손해배상(기)・손해배상(기)・손해배상(기)・손해배상(기)(네이트・싸이월드 회원들의 개인정보 유출로 인한 손해배상 청구사건)

[대법원, 2018. 1. 25., 2015다24904, 24911, 24928, 24935]

【판시사항】

[1] 정보통신서비스 제공자가 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조 제1항이나 정보통신서비스 이용계약에 따른 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였는지 판단하는 기준

[2] 정보통신서비스 제공자가 '개인정보의 기술적·관리적 보호조치 기준'(방송통신위원회 고시 제2011-1호)에서 정하고 있는 기술적·관리적 보호조치를 다한 경우, 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 볼 수 있는지 여부(원칙적 소극) 및 정보통신서비스 제공자가 위 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였더라도 위법행위로 평가되거나 민법 제760조 제3항에 따른 책임을 부담하게 되는 경우

[3] 인터넷상에서 포털서비스사업을 하는 甲 주식회사가 제공하는 온라인 서비스에 가입한 회원들의 개인정보가 해킹 사고로 유출되었는데, 서비스 이용자인 乙 등이 甲 회사를 상대로 손해배상을 구한 사안에서, 정보통신서비스 제공자가 정보처리시스템에 접속한 개인정보취급자로 하여금 작업 종료 후 로그아웃을 하도록 하는 것은 보호조치 의무에 해당하지만, 위와 같은 보호조치의 미이행과 해킹사고의 발생 사이에 상당인과관계가 인정되지 아니하여 甲 회사의 손해배상책임이 인정되지 않는다고 한 사례

【판결요지】

[1] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '구 정보통신망법'이라고 한다) 제28조 제1항은 정보통신서비스 제공자가 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 그 각호의 기술적·관리적 보호조치를 하여야 한다고 규정하고 있다. 이어 위 조항은 그 각호로 '1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한 조치 4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치'를 규정하고 있다. 그리고 구 정보통신망법 제28조 제1항의 위임을 받은 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 제15조는 정보통신서비스 제공자가 취하여야 할 개인정보의 안전성 확보에 필요한 위와 같은 기술적·관리적 조치를 보다 구체적으로 규정하고 있다. 따라서 정보통신서비스 제공자는 구 정보통신망법 제28조 제1항 등에서 정하고 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 할 법률상 의무를 부담한다. 나아가 정보통신서비스 제공자가 정보통신서비스를 이용하려는 이용자와 정보통신서비스 이용계약을 체결하면서, 이용자로 하여금 이용약관 등을 통해 개인정보 등 회원정보를 필수적으로 제공하도록 요청하여 이를 수집하였다면,

정보통신서비스 제공자는 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. 그런데 정보통신서비스가 '개방성'을 특징으로 하는 인터넷을 통하여 이루어지고 정보통신서비스 제공자가 구축한 네트워크나 시스템과 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 않다. 또한 해커 등은 여러 공격기법을 통해 정보통신서비스 제공자가 취하고 있는 보안조치를 우회하거나 무력화하는 방법으로 정보통신서비스 제공자의 정보통신망 및 이와 관련된 정보시스템에 침입하고, 해커의 침입행위를 방지하기 위한 보안기술은 해커의 새로운 공격방법에 대하여 사후적으로 대응하여 이를 보완하는 방식으로 이루어지는 것이 일반적이다. 이처럼 정보통신서비스 제공자가 취해야 할 개인정보의 안전성 확보에 필요한 보호조치에 관해서는 고려되어야 할 특수한 사정이 있다. 그러므로 정보통신서비스 제공자가 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, 정보통신서비스 제공자의 업종·영업규모와 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다.

