용품을 구매하였다는 사실 등 원고의 구매내역을 수집함으로써 병력 및 가족관계 등 사생활을 뚜렷하게 침해할 우려가 있는 정보를 수집하였는 바 정보통신망법 제23조 제1항을 위반하였고, 기타 개인정보를 수집함에 있어서도 최소수집의무를 위반한 바 정보통신망법 제23조 제2항 위반을 주장할 것입니다.

먼저 원고의 정보통신망법 제23조 제2항 위반 주장에 대해서는, 피고가 이 사건 DB를 구축하기 위해 수집한 개인정보의 내용은 원고들의 개인정보인 ID, 성별, 나이, 거주지 ('동'까지 기재) 외에 최근 3개월간의 구매내역 (구매 일시, 구매한 물품명, 물품의 수량 및 가격, 제품 판매자, 상품평)이며, 그러한 정보에 대한 수집은 정보통신서비스 제공자로서 최소한에 그쳤다고 볼 수 있습니다. B 쇼핑몰 운영에 있어서 위 정보의 수집은 필수불가결한 부분이라 할 것이므로 최소수집의무 위반에 해당하지 않습니다. 또한 판례에 따르면 피고가 회원들의 전화번호, 주소, 혈액형 등의 개인정보를 수집하였다고 하더라도, 이러한 사정만으로는 피고가 최소수집의무를 위반하였다고 인정하기 어렵다고 보았습니다. (대전지방법원 2014. 8. 14. 선고 2012가합101743,2012가합102449(병합) 참조).

다음으로 원고의 정보통신망법 제23조 제1항 위반 주장에 대하여, 피고는 원고들의 사생활을 침해하는 개인정보를 수집했다고 볼 수 없습니다. 원고가 주장하는 바와 같이 원고 E가 피고의 B쇼핑몰을 통해 특정 서적 등을 구매하였다는 사실만으로는 원고 E가 위암 수술을 받았다는 정보를 특정할 수 없습니다. 즉 원고 E가 위 책을 구매한 목적이 단순히 의학에 관심이 있기 때문일 수도 있고, 주변인 중에 위암 환자가 있을 수도 있기에 수집된 본 정보가 원고 E의 사생활을 침해한다는 주장은 타당하지 않습니다. 이는 원고 F에 있어서도 역시 마찬가지입니다. F의 유아용품 구매정보만 가지고는 F가 출산을 하였다는 사실을 단정할 수 없습니다. 그러므로 피고가 수집한 정보가 사생활을 뚜렷하게 침해할 우려가 없습니다.

(2) 개인정보의 취급위탁 시 이용자로부터 동의를 받도록 하는 정보통신망법 제25조의 위반 여부

피고는 정보통신망법 상 개인정보의 취급위탁(제25조) 규정에 따라 제3자에게 이용자의 개인정보를 취급위탁하는 경우에는 위탁업무의 내용과 업무수탁자 내용을 이용자에게 알리고 동의를 받아야 하는 바, 이 사건 피고는 해당 고객들로부터 위탁사실에 관한 동의를 얻

은 바 없으므로 원고들은 피고의 본 조항 위반을 주장할 것입니다. 그러나 동조 제2항에서는 업무수탁자와 위탁 업무의 내용을 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다고 규정하고 있으며, 피고는 동법 시행령 제14조 제1항 제1호에 따라 위탁업무의 내용과 업무수탁자를 피고 홈페이지 첫 화면에 연결된 개인정보 처리방침에 공개하였으므로 동조 위반이 없습니다.

(3) 개인정보 취급위탁 시 관리, 감독할 의무(제25조 제4항)를 위반하였는지 여부

피고는 정보통신망법 제25조 제4항에 따라 수탁업자인 C에 대한 관리, 감독 의무가 있는바, 원고들이 피고에게 C의 직원 D의 과실로 이 사건 개인정보 유출이 있었음을 이유로 정보통신망법 제32조에 따른 책임을 물을 것으로 보입니다. 피고는 주위적 청구에서 살펴보았듯이 C의 업무 환경 및 C에 대한 직접적 감독이 어려운 사정 등을 생각해볼 때, 보안서약서 징구 및 C에 대한 1회 보안교육을 한 것만으로 충분히 그 관리감독의무를 다했다고 볼 것입니다.

