

수사정보의 보호 및 관리에 관한 법률안

(송영길의원 대표발의)

의안 번호	21651
----------	-------

발의연월일 : 2026. 9. 30.

발 의 자 : 송영길 · 전용기 · 허종식
민병덕 · 임미애 · 박희승
김 윤 · 김남근 · 이훈기
박해철 · 서미화 · 김준환
이주희 · 조계원 · 김성범
장종태 · 모경중 · 허성무
박선원 · 진성준 · 권향엽
전은수 · 임문영 의원
(23인)

제안이유

수사기관은 수사과정에서 진술조서, 녹취자료, 전자적 의사소통 내용, 압수·수색 자료 및 디지털 포렌식 자료 등 다양한 수사정보를 취득·관리하고 있으나, 이러한 정보가 직무 목적을 벗어나 이용·제공되거나 사적으로 보관되는 것을 방지하고 그 처리과정을 체계적으로 관리할 필요가 있음.

이에 수사정보의 목적 외 이용 및 무단 제공을 금지하고, 퇴직·전보 등으로 직무상 필요가 없어진 경우 수사정보의 반환·삭제를 의무화하는 한편, 사적 저장·전송·보관을 금지하고 수사정보의 접근기록을 생성·보존하며 이상접근을 탐지·조사하도록 하는 등 수사정보의

안전한 관리체계를 마련하려는 것임.

주요내용

- 가. 이 법은 수사과정에서 취득·작성되는 수사정보의 적절한 이용과 안전한 관리에 필요한 사항을 정함으로써 수사정보의 부당한 유출 및 사적 이용을 방지하고 국민의 기본권을 보호하며 형사사법에 대한 국민의 신뢰를 확보하는 것을 목적으로 함(안 제1조).
- 나. 수사기관, 수사기관 종사자, 수사정보, 목적 외 이용 및 외부제공의 용어를 정의하고, 수사정보를 범죄수사와 관련하여 수사기관이 작성·취득·수집 또는 보관하는 정보 중 일반에게 공개되지 아니한 정보로 규정함(안 제2조).
- 다. 수사정보는 정당한 직무수행에 필요한 최소한의 범위에서 열람·이용하도록 하고, 수사정보에 대한 접근권한을 직무수행에 필요한 범위에서 최소한으로 부여하며, 수사정보의 분실·도난·유출 방지를 위한 관리계획 수립 및 기술적·관리적 조치를 하도록 함(안 제3조).
- 라. 수사기관 종사자의 정당한 직무상 필요 없는 수사정보의 열람, 목적 외 이용 및 정당한 권한 없는 외부제공을 금지하고, 퇴직·전보·휴직 또는 파견 종료 등으로 직무상 필요가 없어진 경우 수사정보의 반환 또는 삭제 및 그 이행 여부의 확인을 의무화함(안 제5조).

- 마. 퇴직한 수사기관 종사자가 재직 중 직무상 취득한 수사정보를 자신 또는 제3자의 정치적·경제적 이익이나 그 밖의 사적 이익을 위하여 이용하거나 외부제공하는 것을 금지함(안 제6조).
- 바. 수사기관 종사자가 개인 소유의 정보처리장치, 개인 전자우편계정, 승인받지 아니한 클라우드 등 사적 방법으로 수사정보를 저장·전송 또는 보관하는 것을 금지함(안 제7조).
- 사. 수사정보의 검색·열람, 출력, 복제·다운로드, 전송, 이동식 저장매체로의 저장, 기관 외부로의 반출 및 외부기관 또는 제3자에 대한 제공 등의 접근행위에 관한 기록을 전산으로 자동 생성·보존하도록 하고, 접근기록의 무단 삭제·변조·훼손을 금지함(안 제8조).
- 아. 수사정보에 대한 반복적·대량의 접근, 통상적인 업무시간 외의 비정상적인 접근 및 퇴직·전보 등의 전 대량 접근 등을 탐지하기 위한 이상접근탐지시스템을 구축·운영하도록 함(안 제9조).
- 자. 수사정보의 목적 외 이용 또는 외부제공이 의심되거나 이상접근이 탐지된 경우 수사기관의 장이 지체 없이 조사하고, 범죄혐의가 인정되는 경우 수사 및 재발 방지 조치를 하도록 하며 그 결과를 기록·보존하도록 함(안 제10조).
- 차. 수사기관의 수사정보 보호와 적정한 이용에 관한 관리·감독 업무를 총괄하는 수사정보보호책임관을 지정하도록 함(안 제11조).

