시정명령등처분취소청구의소

[서울행정법원 2021. 11. 12. 2020구합59628]

【전문】

【원 고】 주식회사 위메프 (소송대리인 변호사 양대권 외 2인)

【피 고】 개인정보보호위원회 (소송대리인 법무법인 민후 담당변호사 김경환 외 1인)

【변론종결】2021. 8. 27.

【주문】

】

1. 피고가 2019. 12. 27. 원고에 대하여 한 [별지 1] 처분 내역 기재 각 시정명령 및 과징금 부과처분 중 [별지 1] 처분 내역 기재 과징금 부과처분 부분을 취소한다.

2. 원고의 나머지 청구를 기각한다.

3. 소송비용 중 1/2은 원고가, 나머지는 피고가 각 부담한다.

【청구취지】 피고가 2019. 12. 27. 원고에 대하여 한 [별지 1] 처분 내역 기재 각 시정명령 및 과징금 납부명령을 모두 취소한다.

【이유】

】1. 처분의 경위

가. 원고는 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2020. 2. 4. 법률 제16955호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다) 제2조 제1항 제2호에 따른 정보통신서비스 제공자로서, 인터넷 및 모바일 어플리케이션을 통하여 제공되는 온라인 쇼핑몰인 '(쇼핑몰 명칭 생략)'(이하 '이 사건 쇼핑몰'이라 한다)를 운영하는 회사이다.

나. 원고는 2018. 11. 1. 특정 항목의 상품을 10만 원 이상 구매하는 고객에 대하여 50% 적립이용권을 배포하는 '블랙프라이스데이' 이벤트(이하 '이 사건 이벤트'라 한다)를 진행하면서, 일반 웹페이지를 통해 접속할 수 있는 이 사건 쇼핑몰 홈페이지에 적용되는 캐시 정책과는 별도로 모바일 웹을 통해 접속 가능한 이 사건 이벤트 페이지((홈페이지 주소 2 생략), 이하 '이 사건 이벤트 페이지'라 한다)에만 적용되는 캐시 정책(이하 '이 사건 캐시 정책'이라 한다)을 새로이 배포하였다.

다.

원고는 2018. 11. 2. 방송통신위원회에 이 사건 이벤트 페이지에 모바일 웹을 통해 로그인할 경우 다른 사람의 계정으로 로그인됨으로써 특정 페이지(마이페이지, 구매정보)에 접속할 수 있게 되어 20명의 이 사건 쇼핑몰 이용자의 개인정보가 노출(이하 '이 사건 사고'라 한다)되었다는 내용의 신고를 접수하였다.

라. 방송통신위원회(이하 처분의 주체로서 특정할 경우 '피고'라 한다)는 한국인터넷진흥원과 함께 2018. 11. 14. 원고에 대한 현장조사를 실시한 결과 원고가 아래와 같이 구 정보통신망법 제28조 제1항 제2호, 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2020. 3. 3. 대통령령 제30509호로 개정되기 전의 것, 이하 '구 정보통신망법 시행령'이라 한다) 제15조 제2항 제5호, 구 개인정보의 기술적·관리적 보호조치 기준(방송통신위원회고시 제2015-3호, 이하 '구 보호조치 기준'이라 한다) 제4조 제9항을 위반하여 이 사건 쇼핑몰 이용자의 개인정보를 유출한 것으로 보고, 2019. 12. 27. 원고에 대하여 구 정보통신망법 제64조 제4항, 제64조의3 제1항, 구 정보통신망법 시행령 제69조

의2 제1항, 제4항 관련 [별표 8], 구 개인정보보호 법규 위반에 대한 과징금 부과기준(방송통신위원회고시 제2015-30호, 이하 '구 과징금 부과기준'이라 한다) 등에 따라 [별지 1] 처분 내역 기재와 같이 시정명령 및 시정명령 이행결과의 보고(이하 '이 사건 각 시정명령'이라 한다), 과징금 18억 5,200만 원(이하 '이 사건 과징금'이라 한다) 등을 명하는 처분을 하였다(이하 '이 사건 각 시정명령' 부분을 '이 사건 각 시정명령 처분'이라 하고, '이 사건 과징금' 부분을 '이 사건 과징금 처분'이라 하며, '이 사건 각 시정명령 처분' 및 '이 사건 과징금 처분'을 통칭할 경우 '이 사건 각 처분'이라 한다).

