대 법 원

제 3 부

판 결

사 건	2018두56404 과징금부과처분취소
원고, 피상고인	주식회사 케이티
	소송대리인 변호사 김진환 외 3인
피고, 상고인	개인정보 보호위원회(경정 전 피고: 방송통신위원회)
	소송대리인 법무법인 민후
	담당변호사 김경환 외 1인
원 심 판 결	서울고등법원 2018. 8. 24. 선고 2016누64533 판결
판 결 선 고	2021. 8. 19.

주 문

상고를 기각한다.

상고비용은 피고가 부담한다.

이 유

상고이유(상고이유서 제출기간이 경과한 후에 제출된 준비서면의 기재는 상고이유를 보충하는 범위에서)를 판단한다.

1. 상고이유 제1점에 대하여

가. 사건의 경과 및 원심의 판단

1) 원심판결 이유와 기록에 따르면 다음과 같은 사실을 알 수 있다.

가) 이용자가 마이올레 홈페이지에 접속하여 자신의 인증 정보를 입력하면, 위 홈페이지의 웹 서버는 통합인증 서버를 통해 확인된 이용자 인증 정보를 이용자 PC에 전달한다. 만일 이용자가 회원 자격으로 로그인 하였을 경우 9자리 숫자로 구성된 이용자 고유의 서비스계약번호가 쿠키 내에 저장된다.

나) 이용자가 로그인 상태에서 웹 브라우저에 표시된 메뉴 중 '요금명세서 보기'를 선택하면, 웹 브라우저는 웹 서버에 이용자의 서비스계약번호에 상응하는 요금 조회 메시지를 전송하고, 웹 서버는 데이터베이스 서버로부터 그 해당 값을 읽어와 이용자 PC에 이를 송신하여 이용자 PC의 웹 브라우저 화면에 표시하도록 한다.

다) 해커는 자신의 PC에 파로스 프로그램을 설치·실행한 후 마이올레 홈페이지에 접속하여 자신의 인증 정보로 접속하여 '요금명세서 보기'를 선택하면서 웹 브라우저의 요청 메시지가 웹 서버에 전송되기 전 파로스 프로그램을 이용해서 전송을 멈추게 한다. 이어 해커는 위 프로그램을 통해 웹 브라우저의 요청 메시지 중 해커의 서비스계약번호로 되어 있는 '서비스계약번호 항목'을 임의의 9자리 숫자로 변경한 후 전송 버튼을 누른다. 마이올레 홈페이지의 웹 서버는 데이터베이스 서버로부터 임의의 서비스계약번호에 해당하는 요금명세서 값을 이용자 PC의 웹 브라우저 화면에 표시한다.

라) 해커는 임의의 서비스계약번호에 해당하는 이용자의 요금정보와 웹 서버가 웹 브라우저에 송신해 준 '고객의 이름, 주민등록번호, 주소, 서비스가입정보' 등(이는 웹 브라우저 화면에는 표시되지 않는다)을 파로스 프로그램을 통해 수집하였는데, 2013. 8. 8.부터 2014. 2. 25.까지 위 과정을 반복하며 11,708,875건의 개인정보를 유출하였

다.

마) 원고는 2006. 10. 1.과 2006. 10. 25. 국제웹보안표준기구에서 발표한 10대 보안 취약점을 검출할 수 있는 자동화된 점검 도구를 도입하여 이를 원고의 보안점검관리 포털에 연동시켜 마이올레 홈페이지 등 원고 운영 웹사이트 개발자들이 소프트웨어 소스코드를 작성 및 수정(유지·보수)하는 단계에서부터 위와 같은 자동화된 점검 도구를 활용하였다. 또한 원고는 2012. 11.경과 2013. 7.경 마이올레 홈페이지의 시스템을 대상으로 모의해킹을 수행하고, 국가정보원 IT보안인증사무국이 인증한 침입방지시스템을 설치·운영하였다.

2) 원심은, ① 구 「개인정보의 기술적·관리적 보호조치 기준」(2015. 5. 19. 방송통신위원회고시 제2015-3호로 개정되기 전의 것, 이하 '이 사건 고시'라고 한다) 제4조 제9항은 기본적으로 정보통신서비스 제공자 측의 내부적 요인으로 개인정보가 유출되지 않도록 조치를 취하라는 것으로, 파라미터 변조와 같은 해킹을 통한 개인정보 누출 방지를 직접적으로 규율하지는 않고, ② 이 사건 고시 제4조 제9항의 개인정보처리시스템은 기본적으로 소위 내부 영역에 있는 데이터베이스관리시스템을 의미하여, 웹 서버나 웹 페이지는 이에 포함되지 않으며, ③ 원고가 수차례에 걸쳐 웹 취약점을 점검하고 이를 최소화하는 조치를 취하였다는 등의 이유를 들어 이 사건 해킹사고 중 마이올레 홈페이지 부분과 관련하여 원고가 이 사건 고시 제4조 제9항에 따른 보호조치의무를 위반한 것으로 볼 수 없다고 판단하였다.