[2] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 제15조 제6항은 "방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조 제1항 제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다."라고 규정하고 있다. 이에 따라 방송통신위원회가 마련한 '개인정보의 기술적·관리적 보호조치 기준'(방송통신위원회 고시 제2011-1호, 이하 '고시'라고 한다)은 해킹 등 침해사고 당시의 기술 수준 등을 고려하여 정보통신서비스 제공자가 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것) 제28조 제1항 등에 따라 준수해야 할 기술적·관리적 보호조치를 구체적으로 규정하고 있다. 그러므로 정보통신서비스 제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한 정보통신서비스 제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다. 다만 고시는 정보통신서비스 제공자가 반드시 준수해야 할 최소한의 기준을 정한 것으로 보는 것이 타당하다. 따라서 정보통신서비스 제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다고 하더라도, 정보통신서비스 제공자가 마땅히 준수해야 한다고 일반적으로 쉽게 예상할 수 있고 사회통념상으로도 합리적으로 기대 가능한 보호조치를 다하지 아니한 경우에는 위법행위로 평가될 수 있다. 나아가 정보통신서비스 제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다고 하더라도, 불법행위에 도움을 주지 말아야 할 주의의무를 위반하여 타인의 불법행위를 용이하게 하였고 이러한 방조행위와 불법행위에 의한 피해자의 손해 발생 사이에 상당인과관계가 인정된다면 민법 제760조 제3항에 따른 책임을 면할 수 없다.

[3] 인터넷상에서 포털서비스사업을 하는 甲 주식회사가 제공하는 온라인 서비스에 가입한 회원들의 개인정보가 해킹 사고로 유출되었는데, 서비스 이용자인 乙 등이 甲 회사를 상대로 손해배상을 구한 사안에서, 정보통신서비스 제공자가 정보처리시스템에 접속한 개인정보취급자로 하여금 작업 종료 후 로그아웃을 하도록 하는 것은, 비록 '개인정보의 기술적·관리적 보호조치 기준'(방송통신위원회 고시 제2011-1호)에서 정하고 있는 기술적·관리적 보호조치에는 해당하지 않으나, 정보통신서비스 제공자가 마땅히 준수해야 한다고 일반적으로 쉽게 예상할 수 있고 사회통념상으로도 합리적으로 기대 가능한 보호조치에 해당하므로, 정보통신서비스 제공자가 이러한 보호조치를 미이행하여 정보처리시스템에 접속권한이 없는 제3자가 손쉽게 시스템에 접속하여 개인정보의 도난 등의 행위를 할 수 있도록 하였다면 이는 불법행위에 도움을 주지 말아야 할 주의의무를 위반한 것으로써 이러한 방조행위와 피방조자의 불법행위 사이에 상당인과관계가 인정된다면 공동불법행위자로서 책임을 면할 수 없는데, 해킹사고 당시 해커가 이미 키로깅을 통하여 DB 서버 관리자의 아이디와 비밀번호를 획득한 상태였기 때문에 甲 회사의 DB 기술팀 소속 직원이 자신의 컴퓨터에서 로그아웃을 하였는지 여부와 무관하게 언제든지 게이트웨이 서버를 거쳐 DB 서버에 로그인을 할 수 있었던 것으로 보이므로, 위와 같은 보호조치의 미이행과 해킹사고의 발생 사이에 상당인과관계가 인정되지 아니하여 甲 회사의 손해배상책임이 인정되지 않는다고 한 사례.

【참조조문】

[1] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것) 제28조 제1항, 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 제15조, 민법 제390조

[2] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것) 제28조 제1항, 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 제15조, 민법 제390조, 제750조, 제760조 제3항

[3] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것) 제28조 제1항, 제32조, 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 제15조, 민법 제390조, 제750조, 제760조 제3항

【참조판례】

[1]

[2] 대법원 2015. 2. 12. 선고 2013다43994, 44003 판결(공2015상, 453) /

[2] 대법원 2007. 6. 14. 선고 2005다32999 판결(공2007하, 1045)

【전문】

【원고(선정당사자), 상고인】

【피고, 피상고인】 에스케이커뮤니케이션즈 주식회사 (소송대리인 변호사 강지현 외 5인)

【원심판결】 서울고법 2015. 3. 20. 선고 2013나20047, 20054, 20061, 20078 판결

【주문】

】

상고를 모두 기각한다. 상고비용은 원고(선정당사자)들과 선정자들이 부담한다.

【이유】

】 상고이유(상고이유서 제출기간이 지난 후에 제출된 상고이유보충서 기재는 상고이유를 보충하는 범위 내에서)를 판단한다.