Nginx(엔진엑스)

Fast CGI

쿠키정보

(자동로그인 토큰)

[인정근거] 다툼 없는 사실, 갑 제1, 2, 3, 4호증, 을 제1, 2, 3호증의 각 기재, 변론 전체의 취지

2. 이 사건 각 처분의 적법 여부

가. 원고의 주장

1) 처분사유 부존재

가) 이 사건 사고의 원인이 된 이 사건 캐시 정책은 모바일 '웹서버'에 적용된 것인데, '웹서버'는 개인정보를 데이터베이스 형태로 저장한 상태에서 이를 관리 및 운용하는 기능이 없어 구 정보통신망법, 구 정보통신망법 시행령에서 규정하는 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 '개인정보처리시스템'이라 한다)'에 해당하지 아니한다.

그럼에도 이 사건 캐시 정책이 적용된 '웹서버'가 구 보호조치 기준에 따라 보호조치의 대상이 되는 '개인정보처리시스템'에 해당함을 전제로 한 이 사건 각 처분은 위법하다.

나) 구 보호조치 기준 제4조 제9항은 같은 조 제1항 내지 제8항과 달리 개인정보 침해 등의 결과가 발생하지 않도록 하기 위한 구체적인 행위를 규정하고 있지 아니한 채 결과방지의무와 같은 추상적인 형식으로 조치의무를 부과하고 있는 일종의 백지 처벌 규정 혹은 백지 제재 조항에 해당하는바, 구 보호조치 기준 제4조 제9항을 위반하였음을 이유로 이 사건 각 처분을 하는 것은 구체적인 조치의무 위반에 대한 평가 없이 원고에게 결과책임을 묻는 것으로서 부당하다.

다) 원고는 그 동안 개인정보가 유·노출되는 사고를 방지하기 위해 구 정보통신망법 제28조 및 구 보호조치 기준 등에서 요구하는 필요한 조치를 모두 이행하여 왔을 뿐만 아니라, 이 사건 사고의 발생 가능성을 사전에 예견하고 이를 방지하는 것은 사실상 불가능하였다.

2) 이 사건 과징금 산정의 위법

가) 구 정보통신망법 제64조의3 제1항에서는 '위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

'고 규정하고 있을 뿐 '위반행위와 관련한 매출액'의 범위에 대하여 시행령 등 하위 법령에 위임하고 있지 아니함에도 구 정보통신망법 시행령 제69조의2 제1항 본문은 '위반행위와 관련한 매출액이란 해당 정보통신서비스 제공자등의 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액을 말한다.

'고 일률적으로 규정함으로써 위반행위와 시기적으로 무관한 매출액도 관련 매출액에 포함하고 있는바, 이 사건 과징금 처분의 근거 법령인 구 정보통신망법 시행령 제69조의2 제1항은 법률의 위임이 없거나, 법률의 위임 범위를 벗어나 법률유보원칙을 위반한 위법·무효인 규정이다.

나) 구 정보통신망법 시행령 제69조의2 제1항 및 구 과징금 부과기준 제4조의 규정에 의하더라도, 이 사건 사고의 내용이나 경위 등에 비추어 보면, 위반행위(이 사건 사고)와 직접 또는 간접적으로 영향을 받는 정보통신서비스의 범위는 이 사건 이벤트의 모바일 웹 서비스 부분으로 한정되어야 하는데, 이 사건 이벤트의 모바일 웹 서비스 부분만의 매출액은 산정하기 곤란하므로, 구 정보통신망법 제64조의3 제2항 단서에 따라 정액과징금이 부과되어야 한다.

그렇지 않다고 하더라도 과징금 부과기준이 되는 '위반행위와 관련된 매출액'(이하 '관련 매출액'이라 한다)은 이 사건 이벤트가 실시된 2018. 11. 1. 하루 동안 모바일 웹 서비스 부분에서 발행한 매출액인 208,940,210원이나, 2018. 11. 1. 이 사건 이벤트를 통해 발생한 전체 매출액(모바일 웹, 모바일 앱, PC 웹)인 2,765,073,510원을 기준으로 산정되어야 한다.

다) 이 사건 사고를 통해 유출된 개인정보의 이용자도 20명에 불과하였을 뿐만 아니라 이 사건 이벤트의 모바일 웹 서비스에 한정된 사고였고, 극히 이례적인 상황에서 개인정보 유출이 이루어진 점, 유출된 개인정보 내용도 이름, 연락처, 주소 및 이메일 주소에 한정되었던 점, 이 사건 쇼핑몰 이용자의 서비스 이용 상황에서 연결오류로 인해 발생한 사고로서 1대1 구조로만 개인정보가 유출된 점, 수백에서 수천만 건의 개인정보가 유출된 다른 사고들에 비하여 이 사건 과징금의 액수가 지나치게 다액인 점 등에 비추어 보면, 이 사건 과징금 처분에는 비례의 원칙 및 평등의 원칙을 위반하여 재량권을 일탈·남용한 위법이 있다.

