손해배상

[대법원 2018. 12. 28. 2017다256910]

【판시사항】

[1] 정보통신서비스 제공자가 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조 제1항 및 정보통신서비스 이용계약에 근거하여 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)

[3] 甲 주식회사와 정보통신서비스 이용계약을 체결한 乙 등의 개인정보가 해킹사고로 유출되자 乙 등이 甲 회사를 상대로 손해배상을 구한 사안에서, 甲 회사가 퇴직한 개인정보취급자의 개인정보처리시스템 접근권한을 말소하지 않았더라도 그것과 정보유출사고 발생 사이에 상당인과관계를 인정하기 어렵고, 甲 회사가 개인정보처리시스템의 접속기록을 확인·감독함으로써 '개인정보의 기술적·관리적 보호조치 기준'(방송통신위원회 고시 제2011-1호)을 준수하였다고 볼 수 있는데도, 甲 회사가 위 고시에서 정한 기술적·관리적 보호조치를 다하지 않아 정보유출사고가 발생하였다고 본 원심판단에 법리오해의 잘못이 있다고 한 사례

【참조조문】

[1] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것) 제28조 제1항, 민법 제390조, 제750조

[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(2014. 11. 28. 대통령령 제25789호로 개정되기 전의 것) 제15조, 민법 제390조, 제750조

[3] 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(2014. 11. 28. 대통령령 제25789호로 개정되기 전의 것) 제15조, 민법 제390조, 제750조

【참조판례】

[1]

[2] 대법원 2015. 2. 12. 선고 2013다43994, 44003 판결(공2015상, 453), 대법원 2018. 1. 25. 선고 2015다24904, 24911, 24928, 24935 판결(공2018상, 491)

【전문】

【원고, 피상고인】 별지 원고 명단 기재와 같다.

【피고, 상고인】 주식회사 케이티 (소송대리인 법무법인(유한) 태평양 담당변호사 홍기태 외 5인)

【원심판결】 서울중앙지법 2017. 7. 21. 선고 2014나70589 판결

【주문】

】

원심판결을 파기하고, 사건을 서울중앙지방법원에 환송한다.

【이유】

】 상고이유를 판단한다.

1. 가. 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '구 정보통신망법'이라고 한다) 제28조 제1항에 의하면 정보통신서비스 제공자가 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 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 등의 기술적·관리적 조치를 하여야 한다.

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

정보통신서비스 제공자가 정보통신서비스를 이용하려는 이용자와 정보통신서비스 이용계약을 체결할 때에 이용약관 등을 통해 이용자에게 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 이용계약상 의무를 부담한다.

나. 정보통신서비스 제공자가 구 정보통신망법 제28조 제1항 및 정보통신서비스 이용계약에 근거하여 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였는지 여부를 판단할 때에는 해킹 등 침해사고 당시 일반적으로 알려져 있는 정보보안 기술 수준, 정보통신서비스 제공자의 업종과 영업 규모, 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹 기술 수준과 정보보안기술 발전 정도에 따른 피해 발생 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보 누출로 인하여 이용자가 입게 되는 피해 정도 등의 사정을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 하여야 한다.

다.

한편 구 정보통신망법 시행령(2014. 11. 28. 대통령령 제25789호로 개정되기 전의 것, 이하 '구 정보통신망법 시행령'이라고 한다) 제15조는 제1항 내지 제5항에서 구 정보통신망법 제28조 제1항에 의하여 정보통신서비스 제공자가 취하여야 할 기술적·관리적 조치를 구체적으로 규정하고, 제6항에서 "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 하여야 할 기술적·관리적 보호조치의 구체적 기준을 정하고 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 2018. 1. 25. 선고 2015다24904, 24911, 24928, 24935 판결 등 참조).

2. 상고이유 제3점에 관하여

이 사건 고시 제4조 제2항은, 정보통신서비스 제공자 등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다고 규정하고 있다.

기록에 의하면, 소외 1은 소외 2가 퇴직하기 전인 2011. 9.경 이미 N-STEP UI가 ESB 서버와 통신하기 위하여 필요한 데이터 헤더 정보의 변수 값에 해당하는 임의의 값을 찾아내어, 피고의 VPN에 접속되어 있기만 하면 N-STEP 포털의 인증과 N-STEP UI를 통한 AUT 서버 인증을 거칠 필요 없이 곧바로 ESB 서버와 통신을 할 수 있게 되었고, 이 사건 해킹프로그램 역시 위와 같은 인증을 거치지 않고 직접 ESB 서버에 접속하여 피고의 고객정보를 유출하도록 설계되었으며, N-STEP 시스템은 ESB 서버 이후로는 접속권한 인증절차를 두고 있지 않은 사실을 알 수 있다.

