

개인정보보호법상 과징금 제도의 정합성 확보를 위한 개선 과제

홍대식 (서강대학교 법학전문대학원 교수 / ICT 법경제연구소장)

1. 머리말: 개인정보보호법상 과징금 제도의 변화와 새로운 과제

최근 우리 「개인정보 보호법」은 중대한 구조적 변화를 겪었다. 특히 2023 년 3 월 개정되어 동년 9 월에 전면 시행된 개정법은 과징금 부과 상한의 기준을 기존의 정액이나 '위반행위 관련 매출액'에서 기업의 규모와 직결되는 '전체 매출액(위반행위와 관련 없는 매출액 제외)'으로 일원화하였다. 법정 상한을 전체 매출액의 100 분의 3(3%)으로 설정하고, 고의 또는 중과실이 개입되거나 가중 사유에 해당할 경우 상한을 상향 조정할 수 있도록 한 조치는 개인정보 처리의 투명성과 안전성을 강제하는 강력한 이정표가 되었다.

다만 개인정보 침해와 무관한 사업 부문의 매출액까지 처분의 산정 변수로 포함시키는 일원화 방식에 대해서는, 헌법상 비례의 원칙과 과잉금지의 원칙, 그리고 자기책임의 원칙을 침해하다는 문제 제기가 가능하다. 따라서 이 글에서는 수범 주체에게 합리적이고 정당한 규율을 제공하면서도 법 목적을 정합적으로 달성하기 위하여, 개인정보보호법상 과징금 목적의 특수성을 규명하고, 일정한 추정 반복 예외를 전제로 한 전체 매출액 기준의 정당성 확보 방안과 과징금 산정기준의 합리적 설계 방안을 제안하고자 한다. 특히 개인정보처리자의 안전성 확보조치 의무 미이행과 실제 개인정보 유출이라는 결과 간의 '관련성' 평가 방식과 이를 산정에 반영하는 구체적 설계 메커니즘을 심도 있게 분석하고자 한다.

2. 개인정보보호법상 과징금 목적의 특수성과 제재의 정당성

과징금의 역사적 기원과 정당성은 경제적 이익을 목적으로 삼는 「독점규제 및 공정거래에 관한 법률」(공정거래법)상 경쟁법 위반행위에서 찾을 수 있다. 경쟁법상 과징금은 위법한 공동행위나 독점력 남용으로 얻은 부당이득을 박탈하는 '부당이득 환수적 성격'에 위반행위를 억제하기 위한 '행정상의 제재적 성격'이 강하게 결합되어 있다. 이 경우 위반행위 관련 매출액은 사회적 피해와 부당이득의 훌륭한 대리변수로 작동한다.

반면, 개인정보보호법 위반행위—특히 해킹 등 외부 침해에 따른 개인정보 유출 사고—는 이러한 모델을 평면적으로 이식하기 곤란한 목적과 성격의 특수성을 지닌다. 유출 사고가 발생한 상황에서 대다수의 사업자는 경제적 이익을 취하지 않으며, 오히려 제 3 자의 고도화된 해킹 기법에 의한 피해자적 위치에 놓이는 경우가 빈번하다. 즉, 안전성 확보조치(법 제 29 조) 위반으로 인해 매출액이 증대되거나 직접적인 불법 이익을 취득하는 구조가 형성되지 않는다는 의미이다.

대법원은 위메프 판결(대법원 2023.10.12. 선고 2022 두 68923 판결)에서, 개인정보 유출 시 박탈하려는 이득을 '위반행위 자체로 얻은 증가된 매출액'이 아니라, '적절한 보호조치를 취하지 않은 상태의 개인정보를 자신의 영업을 위해 보유함으로써 얻은 이득'으로 변형하여 판시함으로써 정당성을 우회 확보하고자 하였다. 그러나 이러한 해석은 과징금을 실질적으로 '행정적 제재(순수 제재금)'로 성격 규정하는 결과를 낳는다. 따라서 개인정보보호법상 과징금의 본질적 지위는 부당이득의 기계적 환수보다는 행정 의무 준수 제고 및 침해 예방, 그리고 사회적 위험의 억제라는 특수한 행정적 공익에서 구해야 한다. 이러한 목적의 특수성을 도외시하고 공정거래법과 같은 매출액 비례 산정을 획일적으로 강제할 경우 규제 수단과 목적 간의 불합리를 야기한다.

