Law談 칼 럼

사이버 보안 인재 10만 양성론… 새 정부가 먼저 해야할 일

강태욱 변호사(법무법인 태평양 변호사
/저작권보호원 심의조정위원)

디지털 시대를 바라보는 새 정부의 방향성은 아쉽게도 아직 잘 보이지 않는다. 시대의 물결이 디지털 혁신의 가속화, 데이터의 공개와 활용으로 향하고 있음에는 별다른 이견이 없기에 이러한 방향성에 트집을 잡거나 굳이 새로운 물길을 내려는 시도는 불필요한 일이기도 할 것이다.

그럼에도 불구하고 새 정부의 국정 과제 중 디지털 혁신과 데이터 활용을 둘러싼 정책의 방향성에 대한 언급이 부족한 것은 이 정부의 관심사가 아니라는 점을 방증하는 것일까 하는 아쉬움이 다소 있다. 대통령직인수위원회가 내놓은 110대 국정 과제 중 IT 정책과 관련해 두드러지는 것은 '모든 데이터가 연결되는 세계 최고의 디지털 플랫폼 정부 구현'이라는 국정 과제 정도이다. 그 이외의 것들은 기존 정부의 정책과 차별성을 가지지 않는 것들이 대부분이다. 사실 이는 인수위 구성에 있어서 IT 정책과 관련해 민간 분야의 전문가가 포함되지 않은 것에서 이미 예상됐던 바이기도 하다.

IT 정책 중 사이버 시큐리티와 관련한 것들만 살펴보자. 윤 대통령은 후보 시절 사이버 안전망 구축을 위해서 '인공지능을 활용한 통합 사이버 대응 체계를 구축'해 "대한민국을 사이버 공격에서 안전하게 지켜내겠다."는 공약을 발표한 바 있다. 국정과제에서는 이를 좀

〈디지털 시대에 대한 새 정부의 방향성은 아직 명확치 않다는 지적이 나온다. 윤석열 대통령이 국민의 힘 대통령 후보 시절인 지난 1월 디지털 경제정책 관련 공약을 발표하는 모습〉

더 구체화했다. 주요 안전 관리의 디지털 지능화를 통해 국민의 생활 안전을 강화하고, 보안 클러스터 모델의 지역 거점 확산을 통해 기업 성장을 지원하며, 10만 사이버 보안 인재 양성을 하겠다고 제안했다. 나아가 블록체인, 생체인증 등 신 인증기술의 도입을 촉진하고 디지털 인증 활성화를 통한 이용자 편리성 강화와 신시장 창출 지원을 위한 제도 개선을 하겠다고 약속했다. 그리고 2021년 기준 매출액 약 12조6000억원 규모의 보안 산업을 전략적으로 육성해 2027년에는 매출액 20조원 규모의 산업으로 성장시키겠다고 했다.

윤석열 정부 국정과제 중 정보보안 관련 주요 내용

- 국가 필수 전략기술에 '사이버 보안' 지정
- 대통령 직속 '국가사이버안보위원회' 설치
- 보안 클러스터 모델의 지역거점 확산으로 기업 성장 지원
- 2026년 까지 10만 사이버 보안 인재 양성
- 관련 산업 규모 2027년 20조원 목표

'10만 사이버 보안 인재 양성론'은 잘 알려진 것처럼 율곡 이이의 '10만 양병설'에서 기시감이 느껴지는 수사(修辭)이다. 우리는 이미 1990년대 말에 이를 현대화해 제안된 '10만 해커 양성론'이라는 용어에 익숙해 있지만, 해커 양성과 사이버 보안 인재의 양성은 전혀 다른 얘기라는 점에서 뭔가 연관시켜 생각하기는 어렵다.

또한 정보보안 현황조사에 따르면 2020년 기준 정보보안 산업 영역에 종사하는 인력이 약 3만8000명, 물리 보안 인력이 약 1만5000명으로 합계 약 5만4000여명이고, 해마다 신규로 채용되는 인력도 평균 5000명에서 6000명 수준으로 알려져 있다. 5년 동안 10만 사이버 보안 인재를 양성하겠다는 것이라면 매년 2만명 정도의 보안 인력을 키워 내겠다는 것인데, 산업을 분류하는 시각의 차이에서 나온 것이라고 볼 수도 있고, 수치의 문제가 아니라 사이버 보안 영역을 중요하게 생각하고 이 분야 산업을 육성하겠다는 의지라고 볼 수도 있을 것이다.

한편 디지털 '플랫폼' 정부는 클라우드 서비스의 과감한 사용과 민관 협력을 통한 서비스 제공과도 밀접하게 관련이 있다. 단순히 프라이빗 클라우드가 아니라 이미 앞서가고 있는 민간의 퍼블릭 클라우드 서비스를 어느 정도 활용할 것인지에 따라 플랫폼 정부의 성패가 좌우될 것이다. 사이버 안전망의 구축과 관련해서도 플랫폼과 클라우드라는 방향성은 또 다른 관점에서의 통찰력을 요구한다. 기존의 관성을 따르는 전제에서라면 예상보다 훨씬 집행하기 어려운 과제가 될 것이고 새로운 시각과 발상의 전환을 전제로 해야만 달성 가능한 것이기도 하다.

〈지난 2일 당시 안철수 대통령직인수위원회 위원장이 서울 종로구 통의동 인수위원회에서 '디지털 플랫폼 정부로 달라지는 대한민국'에 대한 브리핑을 하는 모습〉

사이버 안전망 강화를 위해 반드시 필요한 것 중의 하나는 보안 산업이 제대로 된 평가를 받을 수 있도록 하는 것이다. 정보 보안을 위해 높은 수준의 기준을 디테일하게 설정하고, 그 기준들이 충족됐는지를 시시콜콜하게 따져서 평가를 하며, 보안 사고가 발생했을 때는 보안 책임자에 대해 "네 잘못을 아느냐?"며 책임을 묻는 방식은 보안 산업이 세계적 수준에 이르게 하기에는 지나치게 고답적인 방식이다.

민간 기업에 정보보호최고책임자(CISO)를 지정·신고하게 하고 CISO를 중심으로 보안 정책을 준수하도록 강제했으면, 자율적으로 가이드에 따른 보안 정책을 수립하고 집행할 수 있도록 하는 여지를 주는 것이 필요하다. 보안 사고가 발생하면 그때마다 보안 최고 책임자에게 형사 처벌을 하겠다는 접근 방식은 현대 사회에 맞지도 않을뿐더러 민간의 자율성 강화를 통한 산업 경쟁력의 증대에도 아무런 도움이 되지 않는다.

그 시작은 비록 미약하지만 국정 과제가 품고 있는 방향성을 잘 다듬어 새 정부가 끝날 즈음에는 정보보호 산업이 사고만 치는 천덕꾸러기 처지가 아니라 세계 최고 수준의 역량을 가진 산업으로 발전할 수 있기를 기대해 본다.

(출처/중앙일보)