MINBYUN-Lawyers for a Democratic Society
민주사회를 위한 변호사모임

서울 서초구 법원로 4길 23 대덕빌딩 2층
전화 02)522-7284, 팩스 02)522-7285
웹페이지 http://minbyun.or.kr
전자우편 admin@minbyun.or.kr

문서번호 : 24-05-디정위-03

수 신 : 각 언론사

발 신 : 민변 디지털정보위원회

제 목 : [논평] 개인정보 대량 유출에도 장기간 책임을 방기한 대법원을 엄중히 규탄한다
- 국가기관 전반의 개인정보 보호 강화 대책이 시급히 마련되고, 실태점검이 이루어져야 -

전송일자 : 2024. 5. 13.(월)

전송매수 : 총 4매

[디지털정보위][논평]

개인정보 대량 유출에도 장기간 책임을 방기한 대법원을 엄중히 규탄한다

- 국가기관 전반의 개인정보 보호 강화 대책이 시급히 마련되고, 실태점검이 이루어져야 -

1. 경찰청은 2024. 5. 12. '법원전산망 해킹 및 자료유출 사건'에 대한 조사 및 수사 결과를 발표하였다. 그 내용은 (1) 북한 해킹조직의 법원전산망에 대한 침입은 2021. 1. 7. 이전부터 2023. 2. 9.까지 있었고, (2) 이 기간에 총 1,014GB의 법원자료가 법원전산망 외부로 유출되어 전송되었는데 조사과정에서 그 중 약 0.5%에 해당하는 극히 일부의 회생사건 관련 파일 4.7GB만을 외부에서 발견하여 구체적인 유출사실을 확인 하였을 뿐이며, 나머지 대다수 데이터는 유출서버 기록이 이미 삭제되어 현재까지 그 내용을 파악하지 못하고 있다는 것이다.

2. 경찰청 수사결과와 지금까지 언론에 보도에 따르면 법원전산망 해킹 및 자료유출에 대하여 법원의 최초 인지 후 대응 경위는 아래와 같다.

(i) 법원은 2023. 2. 7. 해킹사실을 인지했음에도, 당시 시행 중이었던 구 개인정보보호법(2023. 3. 14. 법률 제19234호로 일부개정되기 전의 것) 제34조 및 같은 법 시행령(2023. 9. 12. 대통령령 제33723호로 일부개정되기 전의 것) 제40조에서 규정하고 있는 정보주체에 대한 개인정보 유출 통지 및 유출사실에 대한 개인정보보호위원회 등에 대한 신고 조치를 전혀 취하지 않았다는 점

(ii) 법원은 2023. 2. 7. 해킹사실 인지 이후 10개월이나 지난 2023. 12. 7.이 되어서야 해킹사실에 대한 언론보도와 이를 통한 수사기관의 수사가 진행되자 '보안전문업체에 악성코드 분석 의뢰 및 유출이 의심되는 개인정보 항목 및 건수 불특정' 등의 내용이 담긴 '사법부 전산망 악성코드 탐지 관련 안내문'을 공지하였다는 점

(iii) 법원은 2024. 3. 5. '사법부 전산망 침해사고에 관하여 국민들께 드리는 말씀'을 통해 사안의 중대성과 후속조치 예정, 보안역량 강화를 위한 종합대책 수립 진행의 내용을 공지하였는데 이때에도 구체적인 개인정보 유출에 관한 내용은 포함하지 않았다는 점

(iv) 법원은 2024. 5. 8. 경찰청 등 관계기관 합동으로 이루어진 조사 및 수사 결과를 통보받은 이후 2024. 5. 11.이 되어서야 '사법부 전산망 침해에 의한 개인정보 유출 추가 안내'에서 개인정보 유출 사실 확인과 정보주체들에 대한 피해예방 안내 등을 공지하였다는 점

3. 구 개인정보보호법(2023. 3. 14. 법률 제19234호로 일부개정되기 전의 것) 제34조, 같은 법 시행령(2023. 9. 12. 대통령령 제33723호로 일부개정되기 전의 것) 제40조에 따르면, 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때 '지체없이' 해당 정보주체에게 그 사실을 알려야 하고, 개인정보의 규모 및 주민등록번호 등 개인정보의 내용에 따라 개인정보보호위원회 또는 전문기관(한국인터넷진흥원)에 그 사실을 신고하여야 한다.

이러한 개인정보처리자의 개인정보 유출 통지 및 신고의무는 개인정보 유출 등으로 인한 2차 피해 확산을 최소화하고 이용자 등 정보 주체를 위한 보호조치를 신속하게 하기 위한 것이며, 유출사고를 정부 및 전문기관에 알림으로써 체계적·조직적 대응을 하여 그 원인과 피해 내용을 규명하여 추가 피해를 방지 하기 위함이다.