1. 변론재개신청을 위법하게 배척하였다는 주장에 관하여

가. 당사자가 변론종결 후 주장·증명을 제출하기 위하여 변론재개신청을 한 경우 당사자의 변론재개신청을 받아들일지 여부는 원칙적으로 법원의 재량에 속한다.

그러나 변론재개신청을 한 당사자가 변론종결 전에 그에게 책임을 지우기 어려운 사정으로 주장·증명을 제출할 기회를 제대로 얻지 못하였고, 그 주장·증명의 대상이 판결의 결과를 좌우할 수 있는 관건적 요증사실에 해당하는 경우 등과 같이, 당사자에게 변론을 재개하여 그 주장·증명을 제출할 기회를 주지 않은 채 패소의 판결을 하는 것이 민사소송법이 추구하는 절차적 정의에 반하는 경우에는 법원은 변론을 재개하고 심리를 속행할 의무가 있다(대법원 2010. 10. 28. 선고 2010다20532 판결 등 참조).

나. 기록에 의하면, 다음과 같은 사정을 알 수 있다.

(1) 원고(선정당사자, 이하 '원고'라고 한다) 1이 서울중앙지방검찰청 검사장을 상대로 이 사건 해킹사고 관련 수사기록에 대한 정보공개거부처분의 취소를 구하는 소를 제기하였는데 원심 변론종결 이후에야 위 처분을 일부 취소하는 판결이 확정되었다.

(2) 이에 따라 비로소 열람·등사가 가능하게 된 수사기록 중 일부를 증거로 제출하기 위하여 원고들이 변론재개신청을 하였다.

(3) 또한 원고들은 제1심 공동피고 주식회사 안랩(이하 '안랩'이라고 한다)의 직원이 작성한 보안관제 일일보고서, 피고가 경찰에 제출한 트래픽 관련 자료, 피고의 데이터베이스 기술팀 소속 직원인 소외 1의 경찰 진술조서 등을 참고자료로 제출하였다.

그러면서 이 사건 해킹사고 당시 평소의 임계치를 훨씬 뛰어넘는 대용량의 파일 유출이 실시간으로 감지되어 안랩이 이를 즉시 피고에게 보고한 사실, 소외 1에게 게이트웨이 서버의 접근권한이 없었다는 사실을 주장·증명하고자 하였다.

(4) 그러나 원심은 변론을 재개하지 아니하고 원심판결을 선고하였다.

다.

이러한 사정을 앞에서 본 법리에 비추어 살펴본다.

원고들은 원심 변론종결 이후에야 비로소 위 보안관제 일일보고서 등 수사기록을 열람·등사할 수 있게 되었으므로, 원고들에게 책임을 지우기 어려운 사정으로 주장·증명을 제출할 기회를 제대로 얻지 못하였다고 할 것이다.

그러나 아래와 같은 사정을 종합하여 보면 그 주장·증명의 대상이 판결의 결과를 좌우할 수 있는 관건적 요증사실에 관한 것이라고 보기 어렵고, 달리 원고들에게 변론을 재개하여 그 주장·증명을 제출할 기회를 주지 않은 채 패소의 판결을 하는 것이 민사소송법이 추구하는 절차적 정의에 반한다고 볼만한 사정을 찾아보기 어렵다.

(1) 원고들은 원심 변론종결 전에 이미 이 사건 해킹사고 당시 파일전송 프로토콜(File Transfer Protocol, 인터넷을 통해 컴퓨터 간에 파일을 송수신하는 데 사용되는 통신규약, 이하 'FTP'라고 한다)에 의한 파일전송 등으로 대용량 트래픽이 발생하였다는 주장과 소외 1에게는 게이트웨이 서버의 접근권한이 없다는 주장을 하였다.

(2) 위 보안관제 일일보고서는, 이 사건 해킹사고 당시인 2011. 7. 26. 05:40경부터 같은 날 05:50경까지 ○○빌링 하단의 트래픽이 평소보다 15배가량 증가하였고, 이는 파일전송에 의한 트래픽 증가로 추측되며, 트래픽 증가 시작 시점인 21번 FTP를 이용한 통신을 확인할 필요가 있다는 취지로 기재되어 있다.

