유엔 프라이버시 특보 방한을 위한 한국 시민사회 보고서

프라이버시 특보 방한을 위한 시민사회단체 네트워크

보고서 발행일: 2019.7.11

유엔 프라이버시 특보 방한을 위한
한국 시민사회 보고서

프라이버시 특보 방한을 위한 시민사회단체 네트워크

건강과대안, 민주사회를위한변호사모임, 문화연대, (사)오픈넷,
성소수자차별반대무지개행동, 진보네트워크센터, 참여연대, 청소년인권행동 아수나로,
한국소비자단체협의회, 한국사이버성폭력대응센터, HIV/AIDS 인권활동가네트워크

목 차

1. 정보수사기관과 프라이버시

1) 국가정보원

1-1) 국가정보원의 사찰과 감시[1]

가. 배경 및 문제점

1) 민간인 사찰

- 현행 국정원법에 따르면 국정원이 다룰 수 있는 국내정보 범위는 보안정보에 한정되며, 그것도 대공·대정부전복·방첩·대테러 및 국제범죄조직 수집·작성 및 배포로 제한적으로 열거하고 있음[2]. 따라서 민간기업이나 시민단체 등에 대한 사찰 활동은 명백히 불법임.
- 그럼에도 국정원이 정보수집이라는 명분으로 정권에 반대하거나 비판적인 국민을 불법 사찰했다는 의혹은 끊이지 않음.
  - 독재정권과 권위주의 정부 시절 중앙정보부, 안전기획부로 불렸던 국정원은 정치적 반대세력을 제압하기 위해 감시와 통제 등을 통한 인권탄압을 일삼았음. 1998 년 김대중 정부에서 국정원으로 명칭을 변경하고 이전의 국민 통제, 사찰을 하지 않기로 함
  - 그러나 16 대 대통령선거(2002 년 12 월)을 앞둔 2002 년 9 월, 국회 정무위원회 국정감사에서 한나라당 이성헌 의원이 한화의 대한생명인수과정에서 당시의 박지원 대통령비서실장이 개입했을 가능성이 있다는 의혹을 제기함. 이 사건을 통해 국정원의 불법도청 사실이 사회적 논란이 됨. 당시 안기부가 정치인, 언론인, 기업인, 시민단체 등 사회 각층에 대한 무차별 불법도청을 했다며 국정원 도청자료 문건이 국회 국정감사에서 공개되기도 했음.
  - 2005 년 7 월, 조선일보가 안기부의 비밀조직이 불법도청을 한 사실을 보도하면서 이른바 '안기부 X 파일(또는 삼성 X 파일)' 사건이 터짐. 당시의 김승규 국정원장이 과거 비밀도청조직으로 알려진 '미림팀'의 실상을 조사하도록 지시해 김영삼 정부 당시 안기부와 김대중정부 당시 국정원이 비밀조직을 설치해 정계·재계·언론계 인사들의 대화를 불법도청한 사실이 알려짐. 검찰의 도청 수사결과 김대중 정부 시절 국정원이 통화내용을 도청했던 대상자들 중에 시민단체와 종교계 인사, 재야단체 지도부까지 대거 포함됐던 것으로 밝혀짐.

---

1 작성단체: 참여연대

2 국가정보원법 제 3 조(직무) ① 1. 국외 정보 및 국내 보안정보[대공(對共), 대정부전복(對政府顚覆), 방첩(防諜), 대테러 및 국제범죄조직]의 수집、작성 및 배포

- 2008 년 10 월 한 언론사에 의해 국정원 직원이 공기업과 사기업에 시민단체 기부내역 자료를 요구한 사실이 보도됨. 공 • 사기업에 시민단체 기부내역을 요구한 것은 국정원의 직무범위를 벗어난 정보수집으로 직권 남용에 해당함. 국정원이 정권을 반대하는 정치세력을 탄압하는 정권안보기구이자 정치사찰기구, 국민사찰기구로 사용되는 일이라며 당시 시민단체들이 강력 규탄함
- 2009 년 6 월 박원순 당시 희망제작소 상임이사는 언론과의 인터뷰에서 국정원이 자신이 상임이사로 있는 희망제작소, 아름다운재단에 후원하는 기업에 자료 요구 및 후원 중단을 요구했다는 의혹을 제기함. 박원순 변호사에 대한 사찰 의혹제기를 계기로 시민사회에 대한 다양한 불법사찰 정황이 폭로됨. 국정원이 서울시에 압력을 행사해 환경영화제 지원금 중단 요구, 한반도 대운하반대 교수모임 사찰, 4 대강 정비사업관련 대책위의 집단행동 제지, 연기군의원을 포함한 지역인사에 대한 행정복합도시 수정안 찬성 회유, 광주시에 4 대강 사업 풍자한 미술작품 철거 압력, 조계사 경내 행사 취소 요구 등을 했다는 의혹이 제기됨.
- 2010 년 5 월에는 방한한 UN 표현의자유 특별보고관 프랭크 라뤼씨를 미행하고 캠코더로 촬영하다가 발각되어 항의를 받기도 함.
- 2011 년 3 월 국보법 위반으로 수사받은 시민이 수년간 패킷감청을 당한 사실이 드러남. 이에 대해 시민단체와 피해자가 헌법소원을 제기함[3]. 국정원은 당시 헌법소원 답변서에서 지메일(@gmail.com)에 대하여 그동안 패킷감청 방식으로 감청해 왔으며, 앞으로도 이와 같은 감청을 계속하기 위하여 패킷감청이 계속되어야 한다는 주장을 하여 그동안 외국에 서버가 있는 지메일 감청이 불가능하다는 국정원의 주장이 거짓임이 드러남.
- 2012 년 12 월 전직 국정원 직원의 공익제보로 이명박 정부에서 국정원이 불법여론조작과 국민사찰을 조직적으로 실시했다는 의혹이 제기됨. 국정원 심리전단 소속 사이버팀 공무원들과 민간인 조력자들이 이명박 정부와 여당을 옹호하고 야당과 시민사회단체를 비판하는 게시물을 올리며, 다른 게시물들에 찬반표시를 작성함. 이는 사이버상 국민의 정치적 의사표현을 감시, 통제하려고 한 것임. 나아가 국정원법의 국내정치 관여불가[4] 조항을 위반한 것임
- 2013 년 5 월 민주당 진선미 국회의원에 의해 국내 정치 및 정책사안인 반값등록금 문제를 비롯해, 복지정책 확대, 해고자 복직이나 비정규 근로자 정규직 전환에 대한 정보를 국정원이 수집하고 있음이 알려짐. 특히 이 사안은 그간 알려진 대북심리국이 아니라 국익전략실이 담당한 것으로 드러나 국정원 전체가 정치공작을 벌이는 국기문란 범죄조직으로 전락했다는 비난이 거세짐. 이 사건에 대해 시민단체 등 시민 111 명이 국정원법 위반으로 고발함.

3 헌법재판소 2011 헌마 165

4 국정원법 제 9 조(정치 관여 금지)

- 비밀정보기관의 특성상, 드러난 의혹만도 이 정도면, 직무범위를 벗어난 불법사찰이 어느정도 인지는 가늠할 수가 없음.
- 국정원의 민간인 불법사찰 논란이 끊이지 않는 원인은 다음과 같음.
  - 국정원은 국가보안법 등 일부 범죄에 대해서 수사기관과 별도로 직접 수사, 체포, 구금할 수 있는 권한을 가지고 있음
  - 법률상 업무범위는 상당부분 모호하며 법률에 기반하지 않은 대통령령이나 규칙에 근거하여 권한을 행사하고 있음
  - 내국인 사찰과 같은 인권침해를 자행한 경우에도 수사기관이나 국가인권기구가 이를 독립적이고 공정하게 조사하기를 기대하기 어려움
  - 이에 대한 행정부 내부나 사법부·국회의 민주적 통제 장치가 미비하기 때문임
- 2015 년 6 월 언론보도를 통해 경력 법관 임용 예정자 또는 지원자를 대상으로 국정원이 신원조사를 했으며, 신원조사 과정에서 국가 안보와 전혀 상관없는 사회현안에 대한 견해를 물은 것이 드러남.
  - 대통령령에 해당하는 '보안업무규정' 제 3 장 '신원조사'의 33 조(신원조사) 1 항에서는 공무원임용 예정자나 비밀취급인가 예정자, 공공기관 임직원 등에 대해 "국가정보원장은 국가보안을 위하여 국가에 대한 충성심·성실성 및 신뢰성을 조사하기 위하여 신원조사를 한다."고 되어 있음.
  - 공무원 등의 결격사유를 확인하기 위해 신원조사 절차가 필요할 수도 있으나 범죄이력이나 범죄혐의, 탈세 여부 등의 공무원으로서의 결격사유를 확인하는 것은 국정원과 같은 비밀조직이 아니라 경찰청 국세청, 또는 과거 중앙인사위원회같이 공직자 인선을 위해 만들어진 조직 등에 의해서도 얼마든지 파악할 수 있음에도 여전히 이 규정은 존재하고 국정원이 이를 담당함[5].
  - 국가인권위원회는 2005 년 2 월 17 일에 법률적 근거가 미비하다는 점을 인정하고 개선할 것을 권고결정한 바 있음

2) RCS 해킹프로그램 구입 및 실행 사건

- 2015 년 7 월 이탈리아 해킹팀의 사이트가 해킹되어 고객 명단이 위키리크스에 공개됨으로써 우리나라 국가정보원이 이탈리아의 '해킹팀'이라는 업체로부터 컴퓨터와 스마트폰에 스파이웨어를 침투시켜 그 컴퓨터와 스마트폰을 감시하는 RCS(Remote Control System)를 2012 년부터 구매하고 이용해 왔다는 사실이 알려짐.
  - 당시 국정원은 대북정보수집용이라고 해명했지만 이 해킹감청프로그램을 이용해 민간인들과 정치인 등의 컴퓨터와 스마트폰 등을 불법감청했을 것이란 의심이 팽배했음.

5 보안업무규정 제 33 조(신원조사) ① 국가정보원장은 국가보안을 위하여 국가에 대한 충성심ㆍ성실성 및 신뢰성을 조사하기 위하여 신원조사를 한다.

- ❍ 실제로 해킹팀에 의해 유출된 자료에 따르면 국정원이 카카오톡이나 갤럭시 3 국내 모델을 해킹하려 했고 안랩의 'V3 모바일 2.0'과 같은 국내용 백신을 회피하기 위한 방법을 강구했으며, 서울대 공대 동창회 명부', <미디어오늘> 기자를 사칭한 천안함 보도 관련 문의 워드 파일에 악성코드를 심고자 했다고 함. 또한 네이버 맛집 소개 블로그, 벚꽃축제를 다룬 블로그, 삼성 업데이트 사이트를 미끼로 내건 주소에 '악성 코드를 심어 달라'고 요구하기도 했다고 함.
- ❍ 이는 국정원이 해킹프로그램을 통해 국민들의 컴퓨터와 스마트폰을 엿보고 프라이버시를 침해한 것임. 또한 해킹을 금지하는 정보통신망 이용촉진 및 정보보호에 관한 법률, 허가 받지 아니하는 도청을 금하는 통신비밀보호법을 위배함과 동시에 국정원법상의 직권남용 등의 규정을 위배한 것임.
- ❍ 2015 년 7 월 30 일 2,786 명의 국민고발단과 41 개 시민사회단체, 국정원 해킹사찰 의혹 검찰에 고발함. 이 사건은 아직도 수사 중. 이 사건에 대한 국회의 기술간담회는 물론 국회 정보위원회가 국정감사의 일환으로 추진하던 RCS 프로그램을 이용한 불법 해킹사찰 의혹 현장검증도 무산되는 등 국회차원의 진상조사는 제대로 이루어지지 않음.