나. 관계 법령

[별지 2] '관계 법령' 기재와 같다.

다.

판단

1) 인정사실

앞서 본 증거들에 갑 제8, 9, 10, 17, 18호증의 각 기재에 의하면, 다음과 같은 사실이 인정된다.

가) 이 사건 각 처분과정에서 작성된 2019년 제57차 방송통신위원회 심의·의결서의 주요 내용은 아래와 같다.

Ⅰ. 기초사실 원고는 영리를 목적으로 온라인 쇼핑몰(홈페이지 주소 1 생략) 서비스를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조 제1항 제3호에 따른 정보통신서비스 제공자이고, 원고의 일반현황 및 최근 3년간 매출액은 다음과 같다.

〈원고의 일반현황〉대표이사설립일자자본금주요서비스종업원 수('18. 11. 14. 기준)소외인2010. 5. 28.203억 원온라인 전자상거래1,778명

〈원고의 최근 3년간 매출액 현황〉(단위: 백만 원)구분2015년2016년2017년평균관련 매출액216,505369,098473,071352,891

Ⅱ. 사실조사 결과 2. 행위 사실 가. 개인정보 수집현황 원고 웹페이지(홈페이지 주소 1 생략) 및 모바일 앱(쇼핑몰 명칭 생략)으로 온라인 쇼핑몰 서비스를 제공하면서 2018. 11. 14. 기준으로 18,657,023건의 회원정보를 보유하고 있다.

〈원고의 개인정보 수집 현황〉구분항목수집일건수유효회원[필수] 이름, 생년월일, 이메일, 비밀번호, 휴대전화번호'10. 10. 7.~'18. 11. 14.10,926,651건[선택] 성별, 주소휴면회원상동7,730,372건계18,657,023건

나. 개인정보 유출 규모 및 경로 1) 개인정보 유출 규모 원고가 '온라인 전자상거래' 서비스를 운영하면서 수집한 회원의 개인정보 약 20건*이 타인에게 노출되었다.

* 20명의 이용자 개인정보가 해당 페이지에 로그인한 이용자 29명에게 노출됨

〈원고의 개인정보 유출현황〉구분유출항목건수(쇼핑몰 명칭 생략) 회원이름, 이메일, 휴대폰번호, 배송지 주소20건

2) 유출 경위 원고가 2018. 11. 1. 00:00에 새로운 캐시 정책을 적용한 '블랙프라이스데이' 이벤트 페이지(홈페이지 주소 2 생략)를 오픈하면서 캐시 설정 오류로 인하여 타인의 캐시 데이터를 받은 이용자가 특정 페이지(마이페이지, 구매정보)에 접속하면서 타인의 개인정보 총 20건이 노출되었다.

Ⅲ. 위법성 판단 2. 위법성 판단 가. 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출[정보통신망법 제28조(개인정보 보호조치) 중 개인정보 유·노출 방지조치]되지 않도록 조치를 취하지 않은 행위 구 보호조치 기준 제4조 제9항의 입법 목적은 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성하는 등 보안대책을 마련하여야 한다는 것이다.

원고가 PC web 이벤트 페이지에 대해서는 서버에서 Json을 캐싱하도록 설정하였으나(Html의 body 부분만 캐싱), mobile web 이벤트 페이지는 전체를 캐싱하도록 설정하였고, 이 과정에서 이용자를 식별할 수 있는 쿠키 값(wmp_web_token)마저 캐싱되어, 캐시 저장 후 1분 이내에 이벤트 페이지 접속시 타인의 캐시 데이터를 받은 이용자(29명)가 특정 페이지(마이페이지, 구매정보)에 접속하면서 타인의 정보(20명, 항목: 이름, 이메일, 휴대폰번호, 배송지 주소)가 열람권한 없는 자에게 공개되도록 한 행위는, 정보통신망법 제28조 제1항 제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조 제2항 제5호, 구 보호조치 기준 제4조 제9항을 위반한 것이다.

Ⅴ. 과징금 부과 원고는 정보통신망법 제64조의3 제1항 제6호에 따라 이용자의 개인정보가 분실·유출된 경우로서 개인정보 보호조치(제28조 제1항)를 하지 않은 경우에 해당하여, 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 부과할 수 있다.

원고의 정보통신망법 제28조 제1항 위반에 대한 과징금은 같은 법 제64조의3 제1항 제6호, 같은 법 시행령 제69조의2 제1항과 제4항 [별표 8] (과징금 산정기준과 산정절차) 및 구 과징금 부과기준에 따라 다음과 같이 부과한다.