그런데 이와 같은 구조하에서는 설령 피고가 소외 2 퇴직 후 소외 2의 N-STEP ID(ID 번호 생략)를 폐기하여 개인정보처리시스템인 N-STEP 시스템에 대한 접근권한을 말소하였다고 하더라도, ESB 서버는 그 접근권한 말소 여부를 확인하지 않으므로 이 사건 해킹프로그램을 이용한 고객정보 유출을 막을 수 없다.

또 소외 1로서는 소외 2의 ID 대신 N-STEP ID의 규격에 맞게 임의의 7자리 숫자를 입력하였더라도 이 사건 해킹프로그램을 통해 ESB 서버에 접속할 수 있었을 것으로 보인다.

따라서 설령 피고가 퇴직자 소외 2의 접근권한을 말소하지 않아 위 고시 규정을 위반하였다고 하더라도, 그것과 이 사건 정보유출사고 발생 사이에 상당인과관계를 인정하기 어렵다.

그런데도 원심은 그 판시와 같은 이유만으로 피고가 이 사건 고시 제4조 제2항에 정한 조치를 다하지 않아 이 사건 정보유출사고가 발생하였다는 취지로 판단하였다.

이러한 원심판단에는 위 고시 규정과 상당인과관계 등에 관한 법리를 오해하여 판결에 영향을 미친 잘못이 있다.

이 점을 지적하는 상고이유 주장은 이유 있다.

3. 상고이유 제2점에 관하여

이 사건 고시 제5조 제1항은, 정보통신서비스 제공자 등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 한다고 규정하고 있다.

기록에 의하면 N-STEP 시스템 사용자가 고객정보를 조회할 경우 N-STEP 시스템의 접속경로인 N-STEP UI에서 접속기록이 생성되어 인증 서버인 AUT 서버에 저장되고, 피고는 AUT 서버 단계에서 1일 1,000건이 넘는 고객정보 조회 내역이 탐지되는 경우 경고 메시지를 보내는 등 위 서버에 저장된 접속기록을 확인·감독해온 사실을 알 수 있다.

한편 N-STEP 시스템은 N-STEP UI를 통해 N-STEP 포털 및 AUT 서버에서 인증을 거친 사용자만 ESB 서버에 접근할 수 있는 구조로 설계되어 있었고, 피고로서는 제3자가 AUT 서버를 우회하여 N-STEP 시스템에 접속할 가능성을 예견하기 어려웠을 것으로 보인다.

그리고 원심판단에 따르더라도 ESB 서버 이후 단계에서는 접속권한 인증을 거치지 않는 구조였다는 것만으로 피고가 개인정보 유출 등의 방지를 위한 기술적·관리적 조치를 다하지 않았다고 볼 수 없고, 피고가 N-STEP 포털 및 AUT 서버 단계에 갖추어 놓은 접근통제장치가 불완전하다고 볼 수도 없다는 것이다.

그렇다면 특별한 사정이 없는 한 피고로서는 위와 같이 AUT 서버에 저장된 접속기록을 확인·감독함으로써 위 고시 규정을 준수하였다고 볼 수 있다.

그런데도 원심은 그 판시와 같은 이유만으로 피고가 이 사건 고시 제5조 제1항에 정한 기술적·관리적 보호조치를 다하지 않았다고 판단하였다.

이러한 원심판단에는 구 정보통신망법 제28조 제1항과 위 고시 규정 등에 관한 법리를 오해하여 판결에 영향을 미친 잘못이 있다.

이를 지적하는 상고이유 주장은 이유 있다.

4. 결론

그러므로 나머지 상고이유에 관한 판단을 생략한 채 원심판결을 파기하고, 사건을 다시 심리·판단하도록 원심법원에 환송하기로 하여, 관여 대법관의 일치된 의견으로 주문과 같이 판결한다.

[[별 지] 원고 명단: 생략]

대법관 박정화(재판장) 권순일(주심) 이기택 김선수