(3) 그러나 이 사건 해킹사고 당시 해커는 네이트·싸이월드 이용자들의 개인정보가 저장되어 있는 피고의 데이터베이스 서버(이하 '이 사건 DB'라고 한다)에 침입하여 이용자들의 개인정보를 덤프 파일로 생성·압축하였기에 그 파일 용량이 10GB 정도에 불과하였다.

또한, 해커가 위 파일을 게이트웨이 서버에 내려받은 후 FTP를 이용하여 소외 1·소외 2의 컴퓨터로 내려받고 다시 이를 외부로 전송한 시점이 위 일일보고서에 기재된 트래픽 증가 시점과 일치하지도 않는다.

(4) 한편 소외 1의 경찰 진술조서 중 본인이 관리하는 데이터베이스 서버는 게이트웨이 서버를 통해 접근하는 서버가 아니라는 취지의 진술기재 부분도 있다.

(5) 그러나 위 진술조서 중에는 소외 1이 본인이 관리하는 데이터베이스가 수백 대여서 이름 등을 기억하지 못한다는 취지의 진술기재 부분도 있다.

또한 원심은 "이 사건 DB 서버와 연결된 게이트웨이 서버에는 이글루스 DB 서버도 연결되어 있었고 소외 1은 이글루스 DB 서버를 담당하고 있었기 때문에 소외 1의 컴퓨터에서는 위 게이트웨이 서버에 접근할 수 있었다.

"라고 사실인정을 하였다.

그런데 위 진술조서 작성 당시 소외 1이 이글루스 DB 서버에 접근권한이 있었는지 여부 등에 관하여는 직접적으로 신문이 이루어지지 않았다.

라. 따라서 원고들의 변론재개신청이 변론을 재개하고 심리를 속행하여야 할 예외적인 요건을 갖추었다고 볼 수 없으므로, 이를 받아들이지 아니한 원심의 조치에 상고이유 주장과 같은 법령 위반 또는 절차 위반의 위법이 있다고 할 수 없다.

2. 석명 또는 지적의무를 위반하였다는 주장에 관하여

가. 이 부분 상고이유의 요지는 다음과 같다.

원심은 별지 1. 선정자 목록의 전체 순번 1 내지 117, 1800 내지 2241, 2653 내지 2827, 2855 내지 2882 기재 각 선정자들(이하 '일부 선정자들'이라고 한다)의 개인정보가 유출되었다는 취지의 통지 또는 확인내역이 누락되었다는 점에 관하여 원고들에게 의견진술의 기회를 주지 않았다.

그런데도 일부 선정자들의 개인정보가 이 사건 해킹사고로 인하여 유출되었다는 사실을 인정할 증거가 없다는 이유로 일부 선정자들의 청구를 기각하였다.

따라서 민사소송법 제136조 제4항에 따른 석명 또는 지적의무를 다하지 않은 위법이 있다.

나. 당사자가 부주의 또는 오해로 인하여 증명하지 아니한 것이 분명하거나 쟁점이 될 사항에 관하여 당사자 사이에 명시적인 다툼이 없는 경우에는 법원은 석명을 구하고 증명을 촉구하여야 한다.

만일 당사자가 전혀 의식하지 못하거나 예상하지 못하였던 법률적 관점을 이유로 법원이 청구의 당부를 판단하려는 경우에는 그 법률적 관점에 대하여 당사자에게 의견진술의 기회를 주어야 한다.

그처럼 하지 않고 예상외의 재판으로 당사자 일방에게 불의의 타격을 가하는 것은 석명의무를 다하지 아니하여 심리를 제대로 하지 아니한 위법한 것이 된다(대법원 2008. 9. 11. 선고 2006다50338 판결 등 참조).

다.

기록에 의하면, 원고들이 이 사건 소 제기 당시 개인정보 유출에 관한 증거자료를 갖춘 선정자들과 그렇지 아니한 선정자들을 구분하여 당사자선정서를 제출한 사실, 피고가 청구기각판결을 구하는 답변서를 제출한 이래 줄곧 원고들 주장사실을 전면적으로 부인해 온 사실을 알 수 있다.