수사정보의 보호 및 관리에 관한 법률안

제1조(목적) 이 법은 수사과정에서 취득·작성되는 수사정보의 적절한 이용과 안전한 관리에 필요한 사항을 정함으로써 수사정보의 부당한 유출 및 사적 이용을 방지하고 국민의 사생활과 명예 등 기본권을 보호하며 형사사법에 대한 국민의 신뢰를 확보함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “수사기관”이란 관계 법률에 따라 범죄수사에 관한 직무를 수행하는 국가기관 및 그 소속기관을 말한다.
2. “수사기관 종사자”란 수사기관에서 범죄수사에 관한 직무를 수행하거나 이를 지휘·감독·보조하는 사람 및 그 직무상 수사정보에 접근할 수 있는 사람을 말한다.
3. “수사정보”란 범죄수사와 관련하여 수사기관이 작성·취득·수집 또는 보관하는 다음 각 목의 정보 중 일반에게 공개되지 아니한 정보를 말한다.

가. 피의자·피고인·피해자·참고인 등의 진술 및 진술조서

나. 녹음·녹화 및 그 녹취자료

다. 문자메시지·전자우편·메신저 등 전자적 의사소통 내용

라. 통신사실확인자료·위치정보·금융거래정보

마. 압수·수색을 통하여 확보한 자료

바. 디지털 포렌식 과정에서 취득·복구·분석된 전자정보

사. 수사보고서, 범죄인지자료 및 수사의 단서·경과·방향 등에 관한 자료

아. 그 밖에 대통령령으로 정하는 수사 관련 비공개 자료

4. “목적 외 이용”이란 수사정보를 관계 법률에 따른 수사·공소의 제기 및 유지·재판·감사·감찰·감독 또는 그 밖의 법령상 직무 수행에 필요한 범위를 벗어나 이용하는 것을 말한다.

5. “외부제공”이란 수사정보를 해당 정보를 취급할 정당한 권한이 없는 자가 이용할 수 있도록 전달·전송·열람하게 하거나 그 내용을 알려주는 행위를 말한다.

제3조(수사정보 처리의 기본원칙) ① 수사정보는 범죄수사 등 관계 법률에 따른 정당한 직무수행에 필요한 최소한의 범위에서 열람 및 이용되어야 한다.

② 수사기관 종사자는 수사정보를 취득한 목적 외로 이용하여서는 아니 된다.

③ 수사정보에 대한 접근권한은 해당 직무의 수행에 필요한 범위에서 최소한으로 부여하여야 한다.

④ 수사기관의 장은 수사정보가 분실·도난·유출되지 아니하도록 내부 관리계획 수립, 암호화 등 기술적·관리적 조치를 하여야 한

다.

제4조(다른 법률과의 관계) 수사정보의 보호 및 이용에 관하여 「형법」, 「형사소송법」, 「개인정보 보호법」, 「공공기록물 관리에 관한 법률」 및 그 밖의 법률에 이 법보다 엄격한 규정이 있는 경우에는 그 법률을 적용한다.

제5조(수사정보의 목적 외 이용 등의 금지) ① 수사기관 종사자는 정당한 직무상 필요 없이 수사정보를 열람하여서는 아니 된다.

② 수사기관 종사자는 직무상 취득한 수사정보를 목적 외로 이용하거나 정당한 권한 없이 외부제공하여서는 아니 된다.

③ 수사기관 종사자는 퇴직·전보·휴직 또는 파견 종료 등으로 해당 수사정보를 취급할 직무상 필요가 없어진 경우 보유하고 있는 수사정보의 원본·사본·복제물 또는 이를 재현할 수 있는 전자파일을 대통령령으로 정하는 바에 따라 지체 없이 반환하거나 삭제하여야 한다. 다만, 다른 법률에 따라 이를 보유할 정당한 권한이 있는 경우에는 그러하지 아니하다.

④ 수사기관의 장은 수사기관 종사자가 퇴직·전보·휴직 또는 파견 종료 등의 사유로 해당 수사정보를 취급할 직무상 필요가 없어진 경우에는 제3항에 따라 수사정보의 사본·복제물 등의 반환 또는 삭제 여부를 확인하여야 한다.

제6조(퇴직 수사기관 종사자의 수사정보 이용 및 외부제공 금지) 수사기관 종사자였던 사람은 재직 중 직무상 취득한 수사정보의 전부

또는 일부를 자신 또는 제3자의 정치적·경제적 이익이나 그 밖의 사적 이익을 위하여 이용하거나 외부제공하여서는 아니 된다. 다만, 해당 수사정보가 적법한 절차에 따라 일반에게 공개된 경우에는 그 공개된 정보에 대하여 그러하지 아니하다.

