의 견 서

발행일 2023. 12. 05.

사이버안보 업무규정 일부개정령안 (국가정보원공고 제2023-4호) 에 대한 의견서

국정원감시네트워크

민주사회를 위한 변호사모임, 민주주의법학연구회,
진보네트워크센터, 참여연대, 천주교인권위원회,
투명사회를 위한 정보공개센터, 한국진보연대

목차

요약

1. 개정령안에 대한 의견 제출 이유

- 현행 「사이버안보 업무규정」(이하 '현행 규정')은 법률에 규정해야 할 사항들을 시행령에 담고 있다. 국가정보원의 「사이버안보 업무규정 일부개정령안」(이하 '국정원 개정령안')은 "구체적인 사항이 일부 결여되어 있어 이를 합리적으로 정비"한다는 명분으로, 국정원이 현행보다 더 폭넓게 관여할 수 있도록 권한을 확대 · 강화하는 내용이 곳곳에 담겨 있다. 국정원감시네트워크를 비롯해 시민사회에서는 국회를 통한 민주적 통제 없이 국정원이 자의적으로 권한을 확대하는 상황을 우려해 왔다. 국정원 개정령안은 이러한 우려가 현실이 되고 있음을 보여준다.
- 국정원 개정령안은 법률에서 위임된 범위를 벗어나 국정원이 권한을 자의적으로 확대 · 강화하거나, 민간의 정보통신망과 클라우드 서비스 등에도 개입할 수 있는 권한 등을 부여하고 있다. 국정원이 절대 권력으로서의 권한을 남용해 자칫 민간인 사찰 등 국민의 기본권 침해를 비롯한 온갖 불법행위로 이어질 수 있어 매우 우려스럽다. 따라서 국정원 개정령안에 대해 아래와 같은 문제가 있으므로 개정령안의 전면 폐기 의견을 밝힌다.
- 시행령인 현재 규정에 포함된 내용은 '국가사이버보안' 관련 법률을 통해 규정되어야 한다. 또한 국정원이 제대로 된 법률적 근거를 갖추지 않고 행사하고 있는 '국가사이버보안' 권한도 과학기술정보통신부나 (가칭)'국가사이버보안청'을 신설하여 일반 정부부처나 기관으로 이관되어 투명하고 책임성 있게 이루어져야 한다.

2. 개정령안에 대한 의견 개요

1) 법률에서 위임한 범위를 벗어난 국정원의 권한 확대

- 국가사이버안보센터의 권한 확대 (안 제4조 제2항 및 제3항)
- 사이버안보정보 조사를 위한 자료제출 요구 (안 제5조의2)
- 사이버안보정보에 관련된 대응조치 등 (안 제6조의2)

2) 민간 정보통신망으로의 국정원 권한 확대 · 강화

- 사이버안보 업무규정의 적용 범위 확대 (안 제2조)
- 사이버보안 학술 · 연구기관에 대한 국정원의 통제력 확대 (안 제17조)
- 민간 클라우드 서비스 업체로의 권한 확대 (안 제7조의2 제3호, 제9조 제2항, 제14조 제4항)

3) 정부부처 · 공공기관의 '상급기관'으로서 국정원의 위상 강화

- 사이버안보 업무의 기획 · 조정 권한 (안 제3조의2)
- 공공기관의 범위 확대 (안 제7조)
- 각급기관에 대한 국정원의 감독 권한 확대 (안 제9조 제5항, 제10조, 제12조, 제13조, 제16조)
- 사이버보안 관련 국방부에 대한 통제 (안 제19조)

4) 기타 현행 규정보다 국정원 권한을 확대 · 강화하는 사항

- 현행 규정 제3조 제3항의 삭제
- 정보협력체계 구축의 범위 확대 (안 제5조)