- 이와 같은 국정원의 불법적인 해킹, 사찰 문제의 근본적인 원인은 국정원에 국내정보 수집권한과 수사권을 부여함으로써 국내문제에 개입할 여지를 직무범위에 규정해 둔 것에 있음. 따라서 국정원의 수사권과 국내정보의 수집권한을 국정원으로부터 분리하여 다른 기관으로 이관하도록 해야 할 것임.

3) 국민보호와 공공안전을 위한 테러방지법(일명 테러방지법)

- 2016 년 3 월 2 일 19 대 국회에서 통과되기 훨씬 전인 2001 년부터 국회 매 회기마다 관련 법안이 제출됨.
  - ❍ 2001 년 당시 월드컵을 앞두고 국정원이 테러방지법안을 국회 정보위원회에 제출하였으나 인권시민사회와 국가인권위원회의 반인권 및 헌법위반 우려 의견 제시 등 반대여론에 부딪혀 통과되지 못함.
  - ❍ 이후 2003 년 수정안이 제출되었고 이라크추가 파병 이후 반한감정 증가와 테러위협 증가를 명분으로 다시 국정원이 테러방지법안을 통과시키려고 하였으나 반대여론에 밀려 임기만료 폐기됨.
  - ❍ 2015 년 11 월 파리 이슬람무장단체의 테러공격을 계기로 박근혜 정부가 테러방지법안 통과를 압박하였고 결국 2016 년 3 월 테러위협을 빙자한 '국민감시법', '국정원 강화법'이라고 반대하는 다수의 국민, 시민사회의 반대에도 불구하고 국회 본회의를 통과함.
- 테러방지법의 주요 내용은, 국정원이 주도하는 '대테러센터'를 설립하는 것, '대테러센터'는 테러정보의 수집 외에 대테러활동 기획·지도 및 조정하고, 관계기관에 테러사건 대책본부를 설치하여 국정원의 지도를 받도록 하며 관계기관대책회의를 운영하고 특수부대나 군병력의 출동을 요청할 수 있도록 함.

- 실질적 내용은 포괄적인 테러라는 개념을 도입해 국정원에 국민의 금융정보, 통신기록까지 마음대로 볼 수 있도록 과도하고 포괄적인 권한을 부여하여 국민감시를 무제한 허용하는 것임.
  - ❍ 국정원은 자의적 판단으로 '테러위험인물'을 지정할 수 있고, 테러위험인물에 대한 출입국·금융거래 및 통신 이용정보, 노조·정당의 가입, 정치적 견해, 건강, 성생활 등 민간정보를 포함한 개인정보와 위치정보 등 무차별 수집이 가능함. 또한 테러위험인물에 대한 조사 및 추적권한이 부여되고, 감청사유의 확대로 인해 영장 없이 36 시간 감청할 수 있는 범위(긴급통신제한조치)도 확대됨.
- 2016 년 3 월 2 일 테러방지법이 통과된 후 박근혜 정부는 '사이버테러방지법'을 제정하려고 시도함. 2016 년 5 월에 이철우 새누리당 의원 안, 2017 년 1 월 정부안(국가사이버안보법안)이 제출됨. 국가사이버안보법안의 주요 내용은 국정원의 사이버보안 권한을 법적으로 보장하고, 기존 국가정보통신망에 대한 국정원의 사이버보안 권한을 통신사·포털 등 민간 부문으로 확대하는 것임. 이에 따라 민간부문의 정보통신망에 대한 국정원의 사찰과 감시의 가능성이 우려됨. 국정원은 침해사고 조사를 명분으로 정보통신망에 접근하여 기관과 업체의 민감한 정보 및 개인정보에 영장없이 접근할 수 있음.
- '국가안보위협 사이버 공격' 등 모호한 개념을 사용하고 있어 사이버보안을 명분으로 한 국정원의 무분별한 개입이 가능할 뿐만 아니라, 비밀정보기관인 국정원에 사이버보안에 대한 콘트롤 타워 역할을 부여하는 것은 부적절함.

나. 권고사항

- 국가정보원이 정보기관 본연의 역할을 할 수 있도록 국외정보 수집기관으로 개혁
  - ❍ 타 부처에 대한 통제권 행사의 근거가 되는 국정원의 보안업무 기획·조정권한 폐지
  - ❍ 국내정치 개입의 근거가 되는 국정원의 국내정보 수집업무 폐지
  - ❍ 범죄 수사권을 검경에 이관
  - ❍ 심리전 기능 및 심리전 수행 조직 폐지사이버보안 권한 타 부처로 이관
- 사실상 유일하게 국가정보원을 감독하는 권한을 가진 국회 정보위원회의 역할 제고 등 국회 및 민간통제 강화 방안 마련해야 할 것
- 테러방지법 폐지

다. 담당 부처 및 기관

- 청와대 국가안보실 /국가정보원

1-2) 국가정보원 사이버보안 권한[6]

가. 배경 및 문제점

- 국가정보원은 공공 정보통신망의 사이버 보안에 대한 광범위한 권한을 부여하고 있음.
  - 국가사이버안전에 대한 총괄·조정 역할
  - 공공영역의 주요 정보통신기반시설에 대한 사이버 보안 총괄[7]
  - 주요 정보통신기반시설을 포함한 공공 정보통신망에 대한 보안 관제 업무(Prevents cyber crises and detects attacks)[8]
  - 사이버침해사고 조사 및 위협정보 분석 업무(Investigation of cyber intrusions and analysis of information on threats)[9]
  - 보안적합성 검증(Security Verification Scheme)(국가·공공기관에 도입하는 정보보호시스템에 대한 안전성을 검증하는 제도)[10]
  - 암호모듈 검증(Korea Cryptographic Module Validation Program)[11]
- 그러나 국가정보원이 공공 정보통신망의 사이버보안 권한을 갖는 것은 법적 근거가 없고 정보기관으로서 기관의 역할에 적합하지 않으며, 밀행성을 특징으로 하는 활동 방식과 그동안 권한을 남용하여 민간인 사찰 등을 해왔던 행적에 비추어볼 때, 사이버 공간을 통한 불법적인 정보수집과 사찰 위험성이 큼.
- 국가정보원의 사이버보안 권한은 법적 근거가 취약함. 국가정보원법에서는 해당 권한에 대한 명시적인 규정이 없으며, 국가사이버안전관리규정은 상위법이 없는 대통령 훈령에 불과함. 정보통신기반보호법에서 국가정보원이 '정보통신기반보호위원회' 산하 '공공분야 실무위원회'를 담당하도록 하고 있으나, 이는 공공부문의 정보통신기반시설에 대한 사이버보안 업무에 한정된 것이며, 이 업무 역시 정보기관인 국가정보원이 담당할 이유가 없음.
- 국가정보원이 공공 정보통신망의 사이버보안을 담당하는 과정에서 수집할 수 있는 개인정보의 처리와 관련해서는 아무런 규정이 없음.

---

6 작성단체: 진보네트워크센터

7 정보통신기반보호법에 따라 국가정보원은 '정보통신기반보호위원회' 산하 '공공분야 실무위원회'를 맡고 있고, 공공영역의 주요 정보통신기반시설에 대한 보호대책 이행여부 확인(제 5 조의 2 1 항), 보호계획의 수립지침 작성(제 6 조 4 항), 기술적 지원(제 7 조 1 항), 취약점 분석·평가 기준 작성(제 9 조 4 항) 등을 담당하고 있다.

8 According to the homepage of National Intelligence Agency, "it constantly monitors major national computer networks and conducts simulation training". http://eng.nis.go.kr/EAF/1_7.do

9 Investigation of cyber intrusions and analysis of information on threats. In the event of a cyber intrusion against a government/public organization, including an attack by hackers, the NIS investigates the incident, ascertains its cause. and conducts information analysis on cyber threats. The NIS also has established cooperative ties with relevant organs at home and abroad. (http://eng.nis.go.kr/EAF/1_7.do)

10 Article 56 of the Electronic Government Act and Article 5 of the Enforcement Decree of the Management of Archives by Public Agencies

11 국가·공공기관 정보통신망에서 사용되는 암호모듈을 검증하는 제도. Article 69 of the Enforcement Decree of the Electronic Government Act and the Cryptographic Module Testing and Validation Guidelines.

- 보안 관제 업무(Prevents cyber crisis and detects attacks)와 같은 일상적인 네트워크 감시 업무를 국가정보원이 담당하는 것은 부적절함. 정보기관의 은밀한 감시와 정보수집을 억제할 아무런 보호장치가 없기 때문임.
- 국가정보원은 사이버침해사고 조사 및 위협정보 분석 업무(Investigation of cyber intrusions and analysis of information on threats)를 수행하는데, 여기에는 영장주의도 적용되지 않음. 국가정보원이 암호 모듈을 검증하기 때문에, 기업들은 국가정보원에 소스코드까지 제출해야 함. 이를 통해 국가정보원은 암호 시장에 대한 통제력을 가지고 있는데, 비밀정보기관이 이러한 업무를 담당하는 것은 암호에 대한 신뢰성을 저해할 수 있음.

나. 권고사항

- 공공 정보통신망에 대한 사이버 보안은 필요하지만, 비밀정보기관인 국가정보원이 이를 담당하는 것은 적절하지 않음. 공공 정보통신망에 대한 사이버 보안 권한을 다른 정부부처로 이관할 필요가 있음.

다. 담당 부처 및 기관

- 국가정보원
- 청와대 국가안보실

2) 기무사

2-1) 기무사의 세월호참사 유가족 사찰[12]

가. 배경 및 문제점

- 2014 년 4 월 16 일 전라남도 진도군 조도면 부근 해상에서 여객선 세월호가 침몰하면서 승객 304 명(대부분이 학생)이 사망하거나 실종되었음(이하 '세월호 참사').
- 세월호참사 희생자들의 유가족들은 세월호참사에 대한 진상규명과 책임자처벌을 요구해왔지만 아직까지 명확한 침몰원인은 밝혀지지 않았고, 관련 책임자 처벌도 이루어지지 않고 있음(정부관계자는 1 인만이 처벌되었음).
- 박근혜 전 정부 산하 국가 권력기관은 세월호참사의 진실을 조사하기 위해 설립된 세월호참사 특별조사위원회를 강제해산하는 등 조직적으로 세월호 참사의 진상규명 및 책임자 처벌을 방해하였음.
- 이번 정부에 구성된 민관 합동 조사팀은 기무사가 세월호 참사 다음 날인 2014 년 4 월 17 일부터 소속 부대원에게 세월호 참사 희생자 유가족들의 동향을 파악하라 지시하였음.

12 작성단체: 민주 사회를 위한 변호사 모임

- 기무사는 유가족들의 생년월일, 휴대전화, 포털 활동, 개인 블로그 주소, 전자우편, 인터넷 물품구매내역, 주민등록증, 통장사진 등을 수집하였고, 현장에 사찰하는 요원들에게 유가족으로 신분을 위장하라는 등 지침을 내리기까지 하였음.
- 특히 기무사는 진상규명과 책임자 처벌을 요구하는 세월호 유가족들을 '종북세력'으로 분류하고, 언론에 허위사실을 유포하는 등의 국가범죄를 자행하였음.
- 그럼에도 불구하고 국방부 특별수사단이 2018 년 11 월 발표한 수사결과에 따르면 피의자 중 5 명만이 정식 기소되고, 나머지 4 명이 기소 유예되었음.

