ESG 경영 시대의 CPO의 역할과 지위

홍대식 교수(서강대학교 법학전문대학원)

기업은 영업활동을 통해 영리를 추구하는 단체이다. 따라서 기업을 구성하는 가장 기본적인 조직은 영업활동을 수행하는 조직이다. 그런데 기업이 수행하는 영업활동은 주주 또는 사원, 채권자, 근로자는 물론 거래상대방, 경쟁자와 소비자에게 영향을 미치고, 영업활동의 성격에 따라서는 지역사회와 사회적, 문화적, 자연적 환경에도 일정한 영향을 미칠 수 있다. 이런 이유로 기업법의 영역에서는 기업의 지배구조와 관련하여 전통적인 주주자본주의의 한계를 극복하기 위한 이해관계자자본주의라는 이념이 발전하였고, 기업 경영의 관심사를 사회적으로 확대하는 사회적 책임론도 한때 유행하였다. 최근에는 그 동안 논의된 기업 경영의 핵심 지표를 통합한 ESG(Environment, Social and Governance) 경영이라는 개념이 자리를 잡아가고 있다.

그럼에도 불구하고 기업의 영업활동을 수행하는 조직이 영리 추구만을 우선적인 목표로 설정하고 주주나 이해관계자 나아가 사회에 미치는 영향에 대한 배려를 소홀히 할 경우 그 기업의 영업활동은 이해충돌을 넘어 사회적 해악을 일으킬 수 있다. 기업의 영업활동 수행 조직을 견제하고 감독하기 위하여 생성되고 제도화된 수많은 대내외적 통제 메커니즘은 기본적으로 기업의 영업활동이 갖는 이러한 외부효과의 속성에 대처하기 위한 것이다. 기업의 일반적인 영업활동과 관련된 내부 감독기구인 감사 또는 감사위원회 제도와 외부 감독기구인 외부감사인 제도가 대표적이다. 기업법 영역에서는 내부 통제 강화를 위해 2011년 상법 개정을 통해 준법통제기준 및 준법지원인 제도를 도입되었고, 감사(감사위원회) 기능과 내부회계관리제도 강화, 주기적 지정제를 통한 외부감사인의 독립성 제고 등 기업 내부의 자율적 감독기능의 효과성을 담보하기 위한 제도적 개선이 꾸준히 이루어지고 있다.

우리나라 개인정보보호법에 규정된 개인정보보호 책임자 제도는 이런 맥락에서 그 의의를 이해할 수 있다. 이 제도는 2001년 정보통신서비스제공자와 그로부터 이용자의 개인정보를 제공받는 자를 수범자로 하여 개인정보관리책임자를 지정하도록 의무화하는 규정으로 처음 도입된 후, 명칭 변경과 개인정보보호법과 정보통신망법에 모두 규정된 이원적인 제도를 거쳐 2020년 데이터 3법의 개정에 따라 개인정보보호법에 규정된 제도로 일원화되었다. 흔히 CPO로 불리는 개인정보보호 책임자를 지정할 의무는 모든 개인정보처리자에게 부과된 것이므로, 특히 개인정보처리자인 기업의 경우 조직 내의 누군가가 CPO의 직책을 맡아 법에서 명하는 업무를 수행해야 한다. 주의할 점은 법에서 명하는 업무가 반드시 기업의 영업활동 수행의 목표인 영리 추구에 단기적으로는 부합하지 않을 수 있다는 점이다. 개인정보 처리를 통한 서비스를 주된 영업활동으로 하는 기업 경영자가 영리 추구만을 우선적인 목표로 설정할 경우 개인정보보호를 위한 투자와 배려를 그의 선의에만 기댈 수는 없다. 모든 기업 경영자가 개인정보보호에 관한 지식과 전문성도 갖출 것을

기대하기도 어렵지만, 개인정보 처리가 영업활동을 통한 수익 창출에 큰 비중을 차지하는 기업의 경영자라면 처리 비용을 줄이면서 그 효과는 극대화하려는 유혹을 받지 않을 수 없기 때문이다. 그래서 기업 경영자가 개인정보 처리에 관하여 잘못된 의사결정을 하거나 사고를 일으키지 않도록 사전에 예방, 통제하고 조직 내부의 개인정보 처리 업무를 개선하는 역할을 담당할 사람이 꼭 필요하다. 이런 역할을 하는 사람이 다름아닌 CPO이다. 기업의 영업활동이 무엇인가에 따라 그 역할이 기업 내에서 갖는 비중은 달라질 수 있지만, 개인정보보호법에서 모든 개인정보처리자에게 CPO 지정의무를 부과한 이유도 여기에서 찾을 수 있다.