(4) 개인정보 누출 등의 통지, 신고(제27조의3) 의무 위반 여부

개인정보 누출 등의 통지, 신고(제27조의3)에 관하여 원고들은 피고가 정보통신망법 제27조의3 에 따라 개인정보 유출 관련 사실에 관하여 이용자에 대한 통지 및 방송통신위원회 또는 한국인터넷진흥원에 사실을 안 때부터 24시간 이내에 신고해야 할 의무가 있으며, 그러한 의무를 해태하여 그 사실을 안 지 1주일이 지난 시점에 통지, 신고하였음을 이유로 본 조항 위반을 주장할 것이며 그로 인해 원고에게 손해가 발생하였다고 주장할 것으로 보입니다.

설령 피고가 통지, 신고 의무 위반으로 피고에게 손해배상을 해야 할 의무가 존재한다고 하여도, 피고는 정확한 사실관계를 파악하기 위하여 자체 조사를 하는 도중에 법에서 정한 기간을 도과하여 통지, 신고를 한 것이라고 보아야 합니다. 더구나 이 사건 침해사고의 경위나 그 정도를 살펴볼 때 24시간 이내에 통지될 만큼 중대한 사안도 아니었습니다. 오히려 제대로 된 사실관계 파악 없이 24시간에 통지하였을 경우 이 정보를 알고 해커에게 악의를 가지고 접근한 이들로 인하여 더 큰 손해가 발생할 수 있었던 점 등을 고려해볼 때, 피고의 본 의무 위반에 있어서 정당한 사유가 인정되는바 과실이 없습니다.

나. 손해발생 여부

1) 정보통신망법 제32조 제1항의 경우

주위적 청구에서 살펴본 바와 같이, 이 사건 개인정보 유출로 인하여 원고들에게는 어떠한 손해도 발생하지 아니하였습니다.

2) 정보통신망법 제32조의2의 경우

정보통신망법 제32조의2는 피고의 손해발생 사실의 입증을 요하지 않습니다. 그러나 그 의미는 원고들의 손해배상 증명 책임을 완화한다는 것일 뿐 손해발생 사실 자체가 없음에도 피고가 원고들에 대하여 손해배상을 할 의무를 부담한다는 것은 아닙니다. 정보통신망법 제32조 제1항의 경우와 마찬가지로 이 사건에서 손해발생 자체를 인정할 수 없으므로, 피고는 원고들에 대하여 손해배상책임이 없습니다.

다. 소결

피고는 정보통신망법 상 개인정보의 수집 제한(제23조), 개인정보의 취급위탁 시 동의(제25조 제1항), 수탁자에 대한 관리, 감독의무(제25조 제4항), 개인정보 보호조치(제28조)에 대한 위반 사항이 없으며, 개인정보 누출 등의 통지, 신고(제27조의3)의 위반에 있어서 어떠한 과실도 없습니다. 그러므로 정보통신망법 제32조 제1항 상 "이 장의 규정" 위반을 하지 않았고, 위반을 하였더라도 그러한 위반에 과실이 없습니다. 또한 피고에게는 어떠한 손해도 발생한 바 없습니다. 비록 정보통신망법 제32조의2의 규정이 원고에게 손해발생의 입증 책임을 경감시켜주는 조항이나 손해발생이 없는 경우까지 피고에 대하여 배상책임을 지우는 것이 아닙니다. 그러므로 원고에 대하여 정보통신망법 제32조 제1항에 따른 손해배상책임이 없으며, 그에 대신하여 청구한 정보통신망법 제32조의2에 따른 손해배상책임도 없습니다.

5. 결론

피고는 원고들의 주위적 청구로써 정보통신망법 제32조 제2항 상의 위반이 없으며, 예비적 청구로서 이용계약상 의무위반, 정보통신망법 제32조 제1항 및 제32조의2의 위반이 없습니다. 그에 따라 피고는 원고들에 대하여 이 사건 개인정보유출에 대해 손해배상책임을 지지 않습니다.

2016. 9. 20.

위 피고 주식회사 A 소송대리인 법무법인 옳음,
담당변호사 나승소 (서명 또는 날인)

서울중앙지방법원 민사제22부 귀중