들어가며

2023년 10월 27일, 국가정보원(이하 '국정원')은 「사이버안보 업무규정 일부개정령안」(이하 '국정원 개정령안')을 입법예고했다(국가정보원공고 제2023-4호). 국정원은 "2020. 12. 15.「국가정보원법」 전부개정(법률 제17646호)에 따라 "국가 全 영역에서의 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집 · 작성 · 배포 및 관련 대응조치와 공공분야 대상 사이버공격에 대한 예방 및 대응 직무가 부여된 바 있"고, "2020. 12. 31. 제정된 「사이버안보 업무규정(대통령령)」에는 해당 직무를 수행하기 위한 구체적인 사항이 일부 결여되어 있어 이를 합리적으로 정비하고자 하려는 것"이라고 밝혔다. 그러나 국정원의 개정령안은 현행 규정에 비해 국정원의 '국가사이버보안' 권한을 대폭 확대하고 있다. 이처럼 법률에 규정해야 할 사항들을 시행령에 규정함으로써 국정원의 권한을 국회의 통제 없이 자의적으로 확대할 수 있게 된 상황에 대해 매우 우려스럽다.

현행 「사이버안보 업무규정」(이하 '현행 규정')은 국정원이 2017년 국회에 제출했던 「국가사이버안보법안」(의안번호: 제2004955호, 이하 '국정원 2017년안'), 2022년 입법예고에 그쳤던 「국가사이버안보 기본법 제정(안)」(국가정보원공고 제2022-5호, 이하 '국정원 2022년안'), 2020년 6월에 조태용 의원(당시 국민의힘, 현 국가안보실장)이 대표발의한 「사이버안보 기본법안」(의안번호: 제2101220호, 이하 '조태용 의원안') 등에서 규정한 내용을 상당 부분 포함하고 있다.

국정원의 2017년안에 대해서는 6개 시민사회단체들이 반대 의견서를, 2022년안에 대해서도 7개 시민사회단체로 구성된 국정원감시네트워크는 반대 의견서를 제출한 바 있다. '국가사이버보안'을 위한 정부 차원의 조정과 대응은 필요하나, 이는 일반 행정부처 · 기관들에서 투명성과 책임성을 갖고 민간영역을 비롯한 이해관계자와의 참여와 협력을 통해 수행해야 하는 업무로, 밀행성과 은밀성을 전제로 활동하는 비밀정보기관이 '국가사이버보안'의 '컨트롤 타워' 역할을 맡아서는 안 된다는 게 골자다. 지나친 정보 수집과 대공수사권을 앞세워 국내 정치에 개입하고 민간인을 사찰하는 등 불법행위를 저질러 온 국정원이 '국가사이버보안'의 '컨트롤 타워' 권한까지 갖게 되면, 공공 · 민간의 정보통신망 전반에 대한 감시와 사찰로 인해 기본권 침해로 이어질 것을 우려할 수밖에 없다.

국정원은 「국정원법」 제4조 개정을 통해 '사이버안보 정보의 수집 · 작성 · 배포', '사이버공격 및 위협에 대한 예방 및 대응'이 자신의 직무로 포함된 것을 근거로, 기다렸다는 듯 기존에 법률로 추진하려던 사항들을 시행령으로 넘기려 하고 있다. 2020년 「국정원법」 개정으로

국정원의 수사권을 박탈함으로써 권한 남용을 통제하려는 개혁을 표방했으나, 그 이면에서는 국정원의 숙원이던 '국가사이버안보법'의 제정을 시행령으로 우회해 실현시키는 결과로 이어질 수 있다는 게 문제다. 이는 법률유보 원칙의 위반일 뿐 아니라, 이번 개정령안에서 볼 수 있듯이 국정원이 자의적으로 권한을 확대 · 강화할 우려가 있다. 이 때문에 국정원감시네트워크는 지난 2020년 「사이버안보 업무규정」 제정안 입법예고에 대한 의견서에서도, 이 규정을 폐지하고 국정원의 사이버보안 업무를 배제한 국가사이버보안 관련 법률을 제정토록 촉구한 바 있다.