이처럼 개인정보처리자인 기업이라면 반드시 CPO를 지정해야 하지만, 법령에서는 CPO를 개인정보 처리 업무를 총괄해서 책임지는 사람으로 정의하고 일정한 직위를 가진 사람을 CPO로 지정하도록 하는 규정을 두고 있을 뿐, CPO의 자격과 전문성, 독립성에 대해서는 별다른 규정이 없다. 이런 상황에서는 기업 경영자의 개인정보보호의 필요성에 대한 인식 정도에 따라 CPO 제도의 운영은 천차만별일 수밖에 없다. 법적으로 보장되지 않더라도 CPO와 관련 조직에게 다른 영업조직과 독립된 역할을 부여하고 이사회와 소통하도록 권한을 부여하면서 전문성을 갖추도록 배려하는 기업이 있는가 하면, CPO와 관련 조직의 활동이 기업의 영리 추구에 도움이 안 된다고 생각하여 개인정보 처리와 관련된 중요한 의사결정에 관여할 기회를 주지 않으면서 사고처리반으로만 활용하는 기업도 있을 수 있다. 산업재해, 환경오염, 식품안전 등 사회적으로 영향을 주는 기업의 영업활동과 관련된 다른 문제와 마찬가지로 개인정보 침해도 기업 내부에서의 예방과 통제가 최선의 방책이다. 이런 관점에서 볼 때, 현재의 법 규정이 기업 내부의 통상적인 지배구조 하에서 지식과 전문성을 갖춘 CPO가 그 역량을 충분히 발휘할 수 있도록 하는 제도적 장치를 제공하고 있는지는 의문이다.

현행법상 CPO 제도의 한계에 대한 문제의식은 제도 연구의 측면에서 유럽의 일반 개인정보보호법(GDPR)에 규정된 DPO(Data Protection Officer) 제도와의 비교, 검토 과정에서 더욱 증폭되었다. 자세한 설명을 하기에는 지면 사정이 허락하지 않지만, 간단히 말해서 CPO가 기업 내부에서 영업활동이 법규를 준수하여 이루어지는 검토, 조언하는 법무팀의 역할과 유사하다면 DPO는 영업활동을 독립적으로 감독하는 준법감시인 및 감사의 역할과 유사하다. CPO가 기본적으로 기업 내부의 개인정보 처리 업무 및 정책을 관리하는 영업활동의 보조자, 협력자라면, DPO는 개인정보 처리 업무 및 정책을 평가하고 감독하는 영업활동의 감시자에 해당한다. 어느 정도 규모가 있는 기업이라면 법무팀과 준법감시인 및 감사(감사위원회)를 다 두고 있는 만큼, 개인정보 처리 업무가 영업활동에 큰 비중을 차지하는 기업이라면 CPO뿐만 아니라 DPO도 둘 필요가 있다. 그러나 DPO가 먼저 제도화된 유럽과 달리 CPO 제도를 오래 운영해온 우리나라 현실에서 DPO 제도를 도입한다면 CPO와 DPO의 관계를 어떻게 정립할 것인가 하는 점이 어려운 문제이다. 정부가 2021년 1월 입법예고한 개인정보보호법 개정안에 CPO 제도를 유지하면서 개인정보처리자에게 CPO의 독립성을 보장할 의무를 부과하고 개인정보 보호책임자 협의회 구성, 운영에 관한 근거규정과 매출액 또는 개인정보 보유 규모를 고려하여 CPO의 자격 등을 시행령으로 다르게 정할 수 있는 근거규정 신설 내용을 포함한 취지도 이런 고민에서 나온 절충안이라고 생각한다. 모쪼록

CPO 제도가 잘 정비되어 개인정보 처리 업무의 비중이 높은 기업들의 경우 ESG 경영 과제 목록에서 빠질 수 없는 개인정보보호 업무 발전에 큰 도움이 되기 바란다.