나. 권고사항

- 기무사의 세월호참사 유가족 사찰에 대한 철저한 진상조사와 책임자 처벌이 이루어져야 함.
- 세월호참사 유가족 사찰과 같은 범죄행위가 재발하지 않도록 독립적인 감독 체제 등 구체적인 재발방지대책이 마련되어야 함.
- 세월호참사 유가족들의 진실, 정의, 배상의 권리가 보장되어야 함

다. 담당 부처 및 기관

- 국방부
- 군사안보지원사령부 (구 기무사)

2-2) 기무사의 불법감청[13]

가. 배경 및 문제점

- 국군기무사령부는 국방부 산하의 정보수사기관으로 군사에 관한 정보 수집 및 군사 보안 및 방첩, 범죄 수사를 목적으로 함. 그러나 박근혜 정부 당시인 2014 년 세월호 침몰 사고 발생 직후 실종자 가족에 대한 사찰, 2017 년 촛불집회 당시 계엄령 준비 등이 논란이 되어, 2018 년 9 월 해체되고 군사안보지원사령부로 개편됨.
- 민주평화당 천정배 의원이 2019 년 4 월 8 일, 국군기무사령부가 작성한「세월호 TF」 일일보고서를 공개하면서, 박근혜정부 시절 기무사가 일반 시민 다수의 통화를 무작위로 불법감청한 것이 드러남.
- 기무사는 2014 년 6 월 10 일부터 2014 년 7 월 22 일까지 서울, 하남, 성남, 용인, 안성 등에서 자체 보유한 기동방탐장비 또는 미래부(현 정통부) 산하 전파관리소의 전파감시설비를 이용하여 법원의 허가 없이 민간의 통신내용을 불법적으로 청취, 녹음하였음. 택시, 병원, 놀이터, 영화관 등 민간의 대화 내용이 무차별적으로 도청되었음이 드러남.[14]

---

13 작성단체: 진보네트워크센터

14 JTBC, 세월호 직후, 민간인 불법감청…영화관·식당 등 무차별 도청. 2019.4.8

- 세월호 실 소유주인 유병언에 대한 수사는 군 정보기관인 기무사의 직무 범위를 벗어나는 것이며, 법원의 허가없이 감청을 한 것은 통신비밀보호법을 위반한 불법 감청에 해당함.
- 전파관리소의 업무는 '전파법 제 49 조 내지 제 51 조의 규정에 의한 혼선제거 등 전파질서유지를 위한 전파감시'로서 전파관리 외의 목적으로 타인의 대화 내용을 녹음하는 것은 불법감청에 해당함. 기무사는 검찰에 전파관리소를 활용하여 감청할 것을 제안했고, 대검은 실제로 업무협조를 요청하고 실행한 것으로 나타남. 이는 검찰과 미래부 역시 불법행위에 가담한 것이며, 불법 행위를 단속해야 할 자신의 임무를 방기한 것임.
- 2019 년 4 월 15 일, 시민사회단체는 기무사 등 불법감청 관련 대상자를 검찰에 고발하였음.

나. 권고사항

- 기무사의 불법감청에 대한 철저한 진상조사와 처벌이 이루어져야 함.
- 기무사가 자신의 권한을 벗어나서 불법적인 민간인 사찰과 감청을 할 수 없도록, 기무사에 대한 독립적인 감독 체제가 마련되어야 함.

다. 담당 부처 및 기관

- 군사안보지원사령부 (구 기무사)
- 과학기술정보통신부 (구 미래창조과학부)
- 전파관리소

3) 경찰

3-1) 수사정보 시스템[15]

가. 배경 및 문제점

- 2017 년 국정감사 자료에 따르면 경찰은 83 개 데이터베이스시스템에 개인정보 37 억건을 보유하고 있음[16]. 그러나 자세한 현황은 국회도 파악하고 있지 못함.
- 채증시스템 등 대부분의 경찰 데이터베이스시스템 구축·운영이 구체적인 법률적 근거를 두고 있지 않음. 다만 형사사법정보 시스템, 디엔에이신원확인정보 시스템 등 아주 소수의 시스템의 경우에만 구체적인 법률적 근거를 두고 있음.

15 작성단체: 진보네트워크센터

16 뉴시스. (2017). *경찰, 개인정보 37 억건 보유… 형사사법정보시스템 27 억건*. http://www.newsis.com/view/?id=NISX20170114_0000117579 [2019.5.15].

- 법률적 근거 없이 운영되는 이들 경찰 시스템과 그 안의 개인정보들은 다른 목적으로 이용되거나 다른 시스템과 연계되는데 취약하고 점점 더 많이 자동인식(automatic identification)되고 있음
- 결과적으로 경찰의 대규모 개인정보 데이터베이스시스템 및 개인정보 처리에 대하여 법률에 따른 통제가 이루어지고 있지 못하고 있음. 국민들은 경찰 시스템에 대하여 그 수집항목 등 정확한 실태를 알 수 없을뿐더러 자신의 개인정보에 대한 열람, 정정, 삭제 및 처리중지권 등 권리를 행사하지 못하고 있음
- 1999 년 사회단체 활동가들이 구체적인 법률적 근거 없이 경찰이 17 세 이상 전국민의 열손가락 지문날인 정보를 수집하여 데이터베이스 시스템으로 구축, 운영하는 데 대하여 헌법소원을 제기하였음. 그러나 헌법재판소는 2005 년 경찰법 및 경찰관직무집행법에 경찰의 직무에 "치안정보의 수집, 작성 및 배포"가 포함되어 있다는 이유로 기각됨[17].
- 이후로 법원 및 헌법재판소는 모든 경찰 시스템에 대하여 같은 태도를 고수해 옴. 2010 년 사회단체 활동가들이 구체적인 법률적 근거 없이 경찰이 모든 피의자, 참고인은 물론 피해자 정보를 방대하게 수집하여 데이터베이스 시스템(CIMS: Crime Information Management system)으로 구축, 운영하는 데 대하여 손해배상 소송을 제기하였음. 그러나 법원은 원고패소 판결을 내림[18].
- 2018 년 경찰개혁위원회는 “경찰 정보시스템 구축과 운영에 대해서는 그 근거, 절차와 방식 및 통제에 관한 별도의 구체적인 법률상 근거를 마련. 경찰 내외부에 공개하지 않는 정보시스템은 구축운영 금지”할 것을 권고하였으나 그에 대한 개선이 이루어지고 있지 않음.

나. 권고사항

- 경찰이 운영 중인 개인정보 데이터베이스시스템에서 개인정보를 처리하는 목적, 절차, 방식 및 통제장치를 구체적으로 규정된 법률에 따른 통제를 받을 것.
- 경찰 개인정보 데이터베이스시스템에 대하여 독립적인 제 3 의 기관으로부터 감독을 받을 수 있도록 제도를 개선할 것.

다. 담당 부처 및 기관

- 경찰청

3-2) 경찰의 수배차량 검색시스템[19]

17 헌재 2005. 5. 26. 99 헌마 513 등

18 대법원 2012. 10. 25. 2012 다 12641

19 작성단체: 참여연대

가. 배경 및 문제점

- 경찰은 범죄정보관리, 범죄첩보, 우범자첩보 등 광범위한 개인정보를 수집하고 정보시스템으로 집적하고 있지만 목적에 따른 수집, 사용 및 제한에 대해 구체적으로 규정한 법률적 근거를 두고 있음
- 수배차량검색시스템의 경우 2015 년 10 월 제정된 경찰의 자체적인 운영지침만[20]으로 구축 운영되며 1 일 2 천 4 백만 건 이상 무고한 국민의 자동차 이동경로 정보를 수집하여 30 일간 보관하고 있고, CJ 대한통운 민간 택배회사와 MOU 를 맺어 블랙박스 영상까지 제공받고 있음[21].
- 이와 같이 경찰이 국민의 개인정보를 방대하게 수집, 집적하고 있음에도 그 법률적 근거는 '치안정보의 수집·작성 및 배포' 라는 일반규정 또는 자체적인 규칙 혹은 지침에 의해서 관행적으로 개인정보를 처리하고 있는 실정임.
- 특히 '긴급 수배'의 경우 차량번호판의 문자나 숫자 가운데 2 개만 입력해도 '유사 검색'을 할 수 있도록 설계되었다고 함. 수배 차량 번호와 비슷한 번호의 차량을 갖고 있다면 누구라도 수사선상에 올라 차량 이동 경로가 고스란히 드러날 수 있음. 세월호 참사가 발생했던 2014 년 경찰은 수배 중이던 유병언 전 세모그룹 회장을 추적한다며 스마트폰 내비게이션 앱을 통해 특정 지명을 검색한 일반 시민들의 개인정보까지 무작위로 들여다본 사실이 드러나 논란이 되기도 했음. 또한 경찰은 2014 년 철도노조파업 참가 조합원을 추적하면서 수배차량 검색체계도 사용하면서 당사자뿐 아니라 삼촌이나 고모 등 일가 친지의 차량까지 일정 시점 기준 이전 석 달 간 어느 지역에서 운행되었는지를 검색했다고 함.
- 이처럼 아무런 법적 통제장치 없이 운영되는 수배차량 검색시스템은 '저인망식' 수사나 마구잡이 조회에 악용될 가능성이 있으며 국민의 사생활을 감시, 통제하는 강력한 사찰 수단이 될 수 있음.
- 개인정보의 수집·작성 및 배포는 "법률에 특별한 규정"이 있거나 직무의 수행을 위하여 "불가피한 경우"에 한하여 허용됨. 그러나 경찰의 수배차량 검색시스템은 법률유보원칙과 필요최소한도만 수집해야 하는 비례성의 원칙을 위반하는 것임.
- 이에 대해 시민사회는 민간 통제, 정보시스템의 운용현황에 대한 보고서 작성 및 국회보고, 정보시스템의 연동, 열람, 조회 등 노드(근거리 통신망)에 대한 절차통제규정 등의 법적 장치가 필요하다고 주장해 옴

나. 권고사항

- 모든 경찰의 개인정보 수집 및 집적은 국회를 통한 사회적 토론과 입법적인 통제 방안이 마련되어야 함. 이에 수배차량검색 시스템 운영의 법률적 근거를 마련하고 법적

---

20 https://www.police.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000083492&fileSn=1&bbsId=B0000032

21 http://news.donga.com/3/all/20160616/78695611/1

통제장치에는 반드시 정보시스템에 대한 민간통제, 운용현황에 대한 연간 보고서(백서)의 작성 및 국회보고, 정보시스템의 연동, 열람, 조회 등 노드에 대한 절차통제규정을 포함해야 할 것임

다. 담당 부처 및 기관

- 행정안전부/경찰청

3-3) CCTV 통합관제센터[22]

가. 배경 및 문제점

- 현재 지방자치단체가 설치.운영하는 CCTV 통합관제센터는 관내 설치된 여러 공공기관들의 CCTV 를 회선으로 연결, 모든 영상을 한 곳에서 확인할 수 있음.
- 행정안전부에 따르면, 2017 년 말 현재 전국 226 개 기초지방자치단체 중 통합관제센터를 설치.운영하는 곳은 총 208 개(92%). 향후 모든 지자체에 센터 구축 지원을 목표로 하고 있고, 2019 년 속초시, 평창군, 화천군, 양양군, 진도군 등 5 개 시군에 CCTV 통합관제센터 구축사업이 진행중임.

