대 법 원

제 1 부

판 결

사 건	2013다43994 손해배상(기) 2013다44003(병합) 손해배상(기)
원고, 상고인	별지 1, 2 원고 명단 기재와 같다. 소송대리인 법무법인 넥스트로 담당변호사 박진식 외 2인
피고, 피상고인	주식회사 이베이옥션의 소송수계인 주식회사 이베이코리아 외 1인 소송대리인 변호사 손지열 외 1인
원 심 판 결	서울고등법원 2013. 5. 2. 선고 2010나31510, 31527(병합) 판결
판 결 선 고	2015. 2. 12.

주 문

상고를 모두 기각한다.

상고비용은 원고들이 부담한다.

이 유

상고이유를 판단한다.

1. 피고 주식회사 이베이옥션의 소송수계인 주식회사 이베이코리아(이하 '피고 옥션'이라 한다)에 대한 손해배상청구에 관하여

가. 1) 구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2008. 2. 29. 법률 제8852호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다) 제28조 제1항은 "정보통신서비스제공자 등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 조치를 하여야 한다."고 규정하고 있다. 그리고 구 정보통신망법 제28조 제1항의 위임을 받은 구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙」(2008. 9. 23. 행정안전부령 제34호로 전부 개정되기 전의 것, 이하 '구 정보통신부령'이라 한다) 제3조의3 제1항은 정보통신서비스제공자가 취하여야 할 개인정보의 안전성 확보에 필요한 기술적·관리적 조치로 '개인정보의 안전한 취급을 위한 내부관리계획의 수립 및 시행(제1호)', '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치·운영(제2호)', '접속기록의 위조·변조 방지를 위한 조치(제3호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)', '백신소프트웨어의 설치·운영 등 컴퓨터바이러스 방지 조치(제5호)', '그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치(제6호)'를 규정하고 있다. 따라서 정보통신서비스제공자는 구 정보통신부령 제3조의3 제1항 각호에서 정하고 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 할 법률상 의무를 부담한다.

나아가 정보통신서비스제공자가 정보통신서비스를 이용하려는 이용자와 정보통신서

비스 이용계약을 체결하면서, 이용자로 하여금 이용약관 등을 통해 개인정보 등 회원정보를 필수적으로 제공하도록 요청하여 이를 수집하였다면, 정보통신서비스제공자는 위와 같이 수집한 이용자의 개인정보 등이 분실·도난·누출·변조 또는 훼손되지 않도록 개인정보 등의 안전성 확보에 필요한 보호조치를 취하여야 할 정보통신서비스 이용계약상의 의무를 부담한다.

2) 그런데 정보통신서비스가 '개방성'을 특징으로 하는 인터넷을 통하여 이루어지고 정보통신서비스제공자가 구축한 네트워크나 시스템 및 그 운영체제 등은 불가피하게 내재적인 취약점을 내포하고 있어서 이른바 '해커' 등의 불법적인 침입행위에 노출될 수밖에 없고, 완벽한 보안을 갖춘다는 것도 기술의 발전 속도나 사회 전체적인 거래비용 등을 고려할 때 기대하기 쉽지 아니한 점, 해커 등은 여러 공격기법을 통해 정보통신서비스제공자가 취하고 있는 보안조치를 우회하거나 무력화하는 방법으로 정보통신서비스제공자의 정보통신망 및 이와 관련된 정보시스템에 침입하고, 해커의 침입행위를 방지하기 위한 보안기술은 해커의 새로운 공격방법에 대하여 사후적으로 대응하여 이를 보완하는 방식으로 이루어지는 것이 일반적인 점 등의 특수한 사정이 있으므로, 정보통신서비스제공자가 구 정보통신망법 제28조 제1항이나 정보통신서비스 이용계약에 따른 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였는지 여부를 판단함에 있어서는 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, 정보통신서비스제공자의 업종·영업규모와 정보통신서비스제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피가능성, 정보통신서비스제공자가 수집한 개인정보의 내용과 개인정보의 누출

로 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.

특히 구 정보통신부령 제3조의3 제2항은 "정보통신부장관은 제1항 각호의 규정에 의한 보호조치의 구체적인 기준을 정하여 고시하여야 한다."고 규정하고 있고, 이에 따라 정보통신부장관이 마련한 「개인정보의 기술적·관리적 보호조치 기준」(정보통신부 고시 제2005-18호 및 제2007-3호, 이하 '이 사건 고시'라 한다)은 해킹 등 침해사고 당시의 기술수준 등을 고려하여 정보통신서비스제공자가 구 정보통신망법 제28조 제1항에 따라 준수해야 할 기술적·관리적 보호조치를 구체적으로 규정하고 있으므로, 정보통신서비스제공자가 이 사건 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.

