[논평]

AI 개발을 위한 공개된 개인정보의 무분별한 활용을 우려한다

- 학습 데이터 공개, 개인정보 영향평가 등 정보주체 권리 보호조치를 강화하라
- 연구목적 활용 동의 강제하는 플랫폼 기업 단속하라

지난 7월 18일, 개인정보보호위원회는 「인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서」(이하 안내서) 를 공개하였다. 개인정보위는 AI 기업이 공개된 개인정보를 현행 개인정보 규율체계 내에서 적법하고 안전하게 처리할 수 있도록 하는 지침이라고 설명하고 있다. 그러나 우리 단체들은 이 안내서가 AI 개발을 명분으로 공개된 개인정보의 활용을 정당화하고 있는 반면, 실효성있는 안전조치의 이행을 보장할 수 있을지 상당히 우려스럽다. 안내서가 AI 기술 개발과 정보 주체의 권리 보호 측면에서 균형 잡인 역할을 수행하고 있다는 평가를 받기 위해서는,훈련 데이터의 출처 등 관련 정보의 공개 및 개인정보 영향평가 수행 의무화 등 추가적인 조치가 전제될 필요가 있다.

안내서는 유럽 등 해외 사례를 언급하며 한국에서도 공개된 개인정보 처리의 법적 근거로서 개인정보보호법 제15조 제1항 제6호의 '정당한 이익' 조항을 제시하고 있다. 이에 따라 개인정보처리자의 정당한 이익과 정보주체의 권리 사이의 이익 형량을 위한 여러 고려 조건에 대해 설명하고 있다. 그러나 한국의 개인정보보호법은 처리자의 정당한 이익이 '명백하게' 정보주체의 권리보다 우선하고 '정당한 이익과 상당한 관련이 있고 합리적인 범위 내'로 제한하고 있다. 따라서 유럽연합 개인정보보호법(GDPR)보다 엄격하게 해석해야 함에도 안내서는 이 점을 간과하고 있다.

> 제15조(개인정보의 수집・이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
> 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

한국에서는 GDPR과 달리 민간의 개인정보 처리자에게 개인정보 영향평가를 의무화하고 있지 않고 과징금 액수도 크지 않은 등 다른 규제 수준이 낮다는 점을 고려하면 한국의 개인정보보호법에서 '정당한 이익'과 관련한 정보주체의 권리를 더욱 강하게 보호하는 것이 합당하다.. 하지만, 안내서는 이와 같은 개인정보보호법의 문구상의 명확한 차이와 이에 따라 이익 형량을 할 때 정보주체의 권리 보호에 중점을 두어야 한다는 점을 무시하고 있다.

정당한 이익이 무엇인지, 그리고 정당한 이익이 정보주체의 권리보다 '명백하게' 우선하는지는 개인정보처리자가 판단하게 되는데, 이러한 판단이 적절한지를 보장할 수 있는 방안이 없다. 안내서는 적법 요건을 충족할 수 있도록 처리자로 하여금 기술적, 관리적 안전조치를 취하고 정보주체의 권리를 보장하도록 하고 있지만, 어떠한 조합의 안전조치를 취할 것인지 역시 처리자의 선택에 맡겨져 있다. AI 학습에 어떠한 데이터를 활용했는지 공개하도록 하는 조치나 개인정보 영향평가의 수행 역시 권고 사항에 불과하다. 자신의 개인정보가 AI 학습에 활용되었는지 알 수있는 방법이 없는데, 어떻게 정보주체의 권리를 행사할 수 있는지 개인정보위에 묻고 싶다. 적법근거 충족 여부를 자율적으로 평가하고 그 근거를 문서화하도록 하고 있지만, 이 역시 권장 사항이다. 향후에 적절한 평가를 거쳤는지에 대해서 어떻게 감독을 할 수 있을지 의문이다.

물론 해당 AI나 개인정보에 따라 필요한 조치들은 달라질 수 있다. 그러나 AI 기업들의 책임성을 확보할 수 있는 최소한의 조치들은 필요하다. 예를 들어, AI 기업들의 책임성을 위해서는 투명성이 담보되어야 한다. 개인정보 보호 뿐만 아니라 여러가지 이유로 AI 훈련 데이터를 공개하라는 요구가 높아지고 있지만, 현재 주요 AI 기업들은 훈련에 어떠한 데이터를 활용했는지 영업비밀을 주장하며 비밀주의로 일관하고 있다. 어떠한 훈련 데이터를 활용했는지에 대한 공개는 정보주체의 권리 보호를 위한 최소한의 요건이다. 유럽연합의 AI 법에서도 훈련데이터의 상세한 요약본을 공개하도록 의무화하고 있다. 또한, GDPR과 같이 개인정보 영향평가를 민간 기업으로, 특히 대량의 개인정보를 처리하는 AI 기업으로 확대할 필요가 있다. 물론 이를 위해서는 개인정보보호법 또는 국내의 인공지능 법안을 통해 입법화될 필요가 있다. 그 전까지 개인정보위원회는 국내 AI 기업들의 안전조치 이행 현황에 대해 적극적으로 모니터해야 할 것이다.

안내서는 '공개된 정보의 AI 학습데이터 활용'에 적용된다는 전제를 달았으나, 이에 국한하지 않고 모든 영리목적 기술개발에 '정당한 이익'을 주장할 논거가 될 수 있다는 점에서 신중한 접근이 필요하다. 안내서가 단지 공개된 개인정보를 활용하고자 하는 처리자의 민원을 해결하는 수단이 아니라면, 정보주체에게 제공되는 정보가 극히 제한적인 기울어진 운동장을 어떻게 보완할 지에 대한 고민이 필요하다. 예를 들어, 전 국민을 대상으로 '공개된 정보가 AI학습데이터로 활용될 수 있다'는 사실에 대한 공지 및 교육이 필요할 수도 있다.

한편, 메타, 네이버 등 주요 플랫폼들은 최근 개인정보 처리방침을 수정하여 이용자의 동의를 받을 때 수집 목적에 인공지능 기술 개발 목적을 추가하였다. 비단 해당 서비스 자체의 개선에 제한되는 것이 아니라, 해당 기업의 전반적인 AI 기술 개발 목적을 포괄하는 것으로 보인다. 그러나 이는 목적 명확화의 원칙, 개별 동의의 원칙 등 기본적인 개인정보 보호원칙을 침해하는 것이다. 이루다 사태에서 본 바와 같이 이용자들은 특정 서비스 목적으로 제공한 자신의 개인정보가 그와 별개의 다른 서비스(AI를 포함하여) 개발

목적으로 활용되는 것을 원하지 않는다. 회사가 AI 개발 목적으로 활용하고 싶다면 '별도의' 동의를 받아야 한다. 개인정보위는 현재 AI 개발 업체들의 약관과 관행을 조사하여 개인정보보호법을 위반한 동의가 이루어지고 있는지 확인할 것을 촉구한다.

AI 기술 개발 또는 국내 AI 기업의 경쟁력 확보가 개인정보 보호를 무력화하는 명분이 되어서는 안된다. 개인정보위는 안내서가 개인정보 책임 회피를 위한 수단으로 활용되지 않도록 보완 조치를 마련하라. 또한, AI 개발을 명분으로 동의가 남용되지 않도록 감독하라.

2024년 7월 24일

건강권 실현을 위한 보건의료단체연합, 경제정의실천시민연합, 민주사회를 위한 변호사모임 디지털정보위원회, 사단법인 정보인권연구소, 연구공동체 건강과대안, 진보네트워크센터, 참여연대