3. 일정한 예외를 전제로 한 '전체 매출액' 기준의 필요성과 한계

개정법상 '전체 매출액' 상한은 원천적으로 정당한 설계적 배경을 가진다. 법정 과징금 상한액을 규정하는 본질적 취지는 해당 처분이 사업자의 감당 능력을 완전히 일탈하여 기업 파산에 따른 심각한 사회적 비용(social cost of bankruptcy)을 유발하지 않도록 일종의 안전장치를 설정하는 데

있다. 즉, 대기업과 소상공인 등 기업 규모와 부담 한도에 비례하도록 상한을 전체 매출액의 일정 비율로 연동하는 것이다.

그러나 이는 어디까지나 '이론적인 법정 상한액'이어야 하며, 구체적인 과징금의 출발이 되는 '기준금액(기본 산정기준)' 자체가 당연히 전체 매출액에 일정 비율을 곱한 기계적 고정식으로 정립되어서는 안 된다. 헌법재판소는 일찍이 공정거래법상 부당지원행위 과징금 합헌 결정(헌법재판소 2003. 7. 24. 선고 2001 헌가 25 결정)에서, 법상 상한은 전체 매출액이라 하더라도 실제 산출의 토대가 되는 기준금액은 '지원금액'이라는 관련 변수를 사용하고 있음을 가리켜 '이중적 제한 장치'라고 칭하며 합헌성을 인정한 바 있다. 개인정보보호법 역시 법상 상한은 전체 매출액의 3%로 두어 한계선을 설정하되, 기준 산출 시에는 '개인정보 처리 및 의무 위반행위와 실질적 관련성이 있는 범위의 매출액'을 출발점으로 삼아야만 책임원칙에 부합한다.

현행 법 제제 64 조의 2 제 3 항, 시행령 제 60 조의 2 제 3 항이 위반행위와 관련 없는 매출액을 증명하여 차감하는 예외 규정을 두고는 있으나, 이는 수범자(기업)에게 '자기에게 위반과 상관이 없는 소극적 사실'을 입증하도록 하는 입증책임의 전환을 내포하는 한계를 가진다. 만일 기업의 입증이 미흡하다 하여 관련이 극히 희박한 제조업 매출이나 타 사업 부문 매출까지 무차별적으로 포함시킬 경우, 비례의 원칙에 위배되어 사법부의 사법심사를 통과하기 어려울 것이다. 따라서 처분 당국(개인정보보호위원회)이 관련성 영역의 범위를 일차적으로 합리적으로 제한·확정하고, 세부적인 추정 반복의 예외 장치가 상호 간 정교하게 작동하도록 행정 절차적 정합성이 확보되어야 한다.

4. 안전성 확보조치 위반과 유출 간 '관련성(Correlation)'의 의미와 그 평가

법 제 64 조의 2 제 4 항 제 5 호 및 시행령 규정은 개인정보 유출 시 '위반행위와의 관련성 및 유출 규모'를 과징금 부과에 필수적 고려사항으로 적시하고 있다. 과거 사법부는 인터파크 사건(서울고등법원 2019. 11. 1. 선고 2018 누 56291 판결) 등에서 개정 법문의 문언 변화를 근거로 유출이라는 결과와 기술적 조치 미이행 간의 '엄격한 인과관계(Causation)'는 불필요하다고

해석하였다. 그러나 이러한 해석은 자칫 행정 편의적인 무과실 결과책임주의로 경도될 고유의 법적 위험을 안고 있다.

헌법상 자기책임의 원칙을 관철하고 규제의 정당성을 확보하기 위해서는 인과관계까지는 아니더라도 적어도 특정 안전조치 미이행과 개인정보 유출 결과 사이에 일정한 선행의 관련성, 즉 '규범적 상관관계(Correlation)'가 반드시 충족되어야 한다. 헌법재판소 역시 2022 년 합헌 결정(헌법재판소 2022. 5. 26. 선고 2020 헌바 259 결정)에서 '조치의무를 성실히 이행하였다면 유출이 발생했더라도 과징금 대상이 되지 않는다'는 전제 하에 책임 한계를 유추 판시한 바 있다. 즉, 관련성 평가의 규범적 뼈대는 외부 해커의 침투 경로, 이용된 기법, 표적 시스템의 취약점, 그리고 위반으로 지적된 특정 안전조치 항목 간의 기술적·구조적 일치성이 담보되는가에 달려 있다.