나. 이 사건 고시의 적용 범위 및 개인정보처리시스템의 범위

1) 구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2014. 5. 28. 법률 제12681호로 개정되기 전의 것, 이하 '구 정보통신망법'이라고 한다) 제28조 제1항 제2호

는 "정보통신서비스 제공자 등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영의 기술적·관리적 조치를 하여야 한다."라고 정하고 있다. 그 위임에 따른 구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(2020. 8. 4. 대통령령 제30894호로 개정되기 전의 것, 이하 '구 정보통신망법 시행령'이라고 한다) 제15조는 제2항에서 정보통신서비스 제공자 등이 개인정보에 대한 불법적인 접근을 차단하기 위하여 하여야 할 조치로서, 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 '개인정보처리시스템'이라고 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호), 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호), 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호) 등을 열거하면서, "방송통신위원회(경정 전 피고, 이하 '피고'라고 한다)는 제2항의 규정에 따른 사항을 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다."라고 정하고 있다(제6항). 위 제6항의 위임에 따른 이 사건 고시 제4조 제9항은 "정보통신서비스 제공자 등은 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등(이하 '인터넷 홈페이지 등'이라고 한다)을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다."라고 정하고 있다.

이처럼 이 사건 고시 제4조 제9항은 정보통신서비스 제공자 등의 내부적인 부주의로 인하여 개인정보가 외부로 유출되는 사고뿐만 아니라 정보통신서비스 제공자 등이 기술적 보호조치를 충분히 다하지 못하여 해킹과 같이 외부로부터의 불법적인 접근에

의해 개인정보가 외부로 유출되는 사고(이하 내부적 부주의 또는 외부로부터의 불법적인 접근 등으로 인한 개인정보 유출사고를 통틀어 '해킹 등 침해사고'라고 한다)를 방지하기 위한 목적에서 마련되었다.

2) 한편 앞서 본 관련 규정의 체계, 입법 목적에다가 구 정보통신망법 시행령 제15조 제2항 제1호, 이 사건 고시 제2조 제4호에서 모두 '개인정보처리시스템'을 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템'으로 정의하고 있는 점 등에 비추어 볼 때, 이 사건 고시 제4조 제9항의 '개인정보처리시스템'은 개인정보의 생성, 기록, 저장, 검색, 이용과정 등 데이터베이스시스템(DBS) 전체를 의미하는 것으로, 데이터베이스(DB)와 연동되어 개인정보의 처리 과정에 관여하는 웹 서버 등을 포함한다고 봄이 타당하다.

3) 원심이 이 사건 고시 제4조 제9항이 해킹을 통한 개인정보 유출 방지를 직접적으로 규율하지 않고, 개인정보처리시스템에 웹 서버가 포함되지 않는다고 설시한 것은 앞서 본 이유로 부적절하다.

다. 이 사건 고시 제4조 제9항에 따른 보호조치의무 위반 여부

1) 이 사건 고시 제4조 제9항이 해킹을 통한 개인정보 유출 방지를 직접적으로 규율하고, 개인정보처리시스템에 웹 서버가 포함된다는 전제 아래 원고가 이 사건 해킹 사고 중 마이올레 홈페이지 부분의 발생과 관련하여 이 사건 고시 제4조 제9항에 따른 보호조치를 다하였는지를 살펴본다.

2) 정보통신망법령의 문언, 입법 목적 및 규정 체계 등을 고려하면, 이 사건 고시 제4조 제9항에서 정보통신서비스 제공자 등의 의무로 규정하고 있는 조치는 '정보통신서비스 제공자 등이 취급 중인 개인정보가 인터넷 홈페이지 등에 대한 해킹 등 침해사

고에 의해 유출되지 않도록 개인정보처리시스템과 개인정보취급자의 컴퓨터에 취하여야 할 사회통념상 합리적으로 기대 가능한 정도의 기술적 보호조치'라고 해석할 수 있다. 정보통신서비스 제공자 등이 이 사건 고시 제4조 제9항에서 정한 보호조치를 다하였는지 여부는 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, 정보통신서비스 제공자의 업종·영업규모, 정보통신서비스 제공자 등이 인터넷 홈페이지 등의 설계에 반영하여 개발에 적용한 보안대책·보안기술의 내용과 실제 개발된 인터넷 홈페이지 등을 운영·관리하면서 실시한 보안기술의 적정성 검증 및 그에 따른 개선 조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹에 의한 개인정보 유출의 경우 이에 실제 사용된 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피 가능성, 정보통신서비스 제공자 등이 수집한 개인정보의 내용과 개인정보의 유출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 판단하여야 한다.

3) 앞서 본 사실관계를 이러한 법리에 비추어 살펴보면, 원고가 마이올레 홈페이지를 통한 개인정보 유출과 관련하여 이 사건 고시 제4조 제9항에 따른 조치, 즉 자신이 취급 중인 개인정보가 해킹 등 침해사고에 의해 유출되지 않도록 개인정보처리시스템과 개인정보취급자의 컴퓨터에 사회통념상 합리적으로 기대 가능한 정도의 기술적 보호조치를 다하지 않았다고 단정하기는 어렵다. 그 구체적 이유는 다음과 같다.