1. 과징금의 상한액 및 기준금 가. 과징금 상한액 원고의 정보통신망법 제28조 제1항 위반에 대한 과징금 상한액은 같은 법 제64조의3 제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액 1) 고의·중과실 여부 이 사건 과징금 기준 제5조 제1항은, 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조 제1항에 따른 기술적

·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따를 때, ▲ 원고의 행위가 고의성이 없고 단순 과실로 보이는 점을 고려하면 원고에게 중과실이 있다고 보기 어렵다.

2) 중대성의 판단 구 과징금 기준 제5조 제2항은, 위반 정보통신서비스 제공자 등에게 고의·중과실이 없으면 위반행위의 중대성을 보통 위반행위로 판단한다고 규정하고 있다.

이에 따를 때 원고의 고의·중과실이 없으므로 '보통 위반행위'로 판단한다.

3) 기준금액 산출 원고는 위반행위와 관련된 매출액에 대해 개인정보 노출사건으로 인하여 직접 영향을 받은 서비스는 '블랙프라이스데이' 이벤트 모바일 웹 부문에 해당하고 이외에 간접적으로 영향을 받은 서비스를 특별히 산정하기 어려워 위반행위와 관련된 정보통신서비스 매출액은 '블랙프라이스데이' 이벤트 모바일 웹 부문 매출액으로 한정해야 하나, 해당 이벤트는 '18년에 처음 실시된 서비스로' 18년 직전 3개 사업연도의 매출액이 없어 매출액 산정이 곤란한 경우에 해당, 과징금을 부과하더라도 정액 과징금으로 부과하는 것이 타당하다는 의견을 제출하였으나, '블랙프라이스데이' 이벤트는 새로운 사업이 아닌 전체 쇼핑몰 사업의 일환으로 진행되었고 서비스 범위도 동일하여 위반행위 관련 매출액을 '블랙프라이스데이' 이벤트로 한정하여 산정하는 것은 부적절하므로, 위 의견을 수용하지 않았다.

이에 원고의 위반행위와 관련된 '(홈페이지 주소 1 생략)' 매출액을 위반행위와 관련된 매출로 하고, 위반행위와 관련된 직전 3개 사업여도의 연평균 매출액 352,891,867천 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '보통 위반행위'의 부과기준율 1천분의 15를 적용하여 기준금액을 5,293,378,005원으로 한다.

다.

필수적 가중 및 감경 구 과징금 부과기준 제6조와 제7조에 따라 원고 위반행위의 기간이 1년 이내 '단기 위반행위'에 해당하므로 기준금액을 유지하고, 최근 3년간 정보통신망법 제64조의3 제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 2,646,689,003원을 감경한다.

라. 추가적 가중 및 감경 구 과징금 기준 제8조에 따라 위반행위의 주도 여부, 위반행위에 대한 조사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따를 때, 원고가 ▲ 개인정보 유출사실을 자진 신고한 점, ▲ 조사에 성실히 협조한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 30에 해당하는 79,007,701원을 감경한다.

2. 과징금의 결정 원고의 정보통신망법 제28조(개인정보 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3 제1항 제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 구 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 1,852,682,392원이나, 최종 과징금 산출액이 1억 원 이상에 해당하여 백만 원 미만을 절사한 1,852,000,000원을 최종 과징금으로 결정한다.

나) 방송통신위원회와 한국인터넷진흥원에서 2017. 12. 발간한 개인정보의 기술적·관리적 보호조치 기준 해설서(이하 '이 사건 보호조치 기준 해설서'라 한다) 중 이 사건과 관련된 주요 내용은 아래와 같다.

Ⅰ. 개요구분개인정보의 기술적·관리적 보호조치 기준법적 근거○ 구 정보통신망법 제28조(개인정보의 보호조치)○ 구 정보통신망법 시행령 제15조(개인정보의 보호조치)적용대상○ 정보통신서비스 제공자○ 정보통신서비스 제공자로부터 개인정보를 제공받은 자○ 개인정보 수집·취급 등을 위탁받은 자(이하 '수탁자', 준용)○ 방송사업자(준용)목적○ 정보통신서비스 제공자 등이 이용자의 개인정보를 처리할 때 개인정보가 분실·도난·유출·위조·변조 또는 훼손되

는 것을 방지하고 개인정보의 안전성 확보를 위하여 필요한 보호조치의 기준을 정함성격○ 반드시 준수해야 하는 최소한의 기준주요 내용○ 내부관리계획의 수립·시행○ 접근통제○ 접속기록의 위·변조 방지○ 개인정보의 암호화○ 악성 프로그램 방지○ 물리적 접근 방지○ 출력·복사시 보호조치○ 개인정보 표시 제한 보호조치 등

2. 법적 근거 ○ 이 기준에 따른 기술적·관리적 조치를 하지 아니한 자 등에게는 관련 법률에 따라 과징금, 벌칙(징역 또는 벌금), 과태료를 부과할 수 있다.