따라서 부주의 또는 오해로 인하여 증명하지 아니한 것이 분명하다거나 쟁점이 될 사항에 관하여 당사자 사이에 명시적인 다툼이 없는 경우에 해당한다고 보기 어렵다.

그러므로 원심이 원고들에게 일부 선정자들의 개인정보가 유출되었다는 취지의 통지 또는 확인내역이 누락되었다는 점에 관하여 석명을 구하거나 증명을 촉구하지 않았다고 하더라도 상고이유 주장과 같이 석명 또는 지적의무를 위반한 위법이 있다고 볼 수 없다.

3. 나머지 상고이유 주장에 관하여

가. (1) 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '구 정보통신망법'이라고 한다) 제28조 제1항은 정보통신서비스 제공자가 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 그 각호의 기술적·관리적 보호조치를 하여야 한다고 규정하고 있다.

이어 위 조항은 그 각호로 '1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한 조치 4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치'를 규정하고 있다.

그리고 구 정보통신망법 제28조 제1항의 위임을 받은 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것, 이하 '구 정보통신망법 시행령'이라고 한다) 제15조는 정보통신서비스 제공자가 취하여야 할 개인정보의 안전성 확보에 필요한 위와 같은 기술적·관리적 조치를 보다 구체적으로 규정하고 있다.

따라서 정보통신서비스 제공자는 구 정보통신망법 제28조 제1항 등에서 정하고 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 할 법률상 의무를 부담한다.

나아가 정보통신서비스 제공자가 정보통신서비스를 이용하려는 이용자와 정보통신서비스 이용계약을 체결하면서, 이용자로 하여금 이용약관 등을 통해 개인정보 등 회원정보를 필수적으로 제공하도록 요청하여 이를 수집하였다면, 정보통신서비스 제공자는 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 정보통신서비스 제공자가 구축한 네트워크나 시스템과 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 않다.

또한 해커 등은 여러 공격기법을 통해 정보통신서비스 제공자가 취하고 있는 보안조치를 우회하거나 무력화하는 방법으로 정보통신서비스 제공자의 정보통신망 및 이와 관련된 정보시스템에 침입하고, 해커의 침입행위를 방지하기 위한 보안기술은 해커의 새로운 공격방법에 대하여 사후적으로 대응하여 이를 보완하는 방식으로 이루어지는 것이 일반적이다.

이처럼 정보통신서비스 제공자가 취해야 할 개인정보의 안전성 확보에 필요한 보호조치에 관해서는 고려되어야 할 특수한 사정이 있다.

그러므로 정보통신서비스 제공자가 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, 정보통신서비스 제공자의 업종·영업규모와 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다.

(3) 특히 구 정보통신망법 시행령 제15조 제6항은 "방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조 제1항 제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

"라고 규정하고 있다.

이에 따라 방송통신위원회가 마련한 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2011-1호, 이하 '이 사건 고시'라고 한다)은 해킹 등 침해사고 당시의 기술 수준 등을 고려하여 정보통신서비스 제공자가 구 정보통신망법 제28조 제1항 등에 따라 준수해야 할 기술적·관리적 보호조치를 구체적으로 규정하고 있다.

그러므로 정보통신서비스 제공자가 이 사건 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한 정보통신서비스 제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다(대법원 2015. 2. 12. 선고 2013다43994, 44003 판결 등 참조).

(4) 다만 이 사건 고시는 정보통신서비스 제공자가 반드시 준수해야 할 최소한의 기준을 정한 것으로 보는 것이 타당하다.

따라서 정보통신서비스 제공자가 이 사건 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다고 하더라도, 정보통신서비스 제공자가 마땅히 준수해야 한다고 일반적으로 쉽게 예상할 수 있고 사회통념상으로도 합리적으로 기대 가능한 보호조치를 다하지 아니한 경우에는 위법행위로 평가될 수 있다.