제7조(수사정보의 사적 저장·전송·보관 금지) 수사기관 종사자는 수사정보를 다음 각 호의 어느 하나에 해당하는 사적 방법으로 저장·전송 또는 보관하여서는 아니 된다. 다만, 긴급한 직무수행을 위하여 불가피한 경우로서 대통령령으로 정하는 보안조치를 취한 경우에는 그러하지 아니하다.

1. 개인 소유의 휴대전화·컴퓨터 또는 저장장치
2. 개인 전자우편계정
3. 수사기관의 승인을 받지 아니한 클라우드 또는 온라인 저장공간
4. 그 밖에 대통령령으로 정하는 정보처리장치 또는 저장매체

제8조(수사정보 접근기록의 생성·보존 등) ① 수사기관의 장은 수사정보에 대하여 다음 각 호의 접근 행위가 이루어진 경우 그 접근 행위에 관한 사항을 전산을 통하여 자동으로 기록(이하 “접근기록”이라 한다)하도록 하여야 한다.

1. 검색 또는 열람
2. 출력
3. 복제 또는 다운로드
4. 전송

5. 이동식 저장매체로의 저장
6. 기관 외부로의 반출
7. 외부기관 또는 제3자에 대한 제공

② 접근기록에는 다음 각 호의 사항이 포함되어야 한다.

1. 행위자의 신원
2. 행위의 일시
3. 대상 정보
4. 대상 사건
5. 처리행위
6. 이용목적

③ 수사기관의 장은 접근기록을 안전하게 보존할 수 있도록 조치하여야 한다.

④ 누구든지 정당한 권한 없이 접근기록을 삭제·변조하거나 훼손하여서는 아니 된다.

⑤ 접근기록의 열람 권한은 감사·감찰·보안 또는 수사정보 보호 업무 담당자 등 대통령령으로 정하는 사람에게만 부여하여야 한다.

⑥ 접근기록의 생성·보존·열람 등에 필요한 사항은 대통령령으로 정한다.

제9조(이상접근탐지시스템의 구축·운영) ① 수사기관의 장은 수사정보에 대한 다음 각 호의 행위를 이상접근으로 탐지할 수 있는 정보시스템(이하 “이상접근탐지시스템”이라 한다)을 구축·운영하여야

한다.

1. 담당사건이 아닌 사건에 대한 반복적인 접근
 2. 단기간에 이루어지는 대량의 열람·출력 또는 다운로드
 3. 심야 등 통상적인 업무시간 외의 비정상적인 접근
 4. 퇴직·전보 또는 파견 종료 전 일정 기간 중 이루어지는 대량의 열람·복제 또는 다운로드
 5. 그 밖에 이상접근으로 보이는 대통령령으로 정하는 행위
- ② 이상접근탐지시스템의 구축·운영에 필요한 사항은 대통령령으로 정한다.

제10조(수사정보의 목적 외 이용 등에 대한 조사 등 조치) ① 수사기관의 장은 제5조에 따른 수사정보의 목적 외 이용 또는 외부제공이 있었다고 의심할 만한 상당한 사유가 있거나 제9조에 따른 이상접근탐지시스템에서 이상접근 행위가 탐지된 경우에는 지체 없이 해당 사안에 대하여 조사하여야 한다.

② 수사기관의 장은 제1항에 따른 조사 결과 범죄혐의가 있다고 인정되는 경우에는 지체 없이 수사하고 재발 방지 조치를 강구하여야 한다.

③ 수사기관의 장은 제1항에 따른 조사 및 제2항에 따른 조치의 결과를 기록하여 보존하여야 한다.

제11조(수사정보보호책임관의 지정) ① 수사기관의 장은 해당 수사기관의 수사정보 보호와 적정한 이용에 관한 관리·감독 업무를 총괄

하는 자(이하 “수사정보보호책임관”이라 한다)를 지정하여야 한다.

② 수사정보보호책임관의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

제12조(벌칙) ① 제5조제2항 또는 제6조를 위반하여 공개되지 아니한 수사정보를 목적 외로 이용하거나 외부제공한 수사기관 종사자나 수사기관 종사자였던 사람은 7년 이하의 징역 또는 7천만원 이하의 벌금에 처한다.

② 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제5조제3항을 위반하여 정당한 권한 없이 재직 중 확보한 수사정보의 원본·사본·복제물 또는 이를 재현할 수 있는 전자파일을 보유한 수사기관 종사자나 수사기관 종사자였던 사람
2. 제8조제4항을 위반하여 정당한 권한 없이 접근기록을 삭제·변조하거나 훼손한 자

③ 제7조를 위반하여 긴급한 직무수행을 위하여 불가피한 경우를 제외하고 수사정보를 사적 방법으로 저장·전송 또는 보관한 수사기관 종사자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

부 칙

이 법은 공포 후 1년이 경과한 날부터 시행한다.