?Ⅱ. 개인정보의 기술적·관리적 보호조치 기준 전문(중략)?Ⅲ. 개인정보의 기술적·관리적 보호조치 기준 해설 2. 정의

【이유】

】1. 처분의 경위

가. 원고는 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2020. 2. 4. 법률 제16955호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다) 제2조 제1항 제2호에 따른 정보통신서비스 제공자로서, 인터넷 및 모바일 어플리케이션을 통하여 제공되는 온라인 쇼핑몰인 '(쇼핑몰 명칭 생략)'(이하 '이 사건 쇼핑몰'이라 한다)를 운영하는 회사이다.

나. 원고는 2018. 11. 1. 특정 항목의 상품을 10만 원 이상 구매하는 고객에 대하여 50% 적립이용권을 배포하는 '블랙프라이스데이' 이벤트(이하 '이 사건 이벤트'라 한다)를 진행하면서, 일반 웹페이지를 통해 접속할 수 있는 이 사건 쇼핑몰 홈페이지에 적용되는 캐시 정책과는 별도로 모바일 웹을 통해 접속 가능한 이 사건 이벤트 페이지((홈페이지 주소 2 생략), 이하 '이 사건 이벤트 페이지'라 한다)에만 적용되는 캐시 정책(이하 '이 사건 캐시 정책'이라 한다)을 새로이 배포하였다.

다.

원고는 2018. 11. 2. 방송통신위원회에 이 사건 이벤트 페이지에 모바일 웹을 통해 로그인할 경우 다른 사람의 계정으로 로그인됨으로써 특정 페이지(마이페이지, 구매정보)에 접속할 수 있게 되어 20명의 이 사건 쇼핑몰 이용자의 개인정보가 노출(이하 '이 사건 사고'라 한다)되었다는 내용의 신고를 접수하였다.

라. 방송통신위원회(이하 처분의 주체로서 특정할 경우 '피고'라 한다)는 한국인터넷진흥원과 함께 2018. 11. 14. 원고에 대한 현장조사를 실시한 결과 원고가 아래와 같이 구 정보통신망법 제28조 제1항 제2호, 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2020. 3. 3. 대통령령 제30509호로 개정되기 전의 것, 이하 '구 정보통신망법 시행령'이라 한다) 제15조 제2항 제5호, 구 개인정보의 기술적·관리적 보호조치 기준(방송통신위원회고시 제2015-3호, 이하 '구 보호조치 기준'이라 한다) 제4조 제9항을 위반하여 이 사건 쇼핑몰 이용자의 개인정보를 유출한 것으로 보고, 2019. 12. 27. 원고에 대하여 구 정보통신망법 제64조 제4항, 제64조의3 제1항, 구 정보통신망법 시행령 제69조의2 제1항, 제4항 관련 [별표 8], 구 개인정보보호 법규 위반에 대한 과징금 부과기준(방송통신위원회고시 제2015-30호, 이하 '구 과징금 부과기준'이라 한다) 등에 따라 [별지 1] 처분 내역 기재와 같이 시정명령 및 시정명령 이행결과의 보고(이하 '이 사건 각 시정명령'이라 한다), 과징금 18억 5,200만 원(이하 '이 사건 과징금'이라 한다) 등을 명하는 처분을 하였다(이하 '이 사건 각 시정명령' 부분을 '이 사건 각 시정명령 처분'이라 하고, '이 사건 과징금' 부분을 '이 사건 과징금 처분'이라 하며, '이 사건 각 시정명령 처분' 및 '이 사건 과징금 처분'을 통칭할 경우 '이 사건 각 처분'이라 한다).

Nginx(엔진엑스)

Fast CGI

쿠키정보

(자동로그인 토큰)

[인정근거] 다툼 없는 사실, 갑 제1, 2, 3, 4호증, 을 제1, 2, 3호증의 각 기재, 변론 전체의 취지

2. 이 사건 각 처분의 적법 여부

가. 원고의 주장

1) 처분사유 부존재

가) 이 사건 사고의 원인이 된 이 사건 캐시 정책은 모바일 '웹서버'에 적용된 것인데, '웹서버'는 개인정보를 데이터베이스 형태로 저장한 상태에서 이를 관리 및 운용하는 기능이 없어 구 정보통신망법, 구 정보통신망법 시행령에서 규정하는 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 '개인정보처리시스템'이라 한다)'에 해당하지 아니한다.