따라서 7개 시민사회단체로 구성된 국정원감시네트워크는, 국정원의 개정령안에 대한 비판에 앞서, 시행령인 현재 규정에 포함된 내용들은 '국가사이버보안'과 관련한 기본법을 통해 규정되어야 한다는 점을 다시금 밝힌다. 또한 국정원이 제대로 된 법률적 근거를 갖추지 않고 행사하고 있는 '국가사이버보안' 권한도 과학기술정보통신부(이하 '과기부')나 (가칭)'국가사이버보안청'을 신설해 일반 정부부처로 이관되어 투명하고 책임성 있게 이루어져야 한다는 점을 다시 한번 명확히 밝힌다. 이와 함께 국정원 이번 개정령안이 가진 문제점과 그에 대한 의견을 아래에서 구체적으로 제시한다.

법률에서 위임한 범위를 벗어난 국정원의 권한 확대

1. 국가사이버안보센터의 권한 확대 (안 제4조 제2항 및 제3항)

- 개정령안 제4조 제2항 및 제3항은 국가사이버안보센터에 '민관 합동 통합 대응체계를 구축 · 운영을 수행하기 위한 전담 조직' 및 '자문단'을 둘 수 있는 근거를 새로이 두고 있다. 개정령안 제6조의2 제3항에 따른 '민관 합동 통합 대응체계'의 문제점에 대해서는 따로 지적하겠지만, 이처럼 법률 아닌 시행령의 개정만으로 국가사이버안보센터의 권한을 확대하는 것은 문제다. 새로운 권한의 부여는 법률에 규정되어야 한다.

- 현행 규정은 "소속 공무원 또는 임직원의 파견 등 협조를 요청할 수 있"는 대상을 법 제4조 제1항 제4호 각 목의 기관(중앙행정기관등)으로 제한했으나, 개정령안은 이를 법 제5조 제1항에 따른 '국가기관이나 그 밖의 관계 기관 또는 단체'로 확대하고 있다. 개정령안 '국가기관이나 그 밖의 관계 기관 또는 단체'의 범위가 어디까지인지는 명확하지 않기 때문에, 국정원이 관계 기관 또는 단체로 규정하는 모든 기관은 국정원의 협조 요구에 응해야 한다. 또한 법 제5조 제1항은 "사실의 조회 · 확인, 자료의 제출 등 필요한 협조 또는 지원"을 규정하고 있는데, "소속 공무원 또는 임직원의 파견 등"에 까지 협조의 범위를 확대한 것은 법률의 위임 범위를 벗어난 것이다.

2. 사이버안보정보 조사를 위한 자료제출 요구 (안 제5조의2)

- 개정령안은 국정원에 '사이버안보정보 조사'를 위해, "해당 정보가 수록 · 기재된 디지털 자료 등을 그 소유자 · 소지자 또는 보관자로부터 제출받을 수" 있도록 하고 있다. 전기통신사업자가 보관 중인 통신사실확인자료에 대해서는 「통신비밀보호법」 제13조의4에 따른다고 규정한다지만, 이 또한 국정원 등 '정보수사기관'이 "국가안전보장에 대한 위해를 방지하기 위하여 정보수집이 필요한 경우 전기통신사업자에게 통신사실 확인자료제공을 요청할 수" 있도록 한 조항이다. 국정원이 '국가안보'와 관련된 자료라고 규정하면, 언제든 민간 당사자에게도 해당 자료 제출을 요구할 수 있다. 이는 의무 조항은 아니나, 과연 국정원의 '자료제출 요구'를 민간기업이나 개인이 거부할 수 있을지 의문이다.

- 이는 법원의 통제도 없이 국정원이 무한대로 조사하고 자료를 수집할 수 있도록 한 규정이다. 이러한 규정이 존속하는 한, 국정원이 갖고 있는 수사권의 이관이 과연

실효성이 있을지 의문이다. 국정원의 권한 남용을 통제하기 위해서는 국정원이 다른 기관이나 기업으로부터 디지털 자료를 입수 또는 자료제출 요구를 하고자 할 때, 법원의 영장을 요구토록 할 필요가 있다.