<CCTV통합관제센터 설치 현황>

(단위 : 시군구 개수)

구분		최근 통계치							
		~2010	2011	2012	2013	2014	2015	2016	2017
통합관제센터 구축 수		26	34	27	33	29	22	19	18
	누계	26	60	87	120	149	171	190	208

※ 2010년에는 2010년 이전 구축 수를 포함한 수치임

- CCTV 통합관제센터내에 지자체 내에 설치된 CCTV 들을 연결해 촬영영상을 확인, 저장하는 방식으로 운영하고 있고, 대다수의 통합관제센터에 경찰관이 상시근무하면서 범죄상황발생 등에 대응하고 있기도 함
- 2017 년 경찰청 자료에 따르면, 경찰과 지방자치단체(CCTV 통합관제센터) 사이에 영상정보 공유시스템이 구축되어 있고, 경찰서 상황실에서 CCTV 통합관제센터의 영상을 열람할 수 있으나, 2014 년 9 월 29 일 개인정보보호위원회의 결정 이후[23] 범죄수사, 재난관리, 군사훈련 등을 위해서 실시간 제공받고 있음..

---

22 작성단체: 참여연대

23 개인정보위원회 2014.9.29. 결정 <제 **2014-19-20** 호>

연번	지방청	경찰서	지자체 통합관제센터	설치 장소	시스템 접근 가능 PC
1	서울청	용산서	용산 통합관제센터	경찰서 상황실	1
2	서울청	성북서	성북 통합관제센터	경찰서 상황실	1
3	서울청	성동서	성동 통합관제센터	경찰서 상황실	1
4	서울청	강북서	강북 통합관제센터	경찰서 상황실	1
5	서울청	금천서	금천 통합관제센터	경찰서 상황실	3
6	서울청	중랑서	중랑 통합관제센터	경찰서 상황실	1
7	서울청	강동서	강동 통합관제센터	경찰서 상황실	2
8	서울청	종암서	성북 통합관제센터	경찰서 상황실	1
9	서울청	양천서	양천 통합관제센터	경찰서 상황실	1
10	서울청	송파서	송파 통합관제센터	경찰서 상황실	1
11	서울청	방배서	서초 통합관제센터	경찰서 상황실	1
12	서울청	도봉서	도봉 통합관제센터	경찰서 상황실	1
13	서울청	수서서	강남 통합관제센터	경찰서 상황실	1
14	대구청	달성서	달성군 통합관제센터	경찰서 상황실	4
15	대구청	수성서	수성구청 통합관제센터	경찰서 상황실	4
16	인천청	중부서	중구 관제센터 동구 관제센터 옹진군 관제센터	경찰서 상황실	1
17	인천청	남부서	남구 통합관제센터	경찰서 상황실	1
18	인천청	남동서	남동구 통합관제센터	경찰서 상황실	1
19	인천청	부평서	부평구 통합관제센터	경찰서 상황실	1
20	인천청	삼산서		경찰서 상황실	2
21	인천청	계양서	계양구 통합관제센터	경찰서 상황실	1
22	인천청	강화서	강화군 통합관제세너	경찰서 상황실	2
23	인천청	연수서	연수구, 경제청	경찰서 상황실	2
24	경기남부청	수원중부	수원시 통합관제센터	경찰서 상황실	2
25	경기남부청	수원남부		경찰서 상황실	2
26	경기남부청	수원서부		경찰서 상황실	2
27	경기남부청	안양동안	안양시 통합관제센터	경찰서 상황실	1
28	경기남부청	안양만안		경찰서 상황실	2
29	경기남부청	군포	군포시 통합관제센터	경찰서 상황실	1
30	경기남부청	부천소사	부천시 통합관제센터	경찰서 상황실	1
31	경기남부청	부천원미		경찰서 상황실	1
32	경기남부청	부천오정		경찰서 상황실	1
33	경기남부청	광명	광명시 통합관제센터	경찰서 상황실	1

34	경기남부청	안산단원	안산시 통합관제센터	경찰서 상황실	1
35	경기남부청	안산상록		경찰서 상황실	1
36	경기남부청	시흥	시흥시 통합관제센터	경찰서 상황실	1
37	경기남부청	화성동부	오산시 통합관제센터	경찰서 상황실	1
38	경기남부청	용인동부	용인시 합동관제센터	경찰서 상황실	1
39	경기남부청	용인서부		경찰서 상황실	4
40	경기남부청	광주	광주시 통합관제센터	경찰서 상황실	1
41	경기남부청	과천	과천시 통합관제센터	경찰서 상황실	2
42	경기남부청	하남	하남시 통합관제센터	경찰서 상황실	1
43	경기남부청	이천	이천시 통합관제센터	경찰서 상황실	1
44	경기남부청	김포	김포시 통합관제센터	경찰서 상황실	1
45	경기남부청	여주	여주시 통합관제센터	경찰서 상황실	2
46	경기북부	동두천서	동두천시 통합관제센터	경찰서 상황실	1
47	강원청	원주서	원주시 도시정보센터	경찰서 상황실	1
48	강원청	정선서	정선군 CCTV 통합관제센터	경찰서 상황실	1
49	강원청	홍천서	홍천군 CCTV 통합관제센터	경찰서 상황실	1
50	전북청	완산서	전주시 통합관제센터	경찰서 상황실	2
51	전북청	덕진서			
52	전북청	완주서	완주군 통합관제센터	경찰서 상황실	1
53	경북청	예천서	예천통합관제센터	경찰서 상황실	1
54	제주청		제주도 CCTV 통합관제센터	112 종합상황실	1
55	제주청	동부서		경찰서 상황실	1
56	제주청	서부서			1
57	제주청	서귀포서			1

- 국가인권위원회는 CCTV 촬영 영상을 모두 수집.저장.이용하는 통합관제센터는 개인정보 침해 소지가 있음에도 「개인정보 보호법」이나 기타 관련 법률에 설치와 운영 근거를 두고 있지 않고, CCTV 로 촬영한 영상을 당초 설치 목적과 다른 목적으로 이용하거나 특히 범죄 수사 등을 위해 경찰에 제공하는 경우가 빈번하고, 경찰관이 상주 근무하면서 영상을 모니터링하는 사례가 많은 것으로 확인돼, 2018. 5. 3. 행정안전부장관에게 “헌법 기준에 부합하도록 CCTV 통합관제센터 설치.운영의 법률적 근거를 마련하고, 범죄 수사 등

개인영상정보의 이용과 제 3 자 제공에 대한 구체적 요건.절차.대상기관, 개인영상정보의 안전성 확보 방안 등도 보다 상세히 법률에 반영할 것"[24]을 권고하기도 함.

- 현행 개인정보보호법상 CCTV 통합관제센터에 관한 근거규정 없음
  - ❍ 개인정보보호법 등 관련법령상 CCTV 통합관제센터의 설치 및 운영에 관한 규정없음
  - ❍ 행정안전부 고시 <표준 개인정보 보호지침> 등을 두고 있으나, 광범위하게 설치된 CCTV 에 의해 수집저장되는 영상정보 중에는 개인의 초상, 행동, 기호, 사생활 등에 관한 정보가 포함되어 있고 영상장비의 고도화로 인해 개인식별은 물론이고 그 행동까지 감시할 수 있는 수단으로 활용될 수 있다는 점에서 기본권제한의 기본원칙상 법률에 의해 필요최소한에 그쳐야 함에도 관련규정 없음
- 개인영상정보법(안)의 문제점
  - ❍ 국가인권위는 행안부의 개인영상정보법(안)에 대해 통합관제센터 설치목적, 개인영상정보 처리절차, 목적외 사용 및 제 3 자 제공의 목적/요건/절차 등이 구체적으로 규정되지 않아 국민의 인권침해를 최소화하기 위한 법률로서 부족하다는 점을 지적하였음
  - ❍ 개인영상정보법(안)은 영상정보의 활용에만 방점을 두고, 기본권을 침해할 수 있다는 전제에서 그 침해를 최소화하기 위한 절차, 활용의 목적/필요성, 제공대상기관/절차 등에 관해 규정하고 있지 않아 실질적인 기본권 보호장치로 기능하기 어려움

나. 권고사항

- CCTV 통합관제센터를 운영하는 것, CCTV 통합관제센터에서 영상을 다른 기관과 실시간으로 공유하는 것에 관하여 법률에 그 목적, 요건, 절차 등을 엄격하게 규정하고 이에 관한 통제절차를 마련할 것

다. 담당 부처 및 기관

- 행정안전부, 경찰청

3-4) 정보경찰[25]

가. 배경 및 문제점

- 한국 경찰의 경우 경찰법 제 3 조 제 4 항, 경찰관직무집행법 제 2 조 제 4 항 "치안정보의 수집·작성 및 배포"라는 포괄적인 수권 규정에 의해 범죄수사와 관련이 없는 정보를

24 국가인권위원회 상임위원회 결정 2018.5.3. "폐쇄회로 텔레비젼 통합관제센터 설치 및 운영에 대한 개선권고"

25 작성단체: 진보네트워크센터

광범위하게 수집하는 부서를 운영해 왔다. 나아가 경찰 정보 부서는 정부를 비판하는 국민을 사찰하고 집권자의 통치를 위해 정치적인 보고서를 작성해 왔음.

- 언론보도[26]에 따르면 2018 년 정보경찰의 업무 중 제일 많은 비중을 차지한 건 청와대에 보내는 '정책자료'의 작성(22.5%)이었음. 대외협력(20%), 집회관리(12.3%)가 그 뒤를 이었으며, 본연의 업무라 할 수 있는 '범죄첩보'는 단지 1.3%에 불과했음. '치안정보'라고 한다면 위험방지나 범죄수사와 관련이 되어야 함에도 그에 해당하지 않는 정보들을 불법적으로 광범위하게 수집한 증거라 할 수 있음.
- 정보경찰은 그동안 국민 개개인의 정보를 수집하고 이를 활용해 왔음. 그 과정에서 무분별한 개인의 사생활 침해가 발생했으며, 정보 주체 본인이 사찰의 대상이 되었는지 인지 할 수 있는 장치도 없음.
- 정보경찰의 민간인 사찰 증거가 계속해서 나오고 있음. 2019 년 5 월 14 일 경찰인권침해진상조사단에 따르면 삼성전자서비스 염호석 노동자의 경우 노조 탄압에 반발해 파업을 하다가 죽음을 택함. 이후 정보경찰은 해당 기업과 결탁하여 노동자의 가족 및 지인들까지 감시하였음.[27] 뿐만아니라, 안산 단원고에서 진도 팽목항까지 걸어가는 도보 순례를 하는 세월호 참사 유가족들을 미행하다 발각되기도 함.[28]
- 민간인뿐 아니라 국가 공무원이나 국회의원들에 대한 감시도 진행했음. 각 의원들의 성격을 분석해 정부 및 여당이 대응해야 할 방향을 제안하는 등 정권에 부담이 되는 이들이라면 전부 감시하고 분석함.
- 정보경찰은 선거에도 적극 개입함. 2011 년 당시 서울시장 선거에서 여당후보를 당선시키기 위해 상대 후보 동향을 파악하고 관련 시민단체를 사찰하였으며, 선거 판세를 분석하여 선거 전후 청와대의 국정 운영 방안을 제안하는 등 노골적인 정치 행보를 펼쳤음.[29] 박근혜 정부 시절, 여당 의원들의 성향을 파악하여 이들을 경찰에 우호적인 입장으로 바꾸기 위한 전략을 찾아내려고 했음.[30]
- 이명박 정부 시절에는 해당 정부의 성공을 기원하며 '전위대'로 자신들을 사용해 달라고 스스로 요청하기까지 했으며, 그 대가로 정무직 자리를 요구했다는 문건을 작성했음.[31] 해당 문건에는 '경찰이 역대 어느 정부보다 현정부(이명박 정부)의 성공을 기원' 한다고 언급했음.