가) 마이올레 홈페이지와 같이 상당한 규모의 소스코드가 작성되는 소프트웨어의 경우, 입력되는 파라미터가 다양하고 그 입력 값에 대응하여 소프트웨어가 작동할 수 있는 경우의 수 역시 매우 방대하기 때문에, 소스코드를 작성하는 개발 단계에서 파라미터 변조라는 예외적인 상황을 모두 예상하여 이를 소스코드에 반영하도록 기대하기

란 쉽지 않다. 설령 이 사건 마이올레 홈페이지 해킹사고 당시 파라미터 변조와 관련된 웹 취약점이 널리 알려졌다고 하더라도, 이를 사전에 완벽하게 방지하는 것이 용이하였다고 평가할 수는 없다.

나) 특히 이용자가 홈페이지에 정상적으로 로그인을 한 상태라면 이에 기반을 두어 추가적인 정보를 제공받을 권한까지 보장받는다고 보는 것이 일반적이기 때문에, 프로그래머 입장에서는 이러한 전제 아래에서 프로그램을 설계하는 것이 통상적일 것이므로 위 프로그램에 적용된 보안기술이 이 사건 마이올레 홈페이지 해킹사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준에 미치지 못한다고 보기도 어렵다.

다) 원고는 위와 같은 해킹 사실이 알려진 이후 위와 같은 웹 취약점을 인지하고 파라미터로 전달된 서비스계약번호가 로그인한 이용자 본인의 것이 아닌 경우 요금명세서 정보가 제공되지 않도록 소스코드를 수정함으로써 취약점을 제거한 것으로는 보인다. 그러나 사후 시정조치가 비교적 손쉽게 이루어졌다는 사정에만 주목하여 이 사건 고시 제4조 제9항 위반 여부를 판단한다면 이는 결과책임을 묻는 것으로 귀결될 우려가 크다.

라) 결국 파라미터 변조에 대한 웹 취약점과 관련한 이 사건 고시 제4조 제9항 조치의무의 위반 여부는, 정보통신서비스 제공자 등이 인터넷 홈페이지 등을 운영·관리하면서 오랜 시간에 걸쳐 지속적으로 설계에 반영된 보안기술의 적정성을 검증하고 이를 적절하게 해결할 수 있는 개선 조치를 실시하였는지 여부 등을 고려하여 판단하여야 한다. 원고는 마이올레 홈페이지의 개발 당시부터 해킹사고에 이르기까지 오랜 기간 당시 정보보안의 기술 수준에 적합한 자동화된 점검 도구를 활용하거나 모의해킹을 수행하는 등 웹 취약점의 존재를 최소화하도록 하는 조치를 충분히 수행하였다.

4) 따라서 원고가 이 사건 해킹사고 중 마이올레 홈페이지 부분과 관련하여 이 사건 고시 제4조 제9항에 따른 보호조치의무를 위반하지 않았다고 본 원심 판단은 그 결론에 있어 정당한 것으로 수긍할 수 있다. 결국 이러한 원심 판단에 상고이유 주장과 같이 이 사건 고시 제4조 제9항에 관한 법리를 오해하여 판결에 영향을 미친 잘못이 없다.

2. 상고이유 제2점에 대하여

원심은 그 판시와 같은 이유로, 원고가 이 사건 해킹사고 중 올레클럽 홈페이지와 관련하여 이 사건 고시 제4조 제5항을 위반한 것으로 볼 수 없다고 판단하였다.

관련 법리에 비추어 기록을 살펴보면, 이러한 원심 판단에 상고이유 주장과 같이 이 사건 고시 제4조 제5항에 관한 법리를 오해한 잘못이 없다.

3. 상고이유 제3점에 대하여

원심은 그 판시와 같은 이유로 이 사건 처분사유 중 제4처분사유를 제외하고 제1 내지 3처분사유가 인정되지 않는다면 원고의 위반행위의 내용, 위반행위로 인한 개인정보의 피해규모, 구 정보통신망법 제28조 제1항에 따른 기술적·관리적 보호조치의 이행 정도 등에 차이가 나타나므로 피고가 원고의 위반행위를 '중대한 위반행위'로 평가하여 과징금을 산정한 것은 재량권을 일탈·남용한 것으로 볼 수 있다고 판단하였다.

관련 법리에 비추어 기록을 살펴보면, 이러한 원심 판단에 상고이유 주장과 같이 과징금 산정에 관한 재량권의 일탈·남용 판단 법리를 오해한 잘못이 없다.

4. 결론

그러므로 상고를 기각하고, 상고비용은 패소자가 부담하도록 하여, 관여 대법관의

일치된 의견으로 주문과 같이 판결한다.

재판장 대법관 이흥구

대법관 김재형

주 심 대법관 안철상

대법관 노정희