3. 사이버안보정보에 관련된 대응조치 등 (안 제6조의2)

- 개정령안은 국정원에 정보통신기기 · 소프트웨어를 확인하기 위해 기술적 시험 · 분석 등 검증하고 위험 최소화 조치를 할 수 있는 권한, 국가안보와 국익에 반하는 국제 및 국가배후 해킹조직 등의 활동을 선제적으로 확인 · 견제 · 차단하기 위해 국외 및 북한을 대상으로 추적, 무력화 등 공세적 조치를 할 수 있는 권한, 위기상황을 관리하기 위한 민관 합동 통합대응 체계를 구축 · 운영할 권한 등을 부여하고 있다. 국정원은 이를 "「국정원법」상 사이버안보정보에 관련된 대응조치 업무를 구체화"한 것이라고 설명한다.

- 국정원감시네트워크는 2020년 국정원법 개정 당시부터 법 제4조 제1항 제3호의 '대응조치'에 대해 "그 개념이 명확하지 않아 정보수집 활동을 넘어 공작활동 등을 대응조치라는 이름으로 합법화할 가능성"을 우려해 왔다. 시민사회가 우려한 바와 같이, 개정령안은 국정원에 마치 군사작전을 수행하듯 '선제적으로', '공세적 조치'를 취할 수 있는 권한을 부여하고 있다. '국가안보와 국익에 반하는 활동에 악용되거나 악용될 만한 상당한 개연성', '국민안전 보호를 위하여' 등 그 요건도 지나치게 폭넓고 자의적이다. 또한 이러한 조치가 구체적으로 무엇인지는 명확하지 않기 때문에 국정원은 '국가안보'를 명분으로 정보기관의 업무를 벗어난 다양한 정치적 작전을 수행하지 않을지 우려된다. 가령, 원세훈 전 국정원장은 국정원 직원을 동원해 인터넷 댓글과 트위터 게재 · 배포 등의 활동을 통해 18대 대통령선거 때 박근혜 후보의 당선을 돕는 등 공직선거에 개입하고 국내정치 개입 활동을 한 것을 국정원 심리전단 활동의 일환이라 주장한 바 있다.

- 더구나 위기상황의 관리를 명분으로 '민관 합동 통합대응 체계'를 구축 · 운영할 권한을 국정원에 부여하고 있기 때문에, 심지어 민간 업체들까지도 국정원의 대응조치나 정치적 목적의 작전에 동원될 가능성을 배제하기 어렵다.

- 법 제4조 제1항 제3호의 대응조치 자체가 정보기관으로서의 활동 범위를 넘어선 것이므로, 이번 개정령안에서 삭제되어야 하는 것은 물론이고, 같은 취지와 방향에서 「국정원법」 자체를 개정해야 한다.

민간 정보통신망으로의 국정원 권한 확대 · 강화

---

1. 사이버안보 업무규정의 적용 범위 확대 (안 제2조)

- 현행 규정은 "법 제4조 제1항 제1호 마목, 같은 항 제4호 및 같은 조 제3항에 따라 국가정보원의 직무 중 사이버안보 관련 정보의 수집 · 작성 · 배포 및 사이버공격 · 위협에 대한 예방 · 대응 업무의 수행에 필요한 사항"을 규정하고 있다.
- 그런데 개정령안은 시행령의 규정 대상을 사이버안보 업무로 통칭하고, 다시 이를 '사이버안보정보 업무'와 '사이버보안 업무'로 구분하면서, '사이버보안 업무'에 '법 제4조 제1항 제4호에 따른 예방 및 대응' 업무 뿐만 아니라, '법 제4조 제1항 제2호에 따른 보안업무 중에서 전자적 방법에 의하여 수행되는 업무' 및 '법 제4조 제1항 제6호에 따른 사항 중에서 위 가목 또는 나목과 관련되어 국가정보원장이 따로 정하는 사항'(개정령안 제2조 제3호 나, 다)을 추가적으로 포함하고 있다.
    - 법 제4조 제1항 제2호는 국가 기밀 관련 보안 업무인데, 이 가운데 디지털 암호 모듈 검증 등 국정원이 이미 수행해 오던 업무를 시행령에 포함하려는 것으로 보인다. 그러나 '사이버보안 업무' 뿐만 아니라, 국가 기밀 관련 정책의 수립 업무가 과연 비밀정보기관의 업무가 되어야 하는지 의문이다. 또한 과거와 달리 디지털 암호는 이제 민간에서도 보편적으로 사용되고 있다. 관련 정책에 국정원이 관여하는 것은 적절하지 않으며 오히려 민간 보안기업에 대한 통제 논란만 야기할 뿐이다.
    - 다목의 경우 그 범위조차 명확하게 규정하지 않아, 국정원이 관련 업무를 법률의 위임 범위를 넘어 자의적으로 확대할 여지를 두고 있다.