나. 상고이유 제1점 내지 제8점, 제10점에 관하여

1) 원심판결의 이유 및 기록에 의하면 아래와 같은 사정을 알 수 있다.

가) 원고들은 피고 옥션이 제공하는 상품 중개서비스를 이용하기 위하여 피고 옥션과 서비스 이용계약을 체결하고 피고 옥션의 인터넷 오픈마켓 사이트(이하 '이 사건 사이트'라 한다)에 온라인 회원으로 가입하면서, 피고 옥션의 이용약관 제8조에 따라 피고 옥션에 이름, 주민등록번호, 휴대전화번호, 이메일 주소 등을 제공하였다. 2008. 1. 초경 피고 옥션의 서버에 해킹사고가 발생하였는데, 경찰수사결과에 의하면 위 해킹사고는 중국인 해커로 추정되는 소외인 등이 2008. 1. 3.경 피고 옥션의 웹 서버 중 하나인 이노믹스 서버에 설치된 웹 어플리케이션 서버인 톰캣 서버에 초기설정상태인 아이

디와 비밀번호로 접속하여 위 톰캣 서버의 관리자 페이지에 'job.war'라는 백도어 프로그램을 올렸고, 각종 해킹기법을 통해 이노믹스 서버에 침입하고 이 사건 데이터베이스 서버의 관리자 아이디와 암호화된 비밀번호를 알아낸 다음, 2008. 1. 4.경부터 2008. 1. 8.경까지 네 차례에 걸쳐 이 사건 데이터베이스 서버에 저장되어 있던 회원의 이름, 주민등록번호 등 피고 옥션의 회원정보를 누출한 것으로 추정된다.

나) 한편 피고 옥션은 개인정보 보호 조직의 구성·운영에 관한 사항, 접근 통제 등에 관한 세부 사항, 그 밖에 개인정보 보호를 위하여 필요한 사항 등을 구체적으로 규정한 「정보보호정책 및 관리지침」(이하 '이 사건 관리계획'이라 한다)을 제정하여 임직원으로 하여금 이를 준수하게 하는 등 개인정보 관리계획을 수립·시행하였고, 네트워크에 대한 침입탐지시스템과 침입방지시스템을 설치하여 운영하였으며, 이 사건 관리계획을 통해 패스워드 작성 규칙을 수립·이행하였고, 복수의 백신 소프트웨어를 설치·운영하는 등 개인정보에 대한 불법적인 접근을 통제하기 위하여 구 정보통신망법 제28조 제1항 등에서 요구하고 있는 개인정보 보호를 위한 기술적·관리적 조치를 취하고 있었다.

다) 피고 옥션은 이 사건 해킹사고 당시 회사의 업무 특성상 인터넷을 통해 외부접속이 필요하였던 이노믹스 서버에 대하여 아이디와 비밀번호 입력과 같은 인증 및 인가절차를 시행하고 각종 접근제어 방법을 마련하는 등 다수의 보안조치를 취하였다. 또한, 원고들이 이노믹스 서버 등에 설치가 필요하였다고 주장하는 웹 방화벽은 시스템의 특성 등을 고려하여 도입 여부가 결정되는 선택적인 보안조치의 하나에 불과하고 구 정보통신망법 등 관련 법령상으로도 웹 방화벽의 설치가 의무화되어 있지 않았으므로, 피고 옥션이 원고들이 주장하는 바와 같이 이노믹스 서버 등에 사회통념상 합리적

으로 기대 가능한 정도의 보호조치를 이행하지 않았다고 볼 수 없다.

