대법원 2017다207994, 2017다256910 사건 보도자료

대법원 공보관실(02-3480-1451)

대법원(주심 대법관 권순일)은 2012년 발생한 통신사 A의 고객 개인정보 유출사고 피해자들이 위 회사를 상대로 손해배상을 청구한 두 건의 소송에서, ① 원고들 청구를 기각한 원심판결에 대한 상고를 기각하여 원심판결을 확정하고(대법원 2018. 12. 28. 선고 2017다207994 판결), ② 원고들 청구를 일부 인용한 원심판결은 파기·환송하였음(대법원 2018. 12. 28. 선고 2017다256910 판결)

1. 사건 개요 및 소송 경과

▣ 사건 개요

- 최○○ 등은 최○○이 개발한 해킹프로그램을 이용하여 피고(통신사 A)의 고객정보를 저장한 데이터베이스에 침입해, 2012. 2. 20.부터 2012. 7. 13.까지 피고 고객의 개인정보(주민등록번호, 휴대전화번호, 주소 등) 1,000만 건 이상을 위법하게 취득·유출하였음(이하 '**이 사건 정보유출사고**')

- 이 사건 정보유출사고 피해자 중 341명이 피고를 상대로 '이 사건 정보유출사고로 개인정보통제에 관한 인격권이 침해되었다'고 주장하면서 위자료로 각 50만 원의 지급을 구하는 소를 제기하였음(서울중앙지법 2014. 8. 22. 선고 2012가합533204 판결 ➪ 서울고법 2017. 1. 13. 선고 2014나2032746 판결 ➪ 대법원 2017다207994호. 이하 '**제1소송**')

- 이 사건 정보유출사고의 또 다른 피해자 100명이 피고를 상대로 위와

같은 취지로 주장하면서 위자료로 각 50만 원의 지급을 구하는 소를 제기하였음(서울중앙지법 2014. 12. 5. 선고 2012가단216564 판결 ➪ 서울중앙지법 2017. 7. 21. 선고 2014나70589 판결 ➪ 대법원 2017다256910. 이하 '**제2소송**')

- 현재 하급심에 다수의 유사 사건이 계속 중임 (서울고법 2014나2032739, 2014나2032708 등)

▣ 제1심 및 원심 판단

- 제1, 2소송 모두 제1심에서는 원고들 일부 승소 판결이 선고되었음(인용금액은 원고당 각 10만 원)
- 그러나 **제1소송 항소심**은 다음과 같은 이유로 제1심판결을 파기하고 원고들 청구를 모두 기각함(서울고법 2014나2032746 판결)
  - ❶ 별도 인증서버를 두는 대신 중개 서버나 데이터베이스 서버 자체에는 인증절차를 두지 않은 피고의 접근통제시스템 자체가 불완전하다고 볼 수 없음
  - ❷ 피고가 퇴직자 이○○의 개인정보처리시스템에 대한 접근권한을 말소하지 않았다거나, 그로 인하여 이 사건 정보유출사고가 발생했다고 볼 수 없음
  - ❸ 피고가 개인정보처리시스템의 개인정보 처리 내역 등에 관한 확인·감독을 게을리하였다고 보기 어려움
  - ❹ 피고가 개인정보 등 송·수신시 암호화 의무를 위반하였다고 볼 수 없음
- 이에 반해 **제2소송 항소심**은 위 ❶, ❹ 쟁점에 관해서는 제1소송 항소심과 결론을 같이하면서도, 피고가 위 ❷, ❸과 같은 조치를 다하지 않은 결과 이 사건 정보유출사고가 발생하였다고 보아 피고의 항소를 기각하였음(=제1심의 원고 일부 승소 결론 유지, 서울중앙지법 2014나70589 판결)

2. 대법원 판단 요지 : (제1소송) 상고기각, (제2소송) 파기환송

▣ 피고는 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '구 정보통신망법')에 정한 정보통신서비스 제공자로서 동법 제28조 제1항 등에서 정하고 있는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 할 법률상 의무가 있고, 그 고객들로부터 수집한 개인정보 등이 분실·도난·누출·변조 또는 훼손되지 않도록 개인정보 등의 안전성 확보에 필요한 보호조치를 취해야 할 정보통신서비스 이용계약상 의무도 있음

- 정보통신서비스 제공자가 위와 같은 법률상 또는 계약상 의무를 위반하였는지는, 해킹 등 침해사고 당시 일반적으로 알려져 있는 정보보안 기술 수준, 정보통신서비스 제공자의 업종과 영업 규모, 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안조치에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술 수준과 정보보안기술 발전 정도에 따른 피해 발생 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보 누출로 인하여 이용자가 입게 되는 피해 정도 등의 사정을 고려하여, 정보통신서비스 제공자가 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 등을 종합하여 판단해야 함

▣ 제1, 2소송의 항소심이 모두 인정하였듯이, 별도의 인증서버를 둔 피고의 접근통제시스템 자체가 불완전하다거나, 피고가 개인정보 등 송·수신시 암호화 의무를 위반하였다고 볼 수 없음(위 ❶, ❹)

▣ ① 피고가 2011. 10. 11. 퇴직자 이○○의 전산영업시스템(N-STEP 시스템) ID를 폐기하였을 뿐만 아니라, ② 최○○이 그 이전에 이미 인증서버를 우회하는 방법을 찾아낸 사실에 비추어 보면 위 계정 폐기 여부와 이 사건 정보유출사고 사이에 인과관계도 인정하기 어려움 ➪ 피고가 퇴직자 이○○의 개인정보처리시스템에 대한 접근권한을 말소하지 않았다거나, 그로 인하여 이 사건 정보유출사고가 발생했다고 볼 수 없음(위 ❷)

▣ (적어도 국내에서는 이 사건 정보유출사고와 같이 인증서버를 우회하는

방식의 해킹이 성공한 적이 없었던 상황에서) 피고가 인증서버에 저장된 접속기록을 확인·감독한 이상 개인정보처리시스템의 개인정보 처리 내역 등에 관한 확인·감독을 게을리 하였다고 보기 어려움(위 ❸)

▣ 결론

● 위와 같은 취지로 원고들 청구를 기각한 제1소송 항소심 판결은 정당함 ➪ 원고들 상고 기각

● 위와 달리 원고들 청구를 일부 인용한 제2소송 항소심 판결은 부당함 ➪ 피고 상고 인용, 원심판결 파기·환송

3. 판결의 의의

▣ 정보통신서비스 제공자가 개인정보보호를 위한 법률상 또는 계약상 의무를 위반하였는지를 판단할 때에는, 해킹으로 인한 침해사고의 경우 당시 일반적으로 알려져 있는 정보보안 기술 수준, 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 해킹기술 수준과 정보보안기술 발전 정도에 따른 피해 발생 회피 가능성 등을 종합적으로 고려하여야 한다는 것을 다시 한 번 확인한 판결임