나아가 정보통신서비스 제공자가 이 사건 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다고 하더라도, 불법행위에 도움을 주지 말아야 할 주의의무를 위반하여 타인의 불법행위를 용이하게 하였고 이러한 방조행위와 불법행위에 의한 피해자의 손해 발생 사이에 상당인과관계가 인정된다면 민법 제760조 제3항에 따른 책임을 면할 수 없다(대법원 2007. 6. 14. 선고 2005다32999 판결 등 참조).

나. 원심은 다음과 같은 이유를 들어 '정보통신서비스 제공자인 피고가 이 사건 고시 제4조 제4항, 제5항 등에서 정하고 있는 기술적·관리적 보호조치를 다하지 아니하였고, 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법

률상 또는 계약상 의무를 위반하였다'는 원고들의 주장을 배척하였다.

(1) 이 사건 고시 제4조 제4항의 기술적·관리적 보호조치에 관하여

(가) 이 사건 고시 제4조 제4항은 "정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증수단을 적용하여야 한다.

"라고 규정하고 있다.

(나) 장소적으로 떨어져 있는 두 개의 전산 네트워크 사이를 가상사설전산망(Virtual Private Network, 공중망을 활용하여 암호화된 패킷이나 배타적인 경로를 구성하여 사설망처럼 안전한 통신을 보장하는 가상 네트워크기술, 이하 'VPN'이라고 한다) 등의 전용선을 통하여 연결하고 있으면 이 네트워크 전체를 하나의 내부망으로 볼 수 있다.

이러한 내부망의 한쪽 네트워크에서 다른 쪽 네트워크로 접속하는 것은 이 사건 고시 제4조 제4항에 규정된 '외부에서 개인정보처리시스템에 접속하는 경우'에 해당하지 않는다.

(다) 개인정보취급자인 소외 2 등의 컴퓨터는 피고의 사옥인 서울 서대문구 △△동 소재 □□빌딩에, 이 사건 DB 서버 등은 서울 성동구 ○○동 소재 인터넷데이터센터(Internet Data Center, 이하 'IDC'라고 한다)에 있으나, 피고는 □□빌딩의 네트워크와 IDC를 VPN으로 연결하고 있다.

(라) 따라서 인터넷망 외부에서 직접 개인정보처리시스템인 ○○동 IDC에 접속한 것이 아니라 □□빌딩에 있는 직원 소외 1·소외 2의 컴퓨터에 침입한 후 그 컴퓨터에서 정상적인 접속경로와 같이 VPN을 통하여 IDC에 있는 이 사건 DB 서버에 접속한 이 사건 해킹사고에는 이 사건 고시 제4조 제4항이 적용되지 않는다.

(2) 이 사건 고시 제4조 제5항의 기술적·관리적 보호조치에 관하여

(가) 구 정보통신망법 시행령 제15조 제2항 제2호는 개인정보처리시스템에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 및 침입탐지시스템의 설치·운영을 보호조치의 하나로 규정하고 있다.

(나) 이에 따라 이 사건 고시 제4조 제5항은 정보통신서비스 제공자 등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)'하고, '개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보유출시도를 탐지(제2호)'하는 기능을 포함한 시스템을 설치·운영하여야 한다고 규정하고 있다.

(다) 위 각 규정의 내용 및 취지에 비추어 보면 이 사건 DB 서버에서 대량으로 유출되는 정보를 실시간으로 모니터링하는 기능이나 사용자 컴퓨터에 저장된 전자문서 및 데이터가 외부로 유출되는 것을 탐지 또는 차단하고 이를 감시 및 추적하는 기능을 갖춘 디엘피 솔루션(Data Loss Prevention Solution, 기밀 또는 중요 정보의 유출을 차단·예방하는 활동을 구현한 하드웨어 또는 소프트웨어, 이하 'DLP 솔루션'이라고 한다)을 설치·운영해야 하는 것까지 규정한 것으로 보기는 어렵다.

(라) 또한 피고가 준수해야 할 정보통신망 관련 법령상의 개인정보 보호를 위한 기술적·관리적 보호조치에 개인정보처리시스템에서 대량으로 유출되는 정보를 실시간으로 모니터링하는 보호조치가 포함되어 있다고 보기는 어렵다.