라) 수백 대의 웹 서버와 수십 대의 데이터베이스 서버를 운영하고 있는 피고 옥션의 시스템 구조 특성상, 피고 옥션이 이노믹스 서버의 웹 서비스를 지원하기 위해 설치된 톰캣 서버의 아이디와 비밀번호 설정 등 개개 항목의 취약점을 전부 파악하여 보완하기가 쉽지 않으므로 스캐너와 같은 자동화된 도구를 통해 취약점을 점검하는 것이 보편적인 보안업무의 처리방식이다. 그런데 톰캣 서버의 아이디와 비밀번호의 취약점은 이 사건 해킹사고 이후에야 피고 옥션이 사용하던 스캐너의 취약점 점검 목록 등에 포함되었다. 또한, 피고 옥션이 운영하고 있던 네트워크에 대한 침입탐지시스템이나 이 사건 데이터베이스 서버의 인증 및 접근 제어장치 등 피고 옥션이 취하고 있던 전체적인 보안조치의 내용을 고려하면, 위와 같은 개개 항목의 취약점만을 이유로 피고 옥션이 개인정보의 안전성 확보에 필요한 보호조치를 다하지 않았다고 볼 수는 없다.

마) 피고 옥션은 이 사건 데이터베이스 서버 등에 각종 인증 및 접근제어 시스템을 운용하였고, 데이터베이스 서버 보안솔루션 등 여러 보안조치를 통해 데이터베이스 서버에 대한 비정상적인 접근이나 정보조회 요청인 쿼리(Query)의 정상범위를 벗어난 실행 등을 모니터링하고 있었다. 또한, 피고 옥션의 업무나 시스템 특성, 해킹사고 당시의 보안기술의 수준 등을 고려할 때, 이 사건 해킹사고 당시 피고 옥션이 이상 징후로 설정한 조건이 잘못되었다고 보기도 어렵다. 그런데 해커가 개인정보를 누출하는 과정에서 발생한 쿼리나 데이터 전송량이 피고 옥션의 업무특성 등을 고려할 때 평균적인 수준을 넘지 않는 것이어서, 피고 옥션이 이 사건 해킹사고 당시 해커의 쿼리 실행 등을 탐지하지 못한 것이므로, 피고 옥션이 해커의 쿼리 실행 등을 탐지하지 못하였다는 사정만으로 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 취하지 않았다고

볼 수는 없다.

바) 피고 옥션은 2008. 1. 3.경 이 사건 사이트의 이상 징후를 발견한 이후 자체적으로 수립하고 있던 침해사고 대응절차에 따라 합리적인 대응 조치를 취한 것으로 보이고, 해커가 사용한 악성 프로그램인 웹쉘(Webshell)이 쉽게 발견하기 어려운 종류와 형태이고 피고 옥션이 사용한 백신 프로그램 등이 당시 보편적으로 사용되고 있던 것인 점 등을 고려하면, 피고 옥션이 이 사건 해킹사고 당시 실시간으로 웹셸을 탐지하지 못하였다고 하여 이를 잘못이라고 보기도 어렵다.

사) 해커는 탐지가 어려운 변종 웹쉘의 업로드 및 실행, 방화벽 우회를 위한 포트 포워딩, 'ARP Spoofing' 공격, 패스워드 크래킹 프로그램의 사용 등 여러 고급 해킹기법을 사용해 피고 옥션의 이노믹스 서버에 침입하여 이 사건 데이터베이스 서버의 아이디와 암호화된 비밀번호를 알아낸 후 이 사건 데이터베이스 서버에 저장된 개인정보를 누출한 것으로 추정되고, 이 사건 해킹의 수법이나 당시의 보안기술 수준, 피고 옥션이 취하고 있던 전체적인 보안조치의 내용과 수준 등을 고려하면, 피고 옥션이 이 사건 해킹사고를 근본적으로 방지하기는 어려웠던 것으로 보인다.

2) 위와 같은 사정을 앞서 본 법리에 비추어 보면, 피고 옥션이 원고들이 주장하는 바와 같이 구 정보통신망법 제28조 제1항에서 정한 기술적·관리적 조치를 취하여야 할 의무나 정보통신서비스 이용계약에 따른 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 의무를 위반하였다고 보기 어려울 뿐만 아니라, 피고 옥션이 위와 같이 개인정보의 안전성 확보에 필요한 보호조치를 취하지 않음으로써 이 사건 해킹사고를 방지하지 못한 것으로 단정하기도 어렵다.

같은 취지의 원심의 판단은 정당하여 수긍할 수 있고, 거기에 상고이유 주장과 같이

논리와 경험의 법칙을 위반하고 자유심증주의의 한계를 벗어나거나 정보통신서비스제공자의 손해배상책임에 관한 법리를 오해하는 등의 위법이 없다.