2. 사이버보안 학술 · 연구기관에 대한 국정원의 통제력 확대 (안 제17조)

- 현행 규정과 개정령안에서는 "사이버안보 업무의 수행에 필요한 전략 · 정책 및 기술의 연구 · 개발"을 명분으로 관련 학회, 학술단체 등 비영리법인을 전문기관으로 지정하고 경비 등을 지원할 수 있도록 하고 있다. 이는 국정원이 사실상 금전적 지원을 매개로 관련 학술 · 연구기관과 단체를 포섭하겠다는 것이나 다름없다. 이제껏 국정원이 수행해 오던

전략으로, 국내의 관련 학계에서 국정원에 대한 비판의 목소리를 찾아보기 힘든 것도 이러한 이유 때문이다.

- 더구나 국정원 예산 대부분을 특수활동비라는 이유로 공개하지 않고 있고, 국정원이 정하겠다는 '전문기관 지정 관련 세부사항'(안 제17조 제3항)도 비공개할 것이 뻔한 상황에서 전문기관 지정과 경비 지원이 투명하고 책임성 있게 이루어질 것이라 기대하기 어렵다.

3. 민간 클라우드 서비스 업체로의 권한 확대 (안 제7조의2 제3호, 제9조 제2항, 제14조 제4항)

- 개정령안은 "각급기관 대상 사이버공격 · 위협"의 개념을 '각급기관이 이용하는 클라우드컴퓨팅서비스 이용영역(물리적, 논리적 영역을 포함한다)을 대상으로 하는 사이버공격 · 위협'을 포함하는 것으로 확대하고 있다(안 제7조의2 제3호). 또 국정원으로 하여금 클라우드컴퓨팅서비스 이용영역의 도입 · 운영 · 이용에 관한 보안대책을 수립할 수 있도록 하고 있다(안 제9조 제2항). 뿐만 아니라, 클라우드컴퓨팅서비스 제공자에게 국가보안관제에 필요한 협조 또는 지원을 요청할 수 있도록 하고 있다. 이 경우 요청을 받은 클라우드컴퓨팅서비스 제공자는 정당한 사유가 없으면 그 요청에 따르도록 하고 있다(안 제14조 제4항).

- 국내 시민사회단체들은 이미 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」의 제정이 논의될 때부터, 국정원이 민간 정보통신서비스 부문에 개입하는 것에 대해 우려를 표명한 바 있다(관련 5개 단체 의견서, 2014. 9. 5.). 이에 대한 비판이 커지자, 다행히 민간 클라우드 서비스에 대해 국정원이 관여할 수 있는 조항을 삭제하고 관련 법률이 제정되었다. 그런데 공공기관이 민간 클라우드 서비스를 이용한다는 이유로, 국정원이 또다시 '사이버보안' 권한을 민간 클라우드 서비스로 확대하려 시도하고 있는 것이다.

- 민간 클라우드 서비스를 이용하는 공공기관의 보안이 우려된다면, 민간 서비스를 이용하지 않으면 된다. 혹은 국정원이 아니라 투명하고 책임성 있게 권한을 행사할 수 있는 부처와 기관에 사이버보안 권한을 부여해, 민간 클라우드 서비스까지 관리 · 감독할 수 있도록 하면 된다. 국정원에 사이버보안 권한을 부여하면서 민간의 정보통신망까지 관여하게 한다면, 비밀정보기관의 민간 사찰 우려로부터 자유로울 수 없다.