(마) 설령 피고가 대용량 트래픽과 FTP 파일전송에 대하여 실시간으로 모니터링을 하거나 DLP 솔루션을 설치·운영할 의무가 있었다고 하더라도, 원고들이 제출한 증거만으로는 피고가 침입탐지시스템과 DLP 솔루션을 통하여 트래픽과 FTP 파일전송을 실시간 모니터링하여 이상 징후를 탐지해야 할 기술적·관리적 보호조치를 위반하였다고 인정하기에 부족하고 달리 이를 인정할 증거가 없다.

(3) 이 사건 고시 제4조 제5항 제1호에 관하여

(가) 이 사건 DB 서버에 접속하기 위해서는 VPN을 통해 먼저 게이트웨이 서버에 접속해야 한다.

그런데 피고는 게이트웨이 서버에 접속 가능한 IP 주소를 DB 서버에 접속할 권한이 있는 직원들이 사용하는 컴퓨터의 IP 주소로 한정시키고, DB 서버에 접속 가능한 IP 주소는 게이트웨이 서버의 IP 주소로 한정시키는 방법으로 허용되지 않은 IP 주소를 통해 게이트웨이 서버나 DB 서버에 접근할 수 없도록 조치를 취하고 있었다.

(나) 이 사건 해커는 이미 키로깅(keylogging, 사용자가 키보드로 컴퓨터에 입력하는 내용을 몰래 가로채는 해킹 기법)을 통하여 이 사건 DB 서버 관리자인 소외 2의 아이디와 비밀번호를 취득하고 게이트웨이 서버부터는 이를 이용하여 접속하였다.

따라서 피고에게 게이트웨이 서버 이후의 단계에서 해당 접속행위가 애초 소외 1의 컴퓨터로부터 시작되었다는 것까지 인식하여 이를 막을 의무가 있었다거나 피고가 개인정보에 대한 불법적인 접근을 차단하기 위한 기술적·관리적 보호조치를 위반하였다고 볼 수는 없다.

(4) 개인정보처리자가 퇴근 시 로그아웃을 하지 않거나 자동 로그아웃 기능을 설정하지 않은 점에 관하여

(가) 원고들이 제출한 증거만으로는 이 사건 해킹사고 당시 DB 서버 관리자가 작업종료 후 로그아웃을 하여야 한다거나 자동 로그아웃 시간을 설정할 의무가 있었다고 인정하기에 부족하고, 달리 이를 인정할 아무런 증거가 없다.

(나) 해커는 이미 키로깅을 통하여 이 사건 DB 서버 관리자인 소외 2의 아이디와 비밀번호를 획득한 상태였기 때문에 소외 1이 자신의 컴퓨터에서 로그아웃을 하였는지 여부와 무관하게 언제든지 소외 2의 아이디와 비밀번호를 이용하여 게이트웨이 서버를 거쳐 이 사건 DB 서버에 로그인을 할 수 있었던 것으로 보인다.

(다) 따라서 소외 1이 퇴근 시 자신의 업무용 컴퓨터에서 로그아웃을 하지 아니하고 자동 로그아웃 기능을 설정하지 않았다고 하여 정보통신망 관련 법령상의 기술적·관리적 보호조치를 위반한 과실이 있다거나 이 사건 해킹사고의 발생과 사이에 상당인과관계가 있다고 볼 수는 없다.

(5) FTP를 사용한 점에 관하여

(가) 피고의 개인정보보호 업무지침서 제26조 제4항은 "개인정보 접근 PC에 대한 NULL session 접근이 불가능하도록 보안설정을 하고, telnet 및 ftp 서비스 등 보안상 취약한 서비스는 제공하지 않도록 한다.

"라고 규정하고 있다(NULL session 접근이란 사용자인증을 거치지 않고 시스템에 접근하는 것을 말한다).

(나) 구 정보통신망법 제45조에 따른 정보보호지침 제2조는 보호조치의 구체적인 내용으로 [별표 1] 2.2.8.(접근통제 및 보안설정 관리)항에서 불필요한 프로토콜 및 서비스 제거 등 보안설정을 규정하고 있다.