---

26 KBS(2019), *범죄 정보 1.3%…"경찰 정보국 폐지 권고에 청와대는 반대".*
http://news.kbs.co.kr/news/view.do?ncd=4149872&ref=A [2019.5.17]

27 한겨레(2019), *고 염호석 사건, 정보경찰 처음부터 끝까지 삼성 손발 구실했다,*
http://www.hani.co.kr/arti/society/society_general/893837.html [2019.5.17]

28 한겨레(2014), *[단독] 사복 경찰 또 세월호 유가족 미행하다 '들통',*
http://www.hani.co.kr/arti/society/society_general/646775.html [2019.5.17]

29 한겨레(2019). *[단독] 정보경찰, 서울시장 보선 때 '나경원 비선캠프'자임 활동,*
http://www.hani.co.kr/arti/society/society_general/892328.html [2019.5.17]

30 한겨레(2019). *정보경찰, '의원 관리카드' 만들어 인맥 사찰,*
http://www.hani.co.kr/arti/society/society_general/881576.html [2019.5.17]]

31 경향신문(2019), *MB 정권 경찰, '전위대' 자처하며 충성 서약,*
http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201905130600015 [2019.5.17]

뿐만아니라, 해당 문건을 통해 '대선 때 절대다수의 경찰 고위직 인사들이 이명박 후보의 선거대책위에서 활동하며 현직 경찰관에도 영향을 미쳤다'는 내용도 확인할 수 있음.

나. 권고사항

- 범죄수사와 무관한 '정보경찰'을 폐지하고, 그동안 정보경찰이 자행해 온 민간인 사찰 및 선거 개입에 대해 철저히 진상조사를 진행하고 관련 책임자들을 처벌해야 한다.
- 범죄수사를 위한 경찰의 정보활동의 경우 독립적인 기구에 의한 통제와 감독을 강화해야 한다.

다. 관련 부처 및 기관

- 경찰청

4) 문화계 블랙리스트[32]

가. 배경 및 문제점

- 2016 년 11 월, 대한민국의 문화예술인들은 박근혜 정부의 문화예술계 블랙리스트 국가범죄를 폭로하며 약 5 개월 동안 광화문 광장을 점거하고 예술행동을 실천했다. 이 과정에서 문화예술인들은 박근혜, 김기춘, 조윤선 등 주요 정부 인사들을 특검에 고발했다.
- 대한민국 정부는 '문화예술계 블랙리스트 진상조사 및 제도개선 위원회'(2017 년 7 월부터 2018 년 6 월까지) 활동을 통해 이명박·박근혜 정부 시기의 문화예술계 블랙리스트 국가범죄 사실을 공식적으로 확인하고 공표했다.
- 수사권이 없는 조건에도 불구하고 위원회가 밝혀낸 이명박·박근혜 정부 시기 문화예술계 블랙리스트 국가 범죄는 "단체 342 개, 문화예술인 8,931 명"에 이른다. 또한 위원회는 문화예술계 블랙리스트 국가 범죄가 당시 청와대, 국가정보원, 경찰, 문화체육관광부는 물론 대다수의 정부 문화예술 기관을 통해 일상적으로 자행되어 왔다는 사실을 밝혔다.
- 위원회는 대한민국 정부에게 문화예술계 블랙리스트 진상조사와 재발방지를 위해 '책임규명'(책임자 처벌 관련 수사 및 징계 의뢰 131 명), '제도개선 및 후속조치'(법제도 및 기관 개혁 관련 9 개 권고안)을 권고하였다.
- 위원회의 조사결과에 따르면 대한민국 정부(청와대, 국가정보원, 경찰, 문화체육관광부, 문화예술공공기관 다수)는 이명박-박근혜 정부 기간 동안 블랙리스트 정책을 통해 문화예술인들의 개인정보를 불법적이고 일상적으로 취합, 관리했던 것으로 밝혀졌다.
- 특히 대한민국 정부는 문화예술인들의 민감정보(정치적 성향 등)을 불법적으로 취급하며 문화예술인들에 대한 검열, 지원배제 등을 자행하였다.

32 작성단체: 문화연대

나. 권고사항

- 대한민국 정부는 개인정보 침해를 비롯하여 문화예술계 블랙리스트 국가 범죄의 온전한 진실을 밝히기 위해 (가칭)<문화예술계 블랙리스트 진상규명을 위한 특별법>을 제정과 (수사권과 조사권이 보장된) 진상규명 위원회 활동 계획을 제시하라.
- 대한민국 정부는 <문화예술계 블랙리스트 진상조사 및 제도개선 위원회>의 권고를 책임 있게 이행하기 위한 실행 계획을 제시하라.

다. 담당 부처 및 기관

- 정부: 청와대, 국정원, 경찰, 문화체육관광부 외
- 문화체육관광부 소속 문화예술공공기관 다수(문화예술계 블랙리스트 실행 기관)

2. 통신비밀

1) 패킷감청[33]

가. 배경 및 문제점

- 인터넷 회선에 대한 감청(패킷감청)은 유선 또는 모바일 특정회선을 사용해 주고받는 모든 정보를 가로채 지득하는 것임. 특정 회선을 통해 오가는 모든 정보를 가로채가기 때문에 하나의 회선을 여러 명이 사용하는 경우 수사대상이나 정보수집대상인 사람 외에 다른 사람의 통신내용까지 감청하게 됨
- 현재 패킷감청 기술로는 감청대상자의 정보만 선별하는 것이 불가능하고, 감청대상자의 정보 중에서 범죄 관련 정보만 선별하는 것 역시 불가능하므로 현행 통신비밀보호법이 요구하는 대상자 제한, 수집하는 정보 제한이라는 요건을 충족하기 어려움.이런 기술적 한계에도 불구하고 패킷감청에 대한 법원의 감청허가가 이루어지고 있고, 이 허가에 따라 수사기관은 패킷감청을 수사상 정보획득 수단으로 활용해 왔음
- 2008 년 이후 2014 년까지 새로 인가된 전체 감청 설비 73 대 가운데 71 대가 인터넷 감청 설비였다는 사실이 밝혀진 바도 있으며 이마저도 국가정보원이 보유한 설비는 포함되지 않은 숫자임. (2014 년 유승희 국회의원 국정감사 자료) 통비법은 정보수사기관이 감청장비를 도입하는데는 특별히 인가절차를 요구하지 않으며 분기별 국회 정보위원회에 통보하도록 하는 것이 전부임.
- 현재 감청 중 패킷감청이 어느 정도 비율로 이루어지는지 공개되고 있지 않으나 2018 년 한해 기준 전체 감청의 약 99.4%를[34] 국가정보원이 하고 있어 패킷감청 역시 대부분 국가정보원에 의해 이루어지는 것으로 추정하고 있음.
- 직접 수사대상이 아닌 사람이 개통한 인터넷회선에 대해 통신제한조치(감청)을 허가 받아 패킷감청을 한 사례에 대해 헌법재판소는 “불특정 다수가 하나의 인터넷회선을 공유하여 사용하는 경우가 대부분이므로, 실제 집행 단계에서는 법원이 허가한 범위를 넘어 피의자 내지 피내사자의 통신자료뿐만 아니라 동일한 인터넷회선을 이용하는 불특정 다수인의 통신자료까지 수사기관에 모두 수집·저장된다. 따라서 인터넷회선 감청을 통해 수사기관이 취득하는 개인의 통신자료의 양은 전화감청 등 다른 통신제한조치와 비교할 바는 아니다. 인터넷회선 감청은 집행 및 그 이후에 제 3 자의 정보나 범죄수사와 무관한 정보까지 수사기관에 의해 수집·보관되고 있지는 않는지, 수사기관이 원래 허가받은 목적, 범위 내에서 자료를 이용·처리하고 있는지 등을 감독 내지 통제할 법적 장치가 강하게 요구된다”라고 판시하면서 인터넷회선감청에 대한 통제장치가 마련되지 않은 상태에서 이를 허용하는 것은

33 작성단체: 참여연대

34 과학기술정보통신부 2019.5.10.보도자료 <2018 년 하반기 통신자료 및 통신사실확인자료 제공 등 현황 발표>

개인의 통신 및 사생활의 비밀과 자유를 침해하는 것으로 위헌이라는 취지로 헌법불합치결정을 하였음(헌법재판소 2018. 8. 30. 2016 헌마 263).

- 피해사례
  - ❍ 국가보안법 위반혐의로 2008 년 9 월 27 일, 국가정보원에 체포, 구금되었던 남북공동선언실천연대 정책위원 곽동기씨는 2008 년 6 월 12 일부터 2008 년 8 월 11 일까지 집과 사무실의 컴퓨터가 접속하는 모든 IP 주소와 접속 내역을 국가정보원이 실시간으로 패킷감청한 사실이 재판과정에서 드러남.
  - ❍ 과거 국가보안법 혐의에 대해 무죄를 선고받은 바 있는 김모씨에 대해 2011 년 2 월 국가정보원이 재수사를 하는 과정에서 '패킷감청'을 실시한 사실을 통보하면서 알려짐. 이에 2011 년 3 월 29 일 피해자가 헌법소원을 제기하였으나 2016 년 2 월 25 일 청구인 사망을 이유로 심판 종료를 선언함. 이에 시민사회단체가 2016 년 3.29. 또다른 패킷감청 피해자와 함께 헌법소원을 제기해 2018.8.30. 패킷감청이 헌법에 불합치한다는 결정을 이끌어 냄
  - ❍ 2014 년 10 월 1 일 정진우 당시 노동당 부대표가 경찰이 자신을 수사하는 과정에서 카카오톡을 압수수색해 같은 단체 방에 있었던 지인까지 총 3 천명을 사찰했다는 주장을 제기함. 이 사건을 계기로 카카오톡의 패킷감청 가능성이 제기되었고 이후 많은 이용자들이 사이버망명에 이르게 됨
  - ❍ ‘경찰 댓글 공작’을 수사 중인 ‘경찰청 특별수사단’(특수단)은 이명박 정부 시절 경찰청 보안국이 직접 구매한 것으로 알려지고 있는 ‘클라이언트 전산시스템’(B.F.S Matrix SW)을 이용해 2010 년 경찰청 보안사이버수사 대장으로 일했던 민아무개 경정이 패킷감청과 유사한 불법감청을 했다고 밝힘. 국군사이버사령부로부터 ‘레드펜’ 자료(정부·정책 등 비난 댓글 작성자 아이디, 닉네임 등)를 건네받아 수사에 활용했고 이 과정에서 감청 프로그램을 이용해 영장 없이 불법 감청한 것인데 얼마나 많은 시민을 패킷감청했는지 그 규모와 기간은 아직 밝혀지지 않음.
  - ❍ 2019 년 방송통신위원회가 불법정보 유통금지를 위해 ‘HTTPS SNI 필드 차단'을 도입했음.자동화 시스템을 통해 SNI 를 차단하는 것과 인터넷회선을 감청하는 것의 기술적 경계가 모호하고 또 이 과정에서 통신사들이 갖게 되는 차단시스템은 언제든 패킷감청에 쓸 수 있을 것이란 우려가 있음.
- 통비법 제 5 조 1 항에서 허용하는 감청 허가가 패킷감청을 허용하는 근거가 되어서는 안됨.
  - ❍ 20 대 국회에는 현행 통비법의 감청허용 대상범죄, 요건,범위, 기간 등을 특정하도록 해야 하고 취득한 자료의 보존, 폐기 및 감청대상에 대한 통지 의무 규정을 엄격히 하는 방향의 법개정안이 다수 발의되어 있음. 패킷감청은 그 대상과 범죄내용만을 특정하기가 기술적으로 어렵기 때문에 통비법의 감청 영장으로 집행된다는 것은 그야말로 백지영장, 포괄영장을 허용하는 것이며 이는 헌법상으로 결코 용납될 수 없는 것임.