대법원(2021. 8. 19. 선고 2018 두 56404 판결, KT 사건) 역시 침투 기법과 시스템 취약점 간의 구체적 조화 여부를 엄격히 따져 합리적 기대 수준의 안전성 확보조치 이행 여부를 판단하였다. 과거 방송통신위원회나 보호위의 실무례(홈플러스 2020, 아디다스 2022)에서 유출 경로가 종국적으로 불명으로 드러난 경우 과징금을 무리하게 부과하지 않았던 선례는 규범적 상관관계와 처분사유 특정 원칙을 균형 있게 고려한 사례였다.

5. 관련성 정도를 정량적으로 반영한 과징금 산정기준의 합리적 설계 방안

이러한 안전조치 의무 위반행위와 유출 결과 간의 관련성 정도와 수범자 특성을 실제 과징금 산정 공식에 정량적으로 이식할 수 있는 제도적 대안을 고안할 필요가 있다. 이를 위해서 해외 감독기구의 선진 모델¹에 기초하여 구체적 설계 방안을 마련할 것을 제안한다.

¹ 이와 같은 산정 모델의 구체적 내용은 홍대식/심연우/박준영, 개인정보보호법상 과징금 부과 실효성 확보 방안, 서강대학교 산학협력단, 개인정보보호위원회 연구용역 보고서 (2022. 9.), 79~96 면.

독일 개인정보보호연합회(DSK)의 4 단계 산정 모델은 수범자의 연 총매출액을 기준으로 영세·소·중·대기업으로 세분화한 후, 각 카테고리의 평균 매출액을 일일 요율(1/360)로 쪼개어 여기에 '침해 중대성 가중치(Multiplier)'를 선형적으로 곱하는 정량적 매트릭스를 활용한다. 또한 영국 개인정보보호청(ICO)의 4 단계 모델은 침해 행위의 '중대성(Seriousness)' 4 단계와 위반자의 주관적 '귀책성(Degree of Culpability)' 3 단계를 완벽하게 교차시킨 12 개의 백분율(Starting Point) 범주 매트릭스를 운영한다. 우리도 획일화된 4 단계 부과비율에 무작정 가감 조정을 할 것이 아니라, 이처럼 '중대성-책임성-관련성 강도'를 정밀하게 결합한 3 차원 매트릭스 모형을 법제화해야 과징금의 행정정당성과 비례성을 고도화할 수 있다.

더불어, 매출액 산정이 불가능하거나 부재한 수범 주체(공공기관, 비영리단체, 영세 개인)에 대한 형평성 보완책이 요구된다. 매출액이 없거나 산정이 곤란한 사업자에 대한 일률적 20 억 원 한도는 대형 공공기관에게는 지극히 경미한 질서벌에 불과하지만 중소 비영리단체에는 즉각적인 사멸을 뜻한다. 공공기관의 경우 공정거래법 사업자단체 규정을 모방하여 '연간 예산액 규모'를 과징금 산출의 대리변수로 적용하거나 별도의 전용 가중 상한 체계를 설계함으로써 형평성 격차를 시정해야 한다.

6. 결론

개인정보 보호라는 헌법적 가치는 단순히 사업자를 파산에 가깝게 징벌하는 사후 가중 처벌 방식만으로 수호되지 않는다. 비합리적이고 불명확한 결과책임적 과징금 집행은 규제 당국과 경제 수범자 간의 끝없는 사법 소송과 방어 비용의 기형적 팽창만을 부를 뿐이다. 과징금 산정의 합리성을 회복하는 것은 개인정보 행정 제재의 비범죄화(Decriminalization)를 이루고, 행정적 강제력의 도덕적 신뢰를 복원하기 위한 선결 과제이다.

마지막으로, 징수된 막대한 과징금 재원이 정작 유출의 직접적 피해 당사자인 '정보주체(국민)'의 사적 구제에는 한 톨도 환원되지 않은 채 일반 국고 회계로 흡수되는 모순을 정비해야 한다. 아울러 공정거래법상 제도를 벤치마킹하여 기업이 고의나 중과실이 없는 한, 대규모 예산을 행정 소송이 아닌 자발적인 사전 피해 복구 및 혁신적인 정보보안 설비 구축에 재투입할 것을 약속하면 과징금

처분을 합리적으로 완화해 주는 '동의의결제도'를 적극 연계해야 한다. 이러한 유연하고 정교한 다원적 규율 패러다임으로 전환될 때, 비로소 예방 중심의 고도 데이터 안심 사회라는 국가적 이념이 구현될 수 있을 것이다.