손해배상(기)

[대법원, 2018. 12. 28., 2017다207994]

【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, 제반 사정에 비추어 甲 회사가 '개인정보의 기술적·관리적 보호조치 기준'(방송통신위원회 고시 제2011-1호)에서 정한 기술적·관리적 보호조치를 취하지 않았다거나 정보통신서비스 제공자에게 요구되는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하지 않아 정보유출사고가 발생하였다고 보기 어렵다고 한 원심판단을 수긍한 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, 상고인】 별지 원고 명단 기재와 같다. (소송대리인 법무법인 인본 담당변호사 정한철 외 3인)

【피고, 피상고인】 주식회사 케이티 (소송대리인 법무법인(유한) 태평양 담당변호사 홍기태 외 6인)

【원심판결】 서울고법 2017. 1. 13. 선고 2014나2032746 판결

【주문】

】

상고를 모두 기각한다. 상고비용은 원고들이 부담한다.

【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, 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 종합적으로 고려하여 정보통신서비스 제공자가 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. 원심은 다음과 같은 이유를 들어, 피고가 이 사건 고시에서 정한 기술적·관리적 보호조치를 취하지 않았다거나 정보통신서비스 제공자에게 요구되는 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하지 않아 이 사건 정보유출사고가 발생하였다고 보기 어렵다고 판단하였다.

가. 이 사건 고시 제4조 제5항에 의하면, 정보통신서비스 제공자 등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는 기능을 포함한 시스템을 설치·운영하여야 한다.

그런데 피고의 N-STEP 시스템이 N-STEP 포털 및 AUT 서버(피고의 고객정보를 보관하는 데이터베이스 서버와는 별도로 설치한 인증 서버)에만 접속권한 인증절차를 두고, 그 이후 단계의 서버에는 별도의 인증절차를 두지 않았다는 것만으로는 위 고시 규정을 위반한 것으로 보기 어렵고, 피고가 N-STEP 포털 서버와 AUT 서버 단계에 갖추어 놓은 접근 통제장치가 불완전하여 위 고시 규정이 요구하는 기술적·관리적 보호조치를 다하지 않은 것으로 보기 어렵다.

나. 이 사건 고시 제4조 제2항에 의하면, 정보통신서비스 제공자 등은 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

기록에 의하면, 피고가 퇴직자 소외 1의 N-STEP 계정을 AUT 서버(인증 서버)에서 인증할 수 없도록 폐기한 사실을 인정할 수 있으므로, 피고가 소외 1의 개인정보처리시스템에 대한 접근권한을 말소하지 않았다고 볼 수 없다.

또 피고가 위 계정을 말소하였는지 여부는 이 사건 정보유출사고 발생과 인과관계가 없으므로, 피고가 위 고시 규정을 위반함으로써 이 사건 정보유출사고가 발생하였다고 볼 수 없다.

다.

이 사건 고시 제5조 제1항에 의하면, 정보통신서비스 제공자 등은 개인정보취급자가 개인정보시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 한다.

N-STEP 시스템은 AUT 서버라는 별도의 인증 서버를 두어 그 인증을 받은 사용자만 해당 시스템을 사용할 수 있도록 설계되어 있고, 피고로서는 제3자가 AUT 서버를 우회하여 N-STEP 시스템에 접속할 가능성을 예견하기 어려웠을 것으로 보이므로, 피고가 AUT 서버 단계에서 접속기록을 보관·확인·감독한 이상 위 규정을 위반하였다고 보기 어렵다.

라. 이 사건 고시 제6조 제3항에 의하면, 정보통신서비스 제공자 등은 정보통신망을 통해 이용자의 개인정보 등을 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화하여야 한다.

피고는 N-STEP 시스템을 통해 대리점 컴퓨터에 고객정보를 전송함에 있어 두 가지 방식(IPSec 방식과 3-DES 방식)으로 이를 암호화하여 전송하였다.

다만 대리점의 VPN(가상사설망) 장비를 거친 후 대리점 컴퓨터에 이르는 구간에서 여러 고객정보 중 '실사용자의 주민등록번호'가 암호화되지 않은 상태로 노출된 것으로 보이지만, 피고의 고객정보를 유출한 소외 2가 이를 확인한 곳은 대리점 PC의 내부 영역이므로 위 규정에 따라 암호화가 요구되는 영역이 아니다.

그러므로 피고가 위 고시 규정을 위반하였다고 보기 어렵다.

3. 앞서 본 법리와 기록에 비추어 원심판결 이유를 살펴보면, 원심의 위와 같은 판단에 상고이유 주장과 같이 정보통신망법 제28조 제1항에 정한 개인정보 보호를 위한 기술적·관리적 보호조치, 위 각 고시 규정의 해석 등에 관한 법리를 오해하거나, 필요한 심리를 다하지 아니한 채 논리와 경험의 법칙에 반하여 자유심증주의의 한계를 벗어나는 등의 잘못이 없다.

한편 원심이 채택한 증거에 의하면 피고가 고객정보를 그 데이터베이스 서버에 저장할 때에 암호화 조치를 취한 사실을 알 수 있다.

따라서 설령 원심판단에 원고들의 이 사건 고시 제6조 제2항(정보통신서비스 제공자 등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

) 위반 주장에 관한 판단을 누락한 잘못이 있다고 하더라도, 이는 판결 결과에 영향을 미치지 못한다.

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

[[별 지] 원고 명단: 생략]

대법관 박정화(재판장) 권순일(주심) 이기택 김선수