- ❍ 또한 헌법재판소는 인터넷패킷감청이 과잉금지원칙 위반으로 2020 년 3 월 31 일까지 개정할 것을 요구하면서[35] 수집되는 정보의 방대함, 감청대상의 포괄성 때문에 집행단계에서부터 권한남용을 통제할 법적 장치 및 집행 이후 통지 제도의 불비 등을 지적함.

- 패킷감청으로 획득한 정보가 실제로 범죄의 증거로 제출된 경우는 거의 없음
  - ❍ 패킷감청은 사생활 침해의 범위나 수위가 다른 감청과 비교할 수 없을 정도로 심각하다는 점을 고려하면 패킷감청을 활용한 수사는 그 필요성이 엄격하게 요구되어야만 함. 즉, 범죄수사에 대한 필수불가결성이 먼저 입증되어야 할 것임.
  - ❍ 실제로 패킷감청의 대부분이 정보기관인 국정원에서 이뤄지고 있으며 국정원이 6 년에 걸쳐 회선 감청을 한 것으로 알려진 조국통일범민족연합 국가보안법 위반 사건에서도 검찰은 감청으로 확보한 자료를 증거로 제출하지 않았고, 위 헌법재판소 심리과정에서도 국가정보원이 7 년동안 인터넷회선감청을 하였으나 그 과정에서 획득한 정보 중 실제 재판에 증거로 제출한 자료가 없음이 드러나기도 했음.
  - ❍ 과거 패킷감청 사례를 통해 패킷감청이 실제 형사사법절차에서 활용할 수 있는 '증거'수집방법으로 과연 필요한 것이었는지에 관한 강한 의문이 제기됨. 증거로 쓰지 않을, 쓰지 못할 광범위한 정보수집이 왜 필요한 것인지에 대해 국정원 등 실제 패킷감청을 실행했던 기관은 제대로 답하지 못하고 있음.
  - ❍ 과연 패킷감청이 범죄수사를 위해 이루어진 것인지 의문인 상황에서 앞으로의 패킷감청에 대한 엄격한 심사가 필요하고 그렇게 되리라는 기대만으로 이를 허용해서는 안되고, 그동안 실행된 패킷감청이 '증거'획득수단으로 무용했다면 개인의 프라이버시에 대한 직접적인 침해를 할 수밖에 없는 이런 이례적인 수단의 사용을 허용하는 것이 필요한지 근본적인 재검토가 필요함

- 정보수사기관의 패킷감청 집행에 대한 법적 제도적 통제장치 불비
  - ❍ 국가기관의 감청장비 인가 및 보유 현황은 과학기술정보통신부가 관리하고 있으나 정보기관은 제외됨. 감청 집행의 절대적 다수를 행하고 있는 국가정보원은 정보기관의 특성상 무영장 감청이 얼마나 행해지고 있고 감청설비를 얼마나 갖고 있는지 등등 감청실태가 사실상 비밀에 쌓여 있음.
  - ❍ 법원의 감청허가를 받고 있으나 그 실행과정, 획득한 정보의 관리나 폐기 등 감청집행으로 취득하는 막대한 양의 자료를 어떻게 처리할 것인지에 관한 사전, 사후통제절차가 전혀 없음

나. 권고사항

- 패킷감청은 그 대상이나 내용을 특정하는 것이 기술적으로 불가능하기 때문에 대상자와 특정 범죄관련 내용을 특정해야 하는 현행 감청제도로는 패킷감청을 운용하는 것이 불가능하므로,

35 헌법재판소 2018.8.30. 2016 헌마 263

이에 대한 엄격한 통제절차를 마련할 필요가 있고, 실행과정에 대한 기술적 감시와 통제가 가능한 제도마련이 필요함.

다. 담당 부처 및 기관

- 법무부
- 과학기술정보통신부

2) 통신사실확인자료[36]

가. 배경 및 개요

- 통신비밀보호법 제 13 조 범죄수사를 위한 통신사실 확인자료의 제공의 절차에 의하면 "수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자에게 통신사실 확인자료의 열람이나 제출을 요청할 수 있다"고 명시하고 있음.
- 명시적으로는 수사기관이 법원의 허가를 얻어 통신사실 확인자료를 요청하도록 되어있지만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있을 경우 수사기관이 법원의 허가 없이 통신사실 확인자료를 요청하고, 이후에 허가를 받을 수 있도록 함.[37] 수사기관이 개인의 통신사실 확인자료를 열람하는데 있어 영장이 아닌 법원의 허가로만으로도 집행할 수 있게 함으로 인해, 통제가 약한 상황에서 무분별한 통신사실 확인자료 요청이 이루어지고 있음.
- 2014 년 국가인권위원회는 <「전기통신사업법」 통신자료제공제도와 「통신비밀보호법」 통신사실확인자료 제공제도 개선권고>에서, '통신사실 확인자료 제출 요청의 허가요건이 지나치게 모호하여 수사기관의 남용을 방지하기 어려우며 사생활 보호에 미흡하다'고 지적한 바 있음.
- 국가인권위는 해당 권고를 통해 통신사실 확인자료의 내용에서 '실시간 위치정보'를 제외할 것과 통신사실 확인자료의 제공 요건을 "피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당사건과 관계가 있다고 인정할 수 있는 것"으로 한정할 것을 권고하였음. 또한 범죄 수사를 목적으로 하는 실시간 위치정보 제공의 요청의 경우 강화된 요건 외에 보충성 요건을 갖춘 경우로 한정할 것을 권고하였음.

---

36 작성단체: 진보네트워크센터

37 통신비밀보호법 제 13 조②제 1 항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다.

<통신수단별 통신사실 확인자료 요청 건수>[38]

(단위: 문서 수)

년도	유선전화	이동전화	PC 통신·인터넷
2014	48,890	177,361	32,933
2015	57,838	207,004	36,100
2016	58,755	213,813	30,753
2017	59,590	204,524	37,207

- 통신사실 확인자료는 비내용적 정보(메타데이터)이긴 하나 여러 정보와 결합·분석을 통해 정보주체에 관한 정보를 유추할 수 있는 민감한 정보[39]임.
- 수사기관이 요청하는 통신사실 확인자료에는 상대방 전화번호, 통화 일시 및 시간 등 통화사실과 인터넷 로그기록 및 접속지 자료(IP Address) 및 발신기지국 위치추적자료를 포함하고 있음.[40]
- 수사기관은 통신사실확인자료를 특정 대상자를 지정하지 않고 특정 시간대 해당 위치의 기지국을 이용한 이용자들의 모든 통신기록을 요청하는 '기지국 수사'와 대상자의 장래 위치를 실시간으로 추적하는 '실시간 위치추적'을 위해 광범위하게 활용하고 있음.
- 2015 년 자유권 위원회는 수사기관이 수사목적을 이유로 영장 없이 전기통신사업자에게 이용자 정보를 요구한다는 것에 대해 우려의 입장을 표했으며, 집회 참가자들을 특정하기 위한 '기지국 수사'의 집행 및 이에 대한 불충분한 규제에 대해서도 우려를 표한 바 있음.[41]
- 기지국 수사는 수사기관이 기본권 주체가 누려야 하는 통신비밀의 불가침과 사생활의 비밀의 불가침을 직접적으로 중대하게 침해함. 또한 범죄의 혐의가 없는 사람도 통신비밀과 위치정보를 침해당하게 됨.

---

38 과학기술정보통신부, 통신자료 및 통신사실확인자료 제공 등 현황(2014~2017 년)

39 헌법재판소 2018.6.28. 2012 헌마 538

40 통신비밀보호법 제 2 조 정의 조항에서 "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 포함한다고 정의하고 있다.

가. 가입자의 전기통신일시

나. 전기통신개시、종료시간

다. 발、착신 통신번호 등 상대방의 가입자번호

라. 사용도수

마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료

바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료

사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

41 CCPR/C/KOR/CO/4, para42~43

- 사실상 통신사실 확인자료 제공 요청에 해당하는 범죄가 특정되어 있지 않아 '모든 범죄'가 그 대상이 됨. 개인의 통신내역, 위치정보 등 민감한 정보가 법원의 영장도 없이 수사기관에 제공되고 있는 것임.
- 2012 년 선거 기간 중 금품살포 의혹을 조사하던 수사당국이 특정 시간 해당 지역 기지국을 이용한 659 명의 통신사실 확인자료를 제공받았음. 이에 대해 같은 해 헌법소원을 신청하였으며 헌법재판소는 2018 년 해당 조항이 과잉금지의 원칙에 반하여 개인정보자기결정권과 통신의 자유를 침해한다는 이유로 헌법불합치 결정을 내렸음.[42]
- 휴대전화 실시간 위치추적은 통화시는 물론 대기모드에서도 매 10~30 분 간격으로 단말기의 위치가 자동으로 확인되고, 해당 기지국의 위치정보가 수사관의 휴대폰에 메시지로 발송됨.
- 현행 통신비밀보호법은 통신사실 확인자료 제공과 관련 대상자를 명확히 하고 있지 않아, 피의자 본인뿐만 아니라 가족 및 관련 없는 지인들까지도 통신사실 확인자료 제공 대상자가 될 수 있게 하고 있음.
- 2011 년 6 월부터 10 월 부산의 조선소 해고노동자를 응원하고자 '희망버스 집회'를 개최하였다는 취지로 '집회 및 시위에 관한 법률'위반 등의 혐의로 기소되었음. 이후 수사기관은 2011 년 12 월부터 2012 년 4 월까지 통신사실 확인자료를 제공받았음. 이에 2012 년 2 월 헌법재판소에 헌법소원을 신청하였고, 헌법재판소는 2018 년 해당 조항이 과잉금지의 원칙에 반하여 개인들의 개인정보자기결정권과 통신의 자유를 침해한다는 이유로 헌법불합치 결정을 내렸음.[43]
- 수사기관이 2013 년 12 월 9 일 ~ 12 월 30 일 까지 철도공사 민영화에 반대하며 파업을 하던 철도노조 위원장을 비롯 철도노조 조합원 15 명과 그들의 가족 21 명의 통신사실 확인자료 제공을 받았음. 당시 수사기관은 휴대전화와 인터넷 사이트 접속위치를 실시간으로 추적했단 사실이 드러났음.[44] 이에 2014 년 헌법소원을 신청하였고, 헌법재판소는 2018 년 해당 조항이 과잉금지의 원칙에 반하여 개인들의 개인정보자기결정권과 통신의 자유를 침해한다는 이유로 헌법불합치 결정을 내림.[45]
- 헌법재판소는 '비내용적 정보인 메타데이터라 할지라도 여러 정보의 결합과 분석을 통해 정보주체에 관한 정보를 유추해낼 수 있는 민감한 정보인 점', "위치정보 추적자료는 충분한 보호가 필요한 민감한 정보에 해당"한다고 함. 이에 통신사실 확인자료 제공 요청의 기준을 강화할 것을 권고함.