그러나 위 규정에 따라 불필요한 프로토콜 등을 제거해야 하는 대상은 주요정보통신서비스 제공자 및 인터넷접속역무 제공자, 집적정보통신시설 사업자이다.

그런데 피고는 위 각 사업자에 해당하지 않으므로, 결국 피고로서는 DB 서버 관리자의 컴퓨터에서 FTP 프로그램을 삭제해야 할 법령상 의무를 부담하지 아니한다.

(다) 피고의 개인정보보호 업무지침서 제26조 제4항은 개인정보 접근 PC에서 FTP 서비스를 제공하는 행위, 즉 개인정보 접근 PC를 FTP 서버로 설정하는 행위를 금지하고 있다.

그런데 이 사건 해킹사고는 개인정보 접근 PC를 FTP 클라이언트로 사용하여 개인정보를 전송한 것이므로, 이 사건 해킹사고와 관련하여 개인정보보호 업무지침서 제26조 제4항을 위반하였다고 볼 수 없다.

(라) FTP 프로그램이 아니더라도 네이트온 등의 메신저, 대용량 웹 메일서비스, 웹서버 업로드, 간이 전자우편 전송 프로토콜(Simple Mail Transfer Protocol) 등 다양한 프로그램이나 방식을 이용하여 대량정보 전송이 가능한 이상 피고가 FTP 프로그램을 사용했다는 사실만으로 어떠한 주의의무를 위반하였다고 단정하기도 어렵다.

다.

먼저 개인정보처리자가 퇴근 시 로그아웃을 하지 않거나 자동 로그아웃 기능을 설정하지 않은 점에 관한 원심의 판단을 살펴본다.

앞에서 본 법리에 비추어 보면, 정보통신서비스 제공자가 정보처리시스템에 접속한 개인정보취급자로 하여금 작업 종료 후 로그아웃을 하도록 하는 것은, 비록 이 사건 고시에서 정하고 있는 기술적·관리적 보호조치에는 해당하지 않으나, 정보통신서비스 제공자가 마땅히 준수해야 한다고 일반적으로 쉽게 예상할 수 있고 사회통념상으로도 합리적으로 기대 가능한 보호조치에 해당한다.

또한, 정보통신서비스 제공자가 이러한 보호조치를 미이행하여 정보처리시스템에 접속권한이 없는 제3자가 손쉽게 위 시스템에 접속하여 개인정보의 도난 등의 행위를 할 수 있도록 하였다면 이는 불법행위에 도움을 주지 말아야 할 주의의무를 위반한 것이다.

만약 이러한 방조행위와 피방조자의 불법행위 사이에 상당인과관계가 인정된다면 공동불법행위자로서 책임을 면할 수 없다.

따라서 원심판단 중 이 사건 고시에 위와 같은 보호조치를 할 의무가 규정되어 있지 않다는 이유만으로 정보통신서비스 제공자가 위와 같은 보호조치 의무를 부담하지 않는 것처럼 판시한 부분은 부적절하다.

그러나 원심판결 이유를 기록에 비추어 살펴보면, 해커는 이미 키로깅을 통하여 이 사건 DB 서버 관리자인 소외 2의 아이디와 비밀번호를 획득한 상태였기 때문에 소외 1이 자신의 컴퓨터에서 로그아웃을 하였는지 여부와 무관하게 언제든지 소외 2의 아이디와 비밀번호를 이용하여 게이트웨이 서버를 거쳐 이 사건 DB 서버에 로그인을 할 수 있었던 것으로 보인다.

따라서 원심이 결론적으로 위와 같은 보호조치의 미이행과 관련한 원고들의 주장을 배척한 것에 상고이유 주장과 같이 민법 제750조의 불법행위 및 상당인과관계에 관한 법리를 오해하여 판결에 영향을 미친 잘못이 없다.

또한 앞에서 본 법리와 기록에 비추어 살펴보면, 원심의 나머지 판단 부분 역시 상고이유 주장과 같이 이 사건 고시의 해석 등을 그르친 잘못이 없다.

4. 결론

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

[[별 지] 선정자 명단: 생략]

대법관 김신(재판장) 박상옥 이기택(주심) 박정화