그럼에도 이 사건 캐시 정책이 적용된 '웹서버'가 구 보호조치 기준에 따라 보호조치의 대상이 되는 '개인정보처리시스템'에 해당함을 전제로 한 이 사건 각 처분은 위법하다.

나) 구 보호조치 기준 제4조 제9항은 같은 조 제1항 내지 제8항과 달리 개인정보 침해 등의 결과가 발생하지 않도록 하기 위한 구체적인 행위를 규정하고 있지 아니한 채 결과방지의무와 같은 추상적인 형식으로 조치의무를 부과하고 있는 일종의 백지 처벌 규정 혹은 백지 제재 조항에 해당하는바, 구 보호조치 기준 제4조 제9항을 위반하였음을 이유로 이 사건 각 처분을 하는 것은 구체적인 조치의무 위반에 대한 평가 없이 원고에게 결과책임을 묻는 것으로서 부당하다.

다) 원고는 그 동안 개인정보가 유·노출되는 사고를 방지하기 위해 구 정보통신망법 제28조 및 구 보호조치 기준 등에서 요구하는 필요한 조치를 모두 이행하여 왔을 뿐만 아니라, 이 사건 사고의 발생 가능성을 사전에 예견하고 이를 방지하는 것은 사실상 불가능하였다.

2) 이 사건 과징금 산정의 위법

가) 구 정보통신망법 제64조의3 제1항에서는 '위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

'고 규정하고 있을 뿐 '위반행위와 관련한 매출액'의 범위에 대하여 시행령 등 하위 법령에 위임하고 있지 아니함에도 구 정보통신망법 시행령 제69조의2 제1항 본문은 '위반행위와 관련한 매출액이란 해당 정보통신서비스 제공자등의 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액을 말한다.

'고 일률적으로 규정함으로써 위반행위와 시기적으로 무관한 매출액도 관련 매출액에 포함하고 있는바, 이 사건 과징금 처분의 근거 법령인 구 정보통신망법 시행령 제69조의2 제1항은 법률의 위임이 없거나, 법률의 위임 범위를 벗어나 법률유보원칙을 위반한 위법·무효인 규정이다.

나) 구 정보통신망법 시행령 제69조의2 제1항 및 구 과징금 부과기준 제4조의 규정에 의하더라도, 이 사건 사고의 내용이나 경위 등에 비추어 보면, 위반행위(이 사건 사고)와 직접 또는 간접적으로 영향을 받는 정보통신서비스의 범위는 이 사건 이벤트의 모바일 웹 서비스 부분으로 한정되어야 하는데, 이 사건 이벤트의 모바일 웹 서비스 부분만의 매출액은 산정하기 곤란하므로, 구 정보통신망법 제64조의3 제2항 단서에 따라 정액과징금이 부과되어야 한다.

그렇지 않다고 하더라도 과징금 부과기준이 되는 '위반행위와 관련된 매출액'(이하 '관련 매출액'이라 한다)은 이 사건 이벤트가 실시된 2018. 11. 1. 하루 동안 모바일 웹 서비스 부분에서 발행한 매출액인 208,940,210원이나, 2018. 11. 1. 이 사건 이벤트를 통해 발생한 전체 매출액(모바일 웹, 모바일 앱, PC 웹)인 2,765,073,510원을 기준으로 산정되어야 한다.

다) 이 사건 사고를 통해 유출된 개인정보의 이용자도 20명에 불과하였을 뿐만 아니라 이 사건 이벤트의 모바일 웹 서비스에 한정된 사고였고, 극히 이례적인 상황에서 개인정보 유출이 이루어진 점, 유출된 개인정보 내용도 이름, 연락처, 주소 및 이메일 주소에 한정되었던 점, 이 사건 쇼핑몰 이용자의 서비스 이용 상황에서 연결오류로 인해 발생한 사고로서 1대1 구조로만 개인정보가 유출된 점, 수백에서 수천만 건의 개인정보가 유출된 다른 사고들에 비하여 이 사건 과징금의 액수가 지나치게 다액인 점 등에 비추어 보면, 이 사건 과징금 처분에는 비례의 원칙 및 평등의 원칙을 위반하여 재량권을 일탈·남용한 위법이 있다.

나. 관계 법령

[별지 2] '관계 법령' 기재와 같다.

다.

판단

1) 인정사실

앞서 본 증거들에 갑 제8, 9, 10, 17, 18호증의 각 기재에 의하면, 다음과 같은 사실이 인정된다.

가) 이 사건 각 처분과정에서 작성된 2019년 제57차 방송통신위원회 심의·의결서의 주요 내용은 아래와 같다.