---

42 헌법재판소 2018.6.28. 2012 헌마 538

43 헌법재판소 2018.6.28. 2012 헌마 191·550, 2014 헌마 357(병합)

44 당시 경찰은 통신사실 확인자료를 통해 당사자들의 휴대전화 위치는 물론 인터넷 접속 위치를 실시간으로 추적했음은 물론 영장도 없이 건강보험공단 등 공공기관이 보유하고 있는 철도노조 집행부 및 가족의 개인정보를 제공받은 사실이 드러났다.

45 헌법재판소 2018.6.28. 2012 헌마 191·550, 2014 헌마 357(병합)

- 정부는 헌법불합치 결정을 받은 '통신제한조치 연장', '위치정보 추적자료', '기지국 수사'와 관련 위헌적 요소를 제거하기 위한 정부 입법안을 내놓았으나, 정작 개인의 인권침해를 최소화하기 위한 충분한 조치를 포함하고 있지 않음. 해당 정부 법안은 여전히 수사의 편의성과 법집행의 효율성만을 앞세워 정보인권 침해 가능성을 그대로 남겨두고 있음.

나. 권고사항

- 수사기관에 의한 정보인권 침해를 최소화하고, 권력기관의 권한 남용을 최소화하기 위한 통신비밀보호법 개정안이 마련되어야 함.
- 통신사실 확인자료의 제공에 영장주의를 도입하여 법원의 통제를 받도록 해야 하며, 송수신이 완료된 전기통신의 압수, 수색, 검증의 요건을 강화하여 상당한 이유 요건과 보충성 요건을 규정하고 그 절차에서 당사자의 참여권을 명시해야 함.
- 기지국 수사의 경우 이에 관한 명확한 규정을 신설하고 그 요건을 강화해야 함.
- 위치정보추적자료, 특히 실시간 위치정보의 경우 실시간 감청의 효과를 지니므로 대상범죄를 통신제한조치의 대상이 된 범죄로 한정하고 요건을 엄격하게 강화해야 함.

다. 담당 부처 및 기관

- 법무부

3) 통신자료 제공[46]

가. 배경 및 문제점

- 전기통신사업법 제 83 조 3 항은 정보수사기관이 전기통신사업자로부터 수사 등을 위하여 필요한 경우 법원의 허가 없이도 통신자료(가입자 정보: 성명, 아이디, 주민등록번호, 주소, 전화번호, 가입일 및 해지일)를 확보할 수 있는 통로를 만들어 두었음. 주로 초동수사 단계에서 수사대상자의 인적사항 파악이 목적이라고 하지만 그 요건이 지나치게 광범위하고 불명확함.
- 헌법재판소는[47] 수사기관의 통신자료 제공 요청이 강제수사에 해당하지 않는다는 취지의 결정을 한 바 있음. 그러나 대법원[48]은 2010 년 3 월 네이버가 수사기관에 회원 통신자료를 넘긴 사건의 손해배상 소송에서 수사기관이 형식적 절차적 요건을 갖추어 전기통신사업자에게 통신자료 제공 요청하면 사실상 통신자료를 제공하는 수밖에 없다고 봄.

46 작성단체: 참여연대

47 헌법재판소 2012.8.23. 2010 헌마 439 결정

48 2016.3.10. 선고 2012 다 105482 판결.

- ❍ 전기통신사업법 제 83 조 3 항은 정보수사기관이 그 필요성을 판단하면 전기통신사업자는 이에 무조건 따라야 하는 방식으로 운영되고 있고, 가입자의 정보가 제공되는 과정에 사법 통제는 전무함.
- ❍ 사전, 사후 전혀 정보주체에게도 통지하지 않고 있음.
- ❍ 이에 정보주체는 자신에 대한 통신자료 수집이 수사의 필요성과 상당성을 갖춘 적법한 직무집행인지 판단하기 위한 기초자료도 확보하기 어려움.
- ❍ 특히 우리나라의 경우 주민등록번호를 기반으로 수많은 정보들이 결합되어 있고, 주민등록번호가 개인정보수집의 키 역할을 하는 상황에서 정보수사기관의 일방적인 판단에 따라 핵심개인정보라 할 수 있는 주민등록번호가 제공될 수 있다는 것은 다른 나라에 비해 기본권침해의 정도가 크다는 점을 고려해야 함.

● 전체 통신에 대한 통신자료 제공은 연 평균 1,034,036 건, 9,539,337 개 계정에 대해 이루어지고 있음(2013 년-2017 년 기준). 2016 년부터 전체 통신에 대한 통신자료제공, 인터넷상 통신자료제공 모두 조금씩 감소하는 추세임.

- ❍ 다만 인터넷상 통신자료제공은 문서수 기준으로 감소추세에 있으나, 2017 년 통신자료가 제공된 계정수가 전년대비 2 배 이상 증가해 이용자의 신원정보 확인이 급증하였음은 주의가 필요

통신자료제공	2013 년		2014 년		2015 년		2016 년		2017 년	
	문서수	계정수	문서수	계정수	문서수	계정수	문서수	계정수	문서수	계정수
통신 전체	944,927	9,574,659	1,001,013	12,967,456	1,124,874	10,577,079	1,109,614	8,272,504	989,751	6,304,985
인터넷 전체[49]	115,194	392,511	114,260	489,916	100,643	423,533	84,302	312,056	65,151	635,795
양대 사업자[50]	1	17	0	0	0	0	0	0	0	0

49 '인터넷 전체'는 과학기술정보통신부 보도자료의 통신수단 중 '인터넷 등'에 해당하며, 유선·이동 전화를 제외한 나머지 통신 사업자(포털 등 부가통신사업자와 인터넷망사업자 기타)가 보고한 수치의 합계이다.

50 양대 사업자는 '양대 사업자'는 투명성보고서를 공개한 국내 양대 온라인 서비스 사업자인 '네이버'(자회사 캠프모바일 포함)와 '카카오'를 의미한다. 범죄 혐의가 불분명한 가입자의 신원정보를 수사기관에 제공한 포털사에게 손해를 배상하라는 하급심 판결(서울고등법원 2012. 10. 18. 선고, 2011 나 19012 판결)이 2012 년에 나온 후, 주요 포털사들은 2013 년부터 통신자료제공을 중단함. 비록

- ❍ 연간 전체 인구수의 18.4%에 해당하는 9 백 5 십 만 개 이상의 계정의 개인정보가 영장 없이 수사기관에게 제공되는 것은 심각한 문제임.

- 국가인권위원회는 현재 심리중인 통신자료 제공 제도 헌법소원(헌재 2016 헌마 388)에 대해 "통신자료 제공 제도는 개인정보 수집 목적과 대상자 범위가 지나치게 넓고, 사전 또는 사후에 사법적 통제가 이루어지지 않으며, 정보주체가 자신의 개인정보 제공 사실을 인지할 수 있는 통지 절차가 마련되지 않아 개인정보자기결정권을 침해할 소지가 있다"는 의견을 헌법재판소에 제출함.
- 수사기관의 통신자료 제공 요청 제도를 개선하기 위해 사법적 통제 장치 마련 등을 골자로 하는 전기통신사업법개정안과 통신비밀보호법개정안이 19 대 국회에 이어 20 대 국회에도 다수 발의되어 있음. 그러나 논의 진척은 거의 없는 수준.
- 피해사례
  - ❍ 회피연아 동영상 게시자 통신자료 무단 제공 네이버에 대한 손해 배상 소송: 2010 년 3 월경 김연아 선수가 유인촌 당시 문체부장관을 어색해 하는 듯한 모습이 담긴 뉴스 영상, 소위 '회피연아' 동영상을 한 네티즌이 네이버 까페 게시판에 스크랩한 것이 유인촌 장관에 대한 명예훼손 혐의로 경찰의 수사를 받게 됨. 이 과정에서 네이버가 자신의 개인정보를 수사기관에 제공했다는 사실을 알게 되고 사전 사후 전혀 통지조차 하지 않은 네이버를 상대로 손해배상 소송 제기.1 심은 청구를 기각했으나 항소심에서는 네이버가 이용자의 개인정보를 충실히 보호하여야 할 의무에 위배하여 원고의 개인정보자기결정권과 익명표현의 자유를 침해하였다며 50 만원의 손해배상책임을 인정함[51]. 이 항소심 승소판결 후 2012 년 10 월말부터 네이버, DAUM, SK 컴즈, 카카오 등 주요 인터넷 기업들은 법원의 영장 없이는 통신자료를 수사기관에 제공하지 않고 있음.
  - ❍ 통신 3 사의 수사기관에 제공한 통신자료 내역 비공개 취소소송: 2013 년 4 월 인터넷포털과 달리 수사기관의 요청에 무조건 통신자료를 제공하고 통신자료 제공현황 요청에도 응하지 않는 이동통신 3 사를 상대로 통신 3 사 이용자들이 통신자료제공현황에 대한 열람청구 및 손해배상청구소송을 제기함. 1 심은 통신자료제공현황을 공개하라는 판결을 선고함(손해배상은 부정), 항소심은 1 심에서 인정하지 않았던 손해배상 책임도 인정[52]. 수사업무에 지장이 발생할 수 있다는 막연한 사정만으로 헌법과 법률이 보장하는 정보주체의 개인정보자기결정권을 제한할 수 없다며, 원고들의 공개청구를 상당기간 거부한 것이 개인정보자기결정권을 침해한

2016 년 3 월 대법원(대법원 2016. 3. 10. 선고, 2012 다 105482 판결)에서 본 판결은 파기되었으나, 양대 사업자들은 이후에도 통신자료제공 요청에 응하지 않고 있음. 주요 포털 서비스 사업자가 통신자료제공을 중단하였으므로, 현재 인터넷 이용자에 대한 통신자료제공은 주로 인터넷 망사업자들에 의하여 이루어지고 있는 것으로 볼 수 있음

51 서울고등법원 2011 나 19012 판결

52 서울고등법원 2014 나 2020811 판결

불법행위라고 인정함. 통신 3 사가이에 불복하고 상고하였으나, 2018 년 7 월 20 일 대법원이 3 년 반 만에 통신 3 사의 상고를 기각하여 항소심 판결이 그대로 확정됨.