정부부처 · 공공기관의 '상급기관'으로서 국정원의 위상 강화

1. 사이버안보 업무의 기획 · 조정 권한 (안 제3조의2)

- 국정원에 사이버안보정보 업무의 협력에 관한 지침, 사이버보안 기본지침 등 여러 지침을 수립할 권한과 "국가안보에 중대한 영향을 미치는 주요 사안에 대해서는 직접 조정"할 권한을 부여하고 있다. 사이버보안 기본지침의 수립이 비밀정보기관의 업무가 되어야 하는지 의문이며, "국가안보에 중대한 영향을 미치는 주요 사안에 대해서는 직접 조정"하는 권한이 국가안보실 등이 아닌 정보기관에 부여되는 것 역시 문제다. 이는 법 제4조 제1항 제5호에 따른 국정원의 "정보 및 보안 업무의 기획 · 조정" 권한을 구체화한 것인데, 이를 통해서도 국정원에 "정보 및 보안 업무의 기획 · 조정" 권한을 부여하는 것이 심각한 문제라는 점이 드러난다.

- 개정령안과 「정보및보안업무기획 · 조정규정」(제6조) 모두 "국가안보에 중대한 영향을 미치는 주요 사안"에 대한 명확하고 구체적인 정의조차 없이 관련 규정을 지침으로 다시 위임하고 있다. "국가안보"를 구실로 국정원이 "조정 대상기관"인 다른 행정부처들에 대해 직접 조정 권한을 행사하는 과정에서 권한을 남용할 여지가 크다. 포괄위임금지 원칙에도 어긋나므로 개정령안 해당 조항의 신설은 물론, 「국정원법」과 「정보및보안업무기획 · 조정규정」 모두 개정해야 한다.

2. 공공기관의 범위 확대 (안 제7조)

- 개정령안은 "현행 규정에 복잡하게 규정되어 있는 공공기관의 범위를 공공기록물법상 공공기관과 일치"시킨다는 명분으로, 법 제4조 제1항 제4호 다목에서 규정한 "대통령령으로 정하는 공공기관"의 범위, 즉 국정원의 사이버공격 및 위협에 대한 예방 및 대응 활동의 대상이 되는 기관의 범위를 확대하고 있다. 즉, 「지방자치단체 출자 · 출연 기관의 운영에 관한 법률」 제2조 제1항에 따른 출자 · 출연기관 중 해당 지방자치단체의 조례로 정하는 기관'이 추가되었고, 특별법에 의하여 설립한 법인의 범위도 일반적으로 확대되었다. 개정령안대로라면, 국정원이 사이버보안을 명분으로 더 많은 공공기관에 개입할 수 있게 된다. 그렇다고 개정령안의 기준이 「공공기록물법」상

공공기관과 정확하게 일치하는 것도 아니기 때문에, 국정원이 대상 범위를 확대하기 위한 변명일 뿐이다.

3. 각급기관에 대한 국정원의 감독 권한 확대 (안 제9조 제5항, 제10조, 제12조, 제13조, 제16조)

- 개정령안은 사이버보안과 관련해 각급기관에 대한 국정원의 감독 권한을 다음과 같이 확대 · 강화하고 있다. 이는 사실상 다른 정부부처나 공공기관에 대한 '상급기관'으로서 국정원의 위상을 유지 · 강화하는데 기여할 내용으로 보인다.
- 보안측정 및 이행결과 확인 권한 부여 (안 제9조 제5항)
    - 개정령안은 기존의 보안관리 컨설팅 권한을 보안측정(보안수준에 대한 평가) 권한으로 강화하고, 각급기관의 장이 측정 결과를 통보받은 날로부터 3개월 이내에 개선대책을 회신하도록 해 국정원이 이행여부를 확인할 수 있는 권한을 부여하고 있다. 이는 국정원의 권한을 보안에 대한 자문 역할에서 공공기관 전반의 보안 감독기구로, 국정원의 위상을 한 단계 높인 것이다.
- 사이버보안 직무교육 지원 권한 확대 (안 제10조)
    - 개정령안은 각급기관에 대해 사이버보안 직무 교육을 운영 · 지원할 수 있는 국정원의 권한을 강화했다.
- 각급기관에 대한 국정원의 진단 · 점검 권한 확대 (안 제12조)
    - 국정원은 현행 시행령상 이미 각급기관에 대한 진단 · 점검 권한을 보유하고 있으나, 개정령안은 이에 더해 국정원이 각급기관에 진단 · 점검 결과 및 조치 결과를 요청할 수 있도록 하고, 요청을 받은 각급기관은 정당한 사유가 없으면 요청에 따르도록 해 국정원의 진단 · 점검 권한을 강화했다.
- 각급기관의 사이버보안 실태 평가 권한 확대 (안 제13조)
    - 개정령안은 국정원이 각급기관의 사이버보안 현황을 파악, 분석하기 위해 각급기관의 장에게 자료의 제출을 요청할 수 있는 권한을 부여하고 있으며, 국정원의 평가 결과 통보에 대해 각급기관으로 하여금 개선 대책을 국정원에