Ⅰ. 기초사실 원고는 영리를 목적으로 온라인 쇼핑몰(홈페이지 주소 1 생략) 서비스를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조 제1항 제3호에 따른 정보통신서비스 제공자이고, 원고의 일반현황 및 최근 3년간 매출액은 다음과 같다.

〈원고의 일반현황〉대표이사설립일자자본금주요서비스종업원 수('18. 11. 14. 기준)소외인2010. 5. 28.203억 원온라인 전자상거래1,778명

〈원고의 최근 3년간 매출액 현황〉(단위: 백만 원)구분2015년2016년2017년평균관련 매출액216,505369,098473,071352,891

Ⅱ. 사실조사 결과 2. 행위 사실 가. 개인정보 수집현황 원고 웹페이지(홈페이지 주소 1 생략) 및 모바일 앱(쇼핑몰 명칭 생략)으로 온라인 쇼핑몰 서비스를 제공하면서 2018. 11. 14. 기준으로 18,657,023건의 회원정보를 보유하고 있다.

〈원고의 개인정보 수집 현황〉구분항목수집일건수유효회원[필수] 이름, 생년월일, 이메일, 비밀번호, 휴대전화번호'10. 10. 7.~'18. 11. 14.10,926,651건[선택] 성별, 주소휴면회원상동7,730,372건계18,657,023건

나. 개인정보 유출 규모 및 경로 1) 개인정보 유출 규모 원고가 '온라인 전자상거래' 서비스를 운영하면서 수집한 회원의 개인정보 약 20건*이 타인에게 노출되었다.

* 20명의 이용자 개인정보가 해당 페이지에 로그인한 이용자 29명에게 노출됨

〈원고의 개인정보 유출현황〉구분유출항목건수(쇼핑몰 명칭 생략) 회원이름, 이메일, 휴대폰번호, 배송지 주소20건

2) 유출 경위 원고가 2018. 11. 1. 00:00에 새로운 캐시 정책을 적용한 '블랙프라이스데이' 이벤트 페이지(홈페이지 주소 2 생략)를 오픈하면서 캐시 설정 오류로 인하여 타인의 캐시 데이터를 받은 이용자가 특정 페이지(마이페이지, 구매정보)에 접속하면서 타인의 개인정보 총 20건이 노출되었다.

Ⅲ. 위법성 판단 2. 위법성 판단 가. 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출[정보통신망법 제28조(개인정보 보호조치) 중 개인정보 유·노출 방지조치]되지 않도록 조치를 취하지 않은 행위 구 보호조치 기준 제4조 제9항의 입법 목적은 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성하는 등 보안대책을 마련하여야 한다는 것이다.

원고가 PC web 이벤트 페이지에 대해서는 서버에서 Json을 캐싱하도록 설정하였으나(Html의 body 부분만 캐싱), mobile web 이벤트 페이지는 전체를 캐싱하도록 설정하였고, 이 과정에서 이용자를 식별할 수 있는 쿠키 값(wmp_web_token)마저 캐싱되어, 캐시 저장 후 1분 이내에 이벤트 페이지 접속시 타인의 캐시 데이터를 받은 이용자(29명)가 특정 페이지(마이페이지, 구매정보)에 접속하면서 타인의 정보(20명, 항목: 이름, 이메일, 휴대폰번호, 배송지 주소)가 열람권한 없는 자에게 공개되도록 한 행위는, 정보통신망법 제28조 제1항 제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조 제2항 제5호, 구 보호조치 기준 제4조 제9항을 위반한 것이다.

Ⅴ. 과징금 부과 원고는 정보통신망법 제64조의3 제1항 제6호에 따라 이용자의 개인정보가 분실·유출된 경우로서 개인정보 보호조치(제28조 제1항)를 하지 않은 경우에 해당하여, 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 부과할 수 있다.

원고의 정보통신망법 제28조 제1항 위반에 대한 과징금은 같은 법 제64조의3 제1항 제6호, 같은 법 시행령 제69조의2 제1항과 제4항 [별표 8] (과징금 산정기준과 산정절차) 및 구 과징금 부과기준에 따라 다음과 같이 부과한다.

1. 과징금의 상한액 및 기준금 가. 과징금 상한액 원고의 정보통신망법 제28조 제1항 위반에 대한 과징금 상한액은 같은 법 제64조의3 제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액 1) 고의·중과실 여부 이 사건 과징금 기준 제5조 제1항은, 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조 제1항에 따른 기술적·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따를 때, ▲ 원고의 행위가 고의성이 없고 단순 과실로 보이는 점을 고려하면 원고에게 중과실이 있다고 보기 어렵다.