위 법은 구체적인 유출 내용을 확인하지 못한 경우라도 개인정보 유출사실 자체를 인지한 이상 통지 및 신고의무가 발생한다고 보며, 개인정보가 유출된 사실과 유출이 확인된 사항만이라도 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있도록 규정하고 있다.

그런데 법원은 2023. 2. 7. 백신 업데이트 과정을 통해 법원전산망이 해킹되고 있다는 사실을 이미 인지했음에도 불구하고 그 즉시 유출 사실 통지 및 신고를 하지 아니하였고, 2023. 12. 18.이 되어서야 외부 보안 전문가 등과 함께 심층조사가 진행되어 정보주체들에 대한 피해예방 등 안내 공지는 2024. 5. 11.에 이르러서야 이루어졌다.

4. 법원전산망 외부로 유출된 1,014GB의 정보 중 약 0.46%인 4.7GB 정도만 유출내용이 확인되었는데, 여기에서 확인되는 개인정보 항목만 하여도 이름 뿐만 아니라 주민등록번호, 신용정보, 의료정보 등 고유식별정보와 민감정보가 포함된 개인정보들이 다수 포함되어 있다고 한다. 법원이 2023. 2. 7. 해킹사실을 확인했음에도 그 이후 상당한 기간 동안 적극적인 조치를 취하지 않고 늦장대처를 함으로써 개인정보 유출 확인의 범위가 축소된 것은 아닌지하는 의문이 생기는 건 당연하다. 지금은 유출된 나머지 1009.3GB의 정보에 누구의, 무엇에 관한 개인정보가 담겨 있었는지 확인할 길이 없게 되었고, 이로 인해 정보주체들은 자신의 정보인권이 어떻게 침해되고 있는지조차 파악하지 못하는 상태에 놓이게 되었다. 법원은 이 책임을 어떻게 질 것인지 묻고 싶다.

5. 법원은 시민의 권리와 의무를 종국적으로 판단하는 국가기관이기에 정보주체의 아주 내밀한 정보까지 처리할 수밖에 없고, 가족관계부 및 등기부, 나아가 전자소송에 이르기까지 엄청난 양의 개인정보를 자체적으로 저장하고 있는 조직이다. 그럼에도 사법부는 수년 동안 법원전산망이 해킹되고 있다는 사실 자체도 인지하지 못했고, 이를 확인한 이후에도 즉각적인 개인정보 유출 확인, 통지 및 신고 등 적극적인 조치를 취하지도 않았으며, 정보주체들에 대한 피해예방 등의 안내 또한 침입 확인 후 1년3개월이난 지난 뒤에서야 공지를 하였다.

6. 한편, 라자루스 악성코드에 침해된 대법원 전산망 관리자 계정의 비밀번호가 'P@ssw0rd', '123qwe', 'oracle99' 등과 같이 쉬운 문자열로 구성되어 있고, 일부 계정은 2016년 8월부터 6년 넘게 'P@ssw0rd' 비밀번호를 바꾸지 않은 것으로 보도 되었다. 대법원의 이처럼 안일한 대처와 관리 행태에 아연실색하지 않을 수 없다. 개인정보 유출이라는 불법행위에 의한 손해배상책임을 판단해 왔던 법원이 자기 조직 내에서의 개인정보 보호에 이 정도로 미흡할 수 있는지 이해하기 어렵다.

7. 우리 위원회는 앞으로 법원이 추가적인 개인정보 보호조치를 어떻게 이행하는지, 이번 사건으로 인해 피해를 입은 정보주체들에 대한 어떠한 책임을 지는지, 재발방지를 위한 대책을 제대로 시행하는지 계속 지켜볼 것이고, 필요하다면 이번 사건으로 인해 피해를 입은 시민들의 권리구제를 위한 손해배상청구 소송도 검토할 것이다. 개인정보가 집적되어

있는 국가기관의 개인정보 보호의 중요성은 아무리 강조해도 지나치지 않다. 대법원이 형사소송의 전자화를 추진하는 상황에서 과연 각종 재판기록이 안전하게 적절히 관리,보관되었는지 그리고 향후에도 잘 보관될 수 있을지 의문을 가질 수 밖에 없다. 이번 사건을 계기로 법원 뿐만 아니라 국가기관 전반의 개인정보 보호 강화 대책이 마련되어야 하고, 그동안 형식적으로 개인정보 관리를 해온 것은 아닌지 점검해보길 강력히 요청한다.

마지막으로 빅데이터 시대라는 이유로 공공데이터 활용 및 산업육성이라는 명분만을 강조하며, 시민들의 개인정보를 국가기관에 집중시키고 활용하는 정책을 추진할 시 시민들에게 어떤 권리침해와 피해가 발생할 수 있는지 국가기관들이 돌아보고 자성하는 계기가 되기를 바란다.

2024. 5. 13.

민변 디지털정보위원회