회신하도록 요구하고 있다. 이는 사이버보안 관련 감독기관으로서의 국정원의 역할을 강화한다.

  - 또한 "국가안전보장에 지장이 없는 범위 내에서"라는 자의적 판단 기준에 따라 "종합 · 분석 결과와 평가 기준 및 결과"를 공개할 수 있도록 하고 있다(안 제13조 제6조). 국정원은 지난 10월 10일 중앙선거관리위원회 투 · 개표 관리 시스템 관련 합동 보안점검 결과를 일방적으로 발표한 바 있다. 국정원이 해당 기관과의 충분한 협의도 거치지 않고 특정한 정치적 의도나 목적에 따라 이 규정을 악용할 여지가 다분하다.

- 사고조사에 대한 감독 권한 확대 (안 제16조)

  - 개정령안은 국정원으로 하여금 사고조사의 결과 및 조치 결과를 요청할 수 있도록 하고 있다. 이 또한 국정원을 '사이버보안 업무 수행과 관련'해 정부부처나 공공기관들에 대한 감독기관으로서 위상 강화를 명문화한 조항이다.

4. 사이버보안 관련 국방부에 대한 통제 (안 제19조)

- 개정령안은 국방부 산하 기관 등에 대한 보안측정, 경보발령, 사고조사 등의 권한을 국방부장관에게 위탁할 수 있도록 하고 있으며, 국방부장관으로 하여금 "국가안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우" 관련 내용을 국정원에 통보하도록 하고 있다. 이는 국방과 관련한 사이버보안 업무조차 국정원의 관할이고, 국방부보다 상급기관의 지위에 있음을 뜻한다.

- 이는 국정원의 2017년안이나 2021년 김병기 의원이 대표발의한 「국가사이버안보법안」(의안번호: 제2113145호)에서 사이버보안에 대한 국방부의 독자적 권한을 그대로 인정한 것에 비추어봐도 후퇴했으며, 국정원이 상급기관으로서의 위상 강화 의도를 노골화한 것으로 볼 수 있다.

기타 현행 규정보다 국정원 권한을 확대 · 강화하는 사항

1. 현행 규정 제3조 제3항의 삭제

- 현행 규정 제3조 제3항에서 '사이버공격예방 · 대응업무를 수행할 때 "「정보통신기반 보호법」에 따른 주요정보통신기반시설인 경우에는 「정보통신기반 보호법」을 우선 적용"토록 하고 있는데, 개정령안은 "법률 적용의 우선순위는 법률해석에 맡긴다"는 명분으로 이 조항을 삭제했다. 해석상으로도 법률인 「정보통신기반 보호법」이 시행령보다 우선 적용되는 것이 원칙이겠으나, 해석의 명확성을 위해 시행령에 이러한 규정을 둔 취지가 있다. 굳이 국정원이 달리 해석하려는 의도가 아니라면 이 조항을 삭제할 필요가 있는지 의문이다.

2. 정보협력체계 구축의 범위 확대 (안 제5조)

- 개정령안은 사이버정보업무 수행을 위한 국정원의 정보협력체계 구축 범위를 확대하고 있다. 즉, 국내적으로는 '중앙행정기관등'을 '법 제5조 제1항에 따른 국가기관이나 그 밖의 관계 기관 또는 단체'로, 국제적으로는 '외국 정보 · 보안기관'에서 이를 포함한 '외국의 사이버안보 업무를 수행하는 기관'으로 확대하고 있다.