2) 중대성의 판단 구 과징금 기준 제5조 제2항은, 위반 정보통신서비스 제공자 등에게 고의·중과실이 없으면 위반행위의 중대성을 보통 위반행위로 판단한다고 규정하고 있다.

이에 따를 때 원고의 고의·중과실이 없으므로 '보통 위반행위'로 판단한다.

3) 기준금액 산출 원고는 위반행위와 관련된 매출액에 대해 개인정보 노출사건으로 인하여 직접 영향을 받은 서비스는 '블랙프라이스데이' 이벤트 모바일 웹 부문에 해당하고 이외에 간접적으로 영향을 받은 서비스를 특별히 산정하기

어려워 위반행위와 관련된 정보통신서비스 매출액은 '블랙프라이스데이' 이벤트 모바일 웹 부문 매출액으로 한정해야 하나, 해당 이벤트는 '18년에 처음 실시된 서비스로' 18년 직전 3개 사업연도의 매출액이 없어 매출액 산정이 곤란한 경우에 해당, 과징금을 부과하더라도 정액 과징금으로 부과하는 것이 타당하다는 의견을 제출하였으나, '블랙프라이스데이' 이벤트는 새로운 사업이 아닌 전체 쇼핑몰 사업의 일환으로 진행되었고 서비스 범위도 동일하여 위반행위 관련 매출액을 '블랙프라이스데이' 이벤트로 한정하여 산정하는 것은 부적절하므로, 위 의견을 수용하지 않았다.

이에 원고의 위반행위와 관련된 '(홈페이지 주소 1 생략)' 매출액을 위반행위와 관련된 매출로 하고, 위반행위와 관련된 직전 3개 사업여도의 연평균 매출액 352,891,867천 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '보통 위반행위'의 부과기준율 1천분의 15를 적용하여 기준금액을 5,293,378,005원으로 한다.

다.

필수적 가중 및 감경 구 과징금 부과기준 제6조와 제7조에 따라 원고 위반행위의 기간이 1년 이내 '단기 위반행위'에 해당하므로 기준금액을 유지하고, 최근 3년간 정보통신망법 제64조의3 제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 2,646,689,003원을 감경한다.

라. 추가적 가중 및 감경 구 과징금 기준 제8조에 따라 위반행위의 주도 여부, 위반행위에 대한 조사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따를 때, 원고가 ▲ 개인정보 유출사실을 자진 신고한 점, ▲ 조사에 성실히 협조한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 30에 해당하는 79,007,701원을 감경한다.

2. 과징금의 결정 원고의 정보통신망법 제28조(개인정보 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3 제1항 제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 구 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 1,852,682,392원이나, 최종 과징금 산출액이 1억 원 이상에 해당하여 백만 원 미만을 절사한 1,852,000,000원을 최종 과징금으로 결정한다.

나) 방송통신위원회와 한국인터넷진흥원에서 2017. 12. 발간한 개인정보의 기술적·관리적 보호조치 기준 해설서(이하 '이 사건 보호조치 기준 해설서'라 한다) 중 이 사건과 관련된 주요 내용은 아래와 같다.

Ⅰ. 개요구분개인정보의 기술적·관리적 보호조치 기준법적 근거○ 구 정보통신망법 제28조(개인정보의 보호조치)○ 구 정보통신망법 시행령 제15조(개인정보의 보호조치)적용대상○ 정보통신서비스 제공자○ 정보통신서비스 제공자로부터 개인정보를 제공받은 자○ 개인정보 수집·취급 등을 위탁받은 자(이하 '수탁자', 준용)○ 방송사업자(준용)목적○ 정보통신서비스 제공자 등이 이용자의 개인정보를 처리할 때 개인정보가 분실·도난·유출·위조·변조 또는 훼손되는 것을 방지하고 개인정보의 안전성 확보를 위하여 필요한 보호조치의 기준을 정함성격○ 반드시 준수해야 하는 최소한의 기준주요 내용○ 내부관리계획의 수립·시행○ 접근통제○ 접속기록의 위·변조 방지○ 개인정보의 암호화○ 악성 프로그램 방지○ 물리적 접근 방지○ 출력·복사시 보호조치○ 개인정보 표시 제한 보호조치 등

2. 법적 근거 ○ 이 기준에 따른 기술적·관리적 조치를 하지 아니한 자 등에게는 관련 법률에 따라 과징금, 벌칙(징역 또는 벌금), 과태료를 부과할 수 있다.

?Ⅱ. 개인정보의 기술적·관리적 보호조치 기준 전문(중략)?Ⅲ. 개인정보의 기술적·관리적 보호조치 기준 해설 2. 정의