다. 상고이유 제9점에 관하여

원심은 이 사건 고시 제5조 제1항이 "정보통신서비스제공자 등은 패스워드, 생체정보 등 본인임을 인증하는 정보에 대해서는 복호되지 아니하도록 일방향 암호화하여 저장한다."고 규정하고 있는데, 2009. 1. 28. 대통령령 제21278호로 개정되어 2010. 1. 28. 시행된「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」제15조 제4항 제2호에서 비로소 주민등록번호의 암호화 저장 규정이 신설된 점 등을 근거로, 주민등록번호는 이 사건 고시 제5조 제1항에서 암호화 대상으로 정하고 있는 본인 인증 정보에 해당되지 않고, 이 사건 해킹사고 당시 암호화 제품의 기술 수준 등을 고려하면, 피고 옥션이 이 사건 해킹사고 당시 관리하고 있던 개인정보인 주민등록번호를 암호화하지 않았다고 하더라도 피고 옥션에게 법률상 또는 계약상 의무위반이 있다고 할 수 없다고 판단하였다.

관련 법리와 기록에 비추어 살펴보면, 원심의 판단은 정당한 것으로 수긍할 수 있고, 거기에 상고이유 주장과 같이 이 사건 고시의 해석이나 정보통신서비스제공자의 손해배상책임에 관한 법리를 오해하는 등의 위법이 없다.

라. 상고이유 제11점에 관하여

원심은 "정보통신서비스제공자 등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화한다."고 규정하고 있는 이 사건 고시 제7조 제1항은 권한을 가진 자가 정상적인 경로를 통해 개인정보 파일 등을 출력할 때 지켜야 할 보호조치를 규정한 것으로서, 이 사

건 해킹사고와 같이 권한 없는 자에 의한 개인정보 누출의 경우에는 이 사건 고시 제7조 제1항이 적용될 수는 없다는 등의 이유로 피고 옥션이 이 사건 고시 제7조 제1항에서 정한 의무를 위반하였다는 원고들의 주장을 배척하였다.

또한 원심은 구 정보통신망법 제45조 제2항에 의하여 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성 확보를 위해 마련하여야 하는 보호조치의 구체적 내용을 규정한 「정보보호조치 및 안전진단방법·절차·수수료에 관한 지침」(정보통신부 고시 제2004-54호, 이하 '이 사건 지침'이라 한다) 제2조와 이 사건 지침 별표 1의 2. 2. 8. 항목에서 정보통신서비스제공자에게 불필요한 프로토콜 및 서비스 제거 등의 보안설정을 보호조치의 내용으로 규정하고 있으나, 이 사건 해킹사고에 사용된 이노믹스 서버의 'DTS 툴'은 데이터 관리, 추출 및 전송 등의 기본적인 데이터베이스 작업을 하는 데 보편적으로 사용되는 것으로서 이를 불필요한 서비스라고 보기 어렵고, 피고 옥션이 이 사건 해킹사고 당시 취하고 있던 보안조치 등을 고려하면 피고 옥션이 위 'DTS 툴'의 기능을 삭제하거나 제한하지 않았다고 하여 피고 옥션이 구 정보통신망법 등에서 정한 의무를 위반한 것으로 볼 수 없다는 등의 이유로 피고 옥션이 이 사건 지침 제2조에서 정한 의무를 위반하였다는 원고들의 주장을 배척하였다.

관련 법리와 기록에 비추어 살펴보면, 원심의 판단은 정당한 것으로 수긍할 수 있고, 거기에 상고이유 주장과 같이 이 사건 고시 및 지침의 해석이나 정보통신서비스제공자의 손해배상책임 등에 관한 법리를 오해하는 등의 위법이 없다.

2. 피고 인포섹 주식회사에 대한 손해배상청구에 관하여

원심은 그 판시와 같이 피고 인포섹 주식회사가 보안관제 업무를 소홀히 하여 이 사건 해킹사고를 사전에 방지하지 못하였다고 볼 수 없다는 이유로 원고들의 청구를 배

척하였다.

관련 법리와 기록에 비추어 살펴보면, 원심의 사실인정 및 판단은 정당한 것으로 수긍할 수 있고, 거기에 논리와 경험의 법칙을 위반하고 자유심증주의의 한계를 벗어나거나 보안관제 담당업체의 손해배상책임에 관한 법리를 오해하는 등의 위법이 없다.

3. 결론

그러므로 상고를 모두 기각하고, 상고비용은 패소자들이 부담하기로 하여 관여 대법관의 일치된 의견으로 주문과 같이 판결한다.

재판장 대법관 이인복

대법관 김용덕

주 심 대법관 고영한

대법관 김소영