국정원에 대한 개혁과 민주적 통제의 필요성

국정원의 2022년안 제12조 및 제13조에서도 국회의 감독 권한을 일정하게 부여한 바 있다. 그러나 국정원이 이번 개정령안과 같이 법률이 아닌 시행령을 통해 권한의 확대 · 강화를 꾀한다면, 국회 등을 통한 민주적 통제는 더더욱 제한적일 것이다. 따라서 '국가사이버보안' 업무를 일반 정부부처인 과기부 등에 맡겨서 해당 업무에 대한 국정원의 영향력을 최소화해야 한다. 국정원 업무 전반에 대한 국회의 감독 권한이 강화되어야 하는 것은 물론이다.

국정원의 예산 전체가 '특수활동비'로 가려지거나 정부 각 행정부처 · 기관들의 예산 속으로 숨겨져 비밀주의로 일관해 온 구조부터 개혁해야 한다. 또한 국회의 예산 심의부터 한층 강화해야 한다. 국정원 직원에 대한 직무감찰, 회계검사, 적법활동 여부 등의 감찰업무를 수행할 '정보감찰관' 신설, 국회 정보위원회 산하에 정보 · 인권분야의 전문가로 구성한 '전문가형 정보기관 감독기구' 설치 · 운영, 「국회법」 제54조2 제1항의 단순위헌 결정(헌법재판소 2022. 1. 27. 결정, 2018헌마1162)에 따른 국회 정보위원회 회의의 공개 등은 매우 시급한 과제다.

무엇보다 국정원감시네트워크를 비롯해 시민사회가 오랫동안 주장해 왔듯, 국정원의 사이버보안 관련 권한은 과기부 등 타 정부부처나 기관으로 이관되어야 한다. '국가사이버보안' 업무는 비밀정보기관의 업무가 아니다. 적어도 비밀정보기관에 대한 민주적 통제가 이루어지고 있는 주요 선진국들에서는 정책 · 실무적 차원에서 '국가사이버보안'의 컨트롤 타워를 비밀정보기관들에 맡기지 않다. '국가사이버보안' 관련 업무도 일반행정부처인 과기부나 '국가사이버보안청' 등을 신설하여 이 기관에서 총괄토록 해야 한다. '국가사이버보안'과 관련한 국정원의 역할은 해외정보전담기관으로서 관련 정보의 수집으로만 제한적으로 수행토록 해야 한다.

비밀정보기관인 국정원에 '국가사이버보안' 업무를 맡기면, 투명성과 책무성을 담보하기 힘들다. '국가사이버보안'과 관련해 반드시 필요한 민간의 이해관계자들과의 원활한 소통과 협력관계를 구축하기도 어렵다. 국정원에 의한 민간 사찰과 우려가 끊임없이 제기될 수밖에 없다. 국정원에서 '국가사이버보안' 전략과 정책이 민주적으로 수립될 것이라 기대할 수도 없고, 가능하지도 않다.

'국가사이버보안'과 관련한 기본법의 제정은 필요하다. '국가사이버보안 컨트롤 타워'도 필요하고, '사이버보안' 관련 현행 법률들도 체계적으로 정비할 필요가 있기 때문이다. 다만 국정원이 제대로 된 법률적 근거도 마련하지 않고 행사하고 있는 '국가사이버보안' 권한의

이관이 반드시 전제되어야 한다. '사이버안보'를 구실로 무분별하게 권한 확대 · 강화를 꾀하는 국정원에 대한 개혁과 민주적 통제의 강화를 더는 미룰 수 없다.

국정원감시네트워크 정책자료

사이버안보 업무규정 일부개정령안
(국가정보원공고 제2023-4호)에 대한 의견서

발행일 2023. 12. 05.
발행처 국정원감시네트워크
담당
- 진보네트워크센터 오병일 대표 02-774-4551
- 참여연대 장동엽 선임간사 02-723-5302 tsc@pspd.org

이 자료는 웹사이트에서도 보실 수 있습니다.