- 2016 년 국회의원, 노조가입자 등 통신자료 무단 수집 500 인 헌법소원: 2016 년 3 월 테러방지법 제정에 반대하는 국회의원, 노조가입자 등 다수의 국민의 통신자료를 수사기관이 수집해 갔다는 폭로가 이어짐. 이에 자신의 통신자료를 수집해 갔는지 확인하는 대국민 캠페인을 시민단체에서 벌임. 자신의 통신자료가 제공된 것이 확인된 국민 500 여명이 전기통신사업법 제 83 조 3 항에 대해 헌법소원을 제기함. 현재 심리 중

나. 권고사항

- 전기통신을 이용하는 국민의 가입자 정보를 법원의 통제없이 수사기관이 무제한 수집할 수 있도록 한 전기통신사업법을 개정할 것
- 전기통신 이용자의 신원정보를 수사기관이 영장 없이 수집할 수 있게 하는 통신자료 제공 제도를 전면 폐지할 것
- 수사기관의 수사편의가 정보인권 가치를 압도하는 현실을 개선하기 위한 방안을 마련할 것

다. 관련 부처 및 기관

- 법무부
- 방송통신위원회
- 과학기술정보통신부

4) 디지털정보 압수수색[53]

가. 배경 및 문제점

- 개인 간의 통신은 개인의 사적 영역의 핵심적인 부분을 차지하고 있으므로 통신사실, 통신내용에 대한 비밀의 보장은 개인의 사생활 보호에 있어 가장 기본적이며 중요함. 그런데 송수신이 완료된 이메일은 현행 형사소송법상의 '물건'과 같이 일반적인 압수수색 절차에 따름. 송수신이 완료된 일정기간의 이메일을 압수수색하기 위해 컴퓨터 서버나 노트북 등을 가져가서 들여다본다면, 그동안 오간 통신의 내용들과 상대 수신자들이 무방비로 노출되는 것임. 수사기관은 이메일 압수수색에서 얻은 이 같은 사적인 정보까지 유죄의 증거로 제시하기도 하여 논란이 되기도 했음.
- 따라서 송수신이 완료되었다고 해도 일정기간 동안 주고받은 이메일은 광범위한 정보 수집에 따른 사생활 침해의 위험이 커 일반적인 압수수색과는 다르게 절차와 기준을 적용해야 한다는 주장이 많음. MBC PD 수첩 제작진들에 대한 명예훼손 혐의 사건은 이 같은 위험을 보여주는 사례임.

53 작성단체: 참여연대

- ❍ PD 수첩 제작진 이메일 압수수색: 이명박 정부의 미국산소 수입 확대에 반대하는 국민들의 대규모 촛불집회가 시작되던 2008 년 4 월 29 일 MBC PD 수첩은 <긴급취재, 미국산 쇠고기, 광우병에서 안전한가?> 편을 방송함
- ❍ 이명박 정부는 국민들의 대규모 촛불집회의 배후가 PD 수첩이라고 지목하고 PD 수첩의 PD, 작가 등 제작진들을 정부(농림수산식품부)에 대한 명예훼손죄로 고발함. 검찰은 사전통지 없이 e 메일 등을 압수수색했을 뿐 아니라, 수사 결과를 발표하며 김은희 작가가 지인에게 보낸 개인적 e 메일을 공개하며 유죄의 증거로 주장하기도 했음. 당시 검찰은 압수수색을 통해 김 작가의 7 개 월치 이메일을 가져가고 범죄혐의와 상관없는 사적인 대화내용까지 엿본 것으로 알려짐.

- 국가인권위원회는 2010 년 8 월 이처럼 e 메일을 무차별적으로 압수수색하는 수사기관의 관행에 대해 국회의장에게 '전기통신사업자의 서버에 저장된 e 메일의 압수수색이나 통신제한조치에 대해 입법적으로 근거와 절차 규정을 마련해야 한다'는 권고와 함께 "e 메일을 압수수색할 때 범죄 혐의와 관련성이 있는 기간 등으로 범위를 특정해야 한다"며 형사소송법 개정안에 대한 권고의견을 제시하였음.
- 인터넷 통신망을 기반으로 유통되는 전자통신의 형태는 다양한데 이들에 대한 수사상 압수수색은 형소법의 일반적인 압수수색 규정에 따라 진행되고 있는 것은 문제임. 컴퓨터 하드디스크에 저장되어 있는 디지털정보의 경우 단순히 물건을 압수수색하는 것과 달리 기술적으로 범죄혐의와 유관한 정보만 따로 추출하는 것이 쉽지 않다 보니 그동안 포괄적인 압수 방법을 취해 왔음. 이로 인해 방대한 디지털정보의 수집이 가능했고 범죄혐의와 무관한 정보주체의 사생활침해, 통신비밀 침해가 현저히 크다는 지적이 많았음. 일례로, 전교조시국선언, 세월호참사 교사선언 고발 사건에서 수사기관이 압수수색을 통해 수집한 정보를 토대로 새로운 수사로 확대한 사례가 논란이 되었음.
  - ❍ 2009 년 6 월경 전교조는 미디어법 입법중단과 한반도 대운하 추진의혹해소 등을 요구하는 시국선언을 하여 교육과학기술부(현 교육부)로부터 국가공무원법위반 혐의로 검찰에 고발됨. 검찰은 법원에서 전교조 사무실에 대한 압수수색영장을 발부받아 서울영등포구에 있는 전교조 본부사무실에서 영장을 집행하면서 데스크탑 컴퓨터 3 대와 서버컴퓨터 10 대를 압수함. 이때 압수해간 컴퓨터에서 취득한 정보를 토대로 시국선언과 별건으로 민주노동당 당원 또는 후원당원으로 가입하여 매월 5 천원~2 만원 내외의 후원금을 납부한 교사들까지 수사범위를 넓힘. 이후 정당법과 정치자금법 위반 등으로 전교조 소속 교사와 공무원들을 대대적으로 기소함.
  - ❍ 이에 대해 전교조측은 검찰이 영장에 적시된 압수수색 방법에서 벗어나 위법하다고 준항고하였음. 대법원은 준항고를 기각하였으나 전자정보에 대한 압수수색은 혐의사실 관련 부분만을 현장에서 문서 출력하거나 복제하는 방식으로 이루어져야 하고 저장매체의 외부반출은 영장에 명기된 예외적인 때에만 허용된다고 판시함.이후 2011 년 7 월 형사소송법이 개정되어 정보저장매체에 대하여는 제한된 범위 내의 사본 압수가 원칙이라는 규정이 신설됨.

- ❍ 2014 년 7 월에 경찰이 세월호참사 관련 교사선언과 조퇴투쟁을 주도한 혐의로 전교조 조합원 76 명에 대해 수사하면서 서초동에 있는 전교조 서버에 대해 긴급 압수수색을 진행함. 당시 영장에는 '홈페이지 서버 자료'와 '서버에 보관된 전교조 이메일 계정 내역'만으로 한정되어 있었다고 함. 그러나 피의자 조사 과정에서 사적인 대화내용이 들어있는 이메일과 네이버 밴드까지 압수수색한 사실이 알려짐. 조사 전까지는 이 사실에 대해 전혀 알지 못함. 이메일과 밴드 압수수색은 범죄혐의 사실과 무관한 대화 내용까지 수사기관이 모두 들여다보았다는 점, 피의자가 아닌 다른 사람들의 대화 내용까지 다 들여다볼 수 있다는 점, 수사기관이 이메일과 밴드에 대해 영장을 집행하고도 당사자들에게 고지하지 않았다는 점에서 위법하며 국민의 기본권을 심각하게 침해한 것이라는 비판이 있었음.

- 대법원은 2015 년 7 월 16 일 전원합의체 판결에서 기존의 전자정보 압수수색의 원칙을 확인하고, 혐의 관련 정보 추출이 완료(압수수색 종료)된 시점까지 피의자 쪽 참여 기회를 보장하고, 탐색 도중 영장 혐의 외 다른 범죄 혐의 자료가 발견될 경우 해당 혐의에 대한 압수수색 영장을 받아야 한다고 했음
- 그 밖의 사례
  - ❍ 2008 년 주경복 당시 서울시교육감 후보(건국대 교수)의 선거법 위반 사건을 수사하면서 검찰이 그의 7 년치 e 메일을 통째로 압수수색하여 가져감. 그러나 주교수에게 통지도 하지 않아 재판 도중에 알게 됨.
  - ❍ 2009 년 박래군 당시 용산참사범국민대책위 공동집행위원장이 변호인과 e 메일을 통해 주고받은 변론 관련 내용까지 압수돼 증거물로 제출된 적도 있음.
  - ❍ 2009 년 경찰이 업무방해 혐의로 조사받던 YTN 조합원 20 명의 회사 e 메일을 압수수색해 9 개 월치 분량을 들여다보았음. 혐의와 관련 없는 언론노조 회의자료나 회계자료 등도 포함돼 있었다고 하며 통지를 하지 않아 당사자들은 석 달 넘게 압수수색 사실조차 몰랐다고 함.
- 이와 같이 전자정보의 압수수색은 법원의 판례와 형사소송법의 규정에 따라 범죄혐의와 관련 있는 부문만 수집해야 함에도 광범위한 정보를 수집하여 범죄와 관련 없는 사생활 정보까지 사찰하여 사생활을 침해해 왔음
- 정보통신기술의 발달로 인터넷을 통해 유통되는 전자정보는 형태가 다양함. 네이버 밴드나 카카오톡 대화방 내용에 대한 압수수색은 경우에 따라서는 실시간 감청과 같은 결과를 가져옴에도 형사소송법상 압수수색 규정에 따라 이루어지고 있음. 이메일도 장기간에 걸쳐 이루어질 경우, 그 수신자가 다양하고 정보의 양도 방대할 수 있으며, 메신저 대화내용 역시 가입자 다수에 대한 사생활 정보가 포함되며, 컴퓨터 서버의 경우도 그 정보량이 어마어마함. 이에 따라 이들에 대한 압수수색은 정보주체의 프라이버시권 등 기본권 침해 강도도 일반적인 압수수색에 비해 훨씬 큼. 따라서 형사소송법상의 압수수색 규정만으로 규율하는 것은 한계가 있음.

나. 권고사항

- 형소법상의 일반 압수수색 영장으로 전자정보를 압수수색하는 것은 비례성 원칙에 반하고 사생활과 통신의 비밀의 침해 정도가 심각하다는 지적을 받아들여 관련 규정을 개선하시오

다. 담당부처 및 기관

- 법무부

3. 주민등록제도

1) 주민등록번호 제도[54]

가. 배경 및 문제점

- 모든 대한민국 국민에게는 태어날 때부터 고유한 국민식별번호인 주민등록번호가 부여됨. 주민등록번호는 13 자리의 숫자로 구성되어 있는데, 앞의 여섯자리는 생년월일, 뒤의 7 자리는 성별, 출생지(출생등록을 한 기관코드), 해당지역 출생신고순서, 오류검증번호로 구성됨. 원칙적으로 주민등록번호는 한번 부여되면 평생 변경할 수 없음.
- 주민등록번호는 다양한 공공 및 민간 영역에서 개인식별을 위해 수집되어 왔으며, 따라서 주민등록번호는 서로 다른 데이터베이스의 정보를 연계하는 열쇠(key)로 작용할 수 있음. 이에 따라 주민등록번호를 포함한 대량 개인정보 유출 사고로 인한 피해가 컸음.
  - 2008 년 옥션 1 천 8 백만 건 유출,
  - 2011 년 SK 컴즈 네이트, 싸이월드 3 천 5 백만 건 유출,
  - 2011 년 넥슨 메이플스토리 1 천 3 백만 건 유출,
  - 2014 년 롯데카드, 농협카드, KB 국민카드 1 억 4 백만 건 유출,
  - 2016 년 인터파크 1 천 3 십만 건 유출
- 2008 년 한국의 1 차 UPR 에서 유엔 인권이사회는 주민번호를 필수적인 공공목적으로 사용 제한할 것을 권고하였음.[55]
- 주민등록번호의 과도한 수집을 제한하기 위해 정보통신망법 개정으로 2012 년 8 월부터 온라인에서 주민등록번호 수집이 금지되었으며, 개인정보보호법 개정으로 2014 년 8 월 7 일부터 법령에서 허용하지 않으면 주민등록번호를 수집할 수 없도록 하고 있음.
- 2014 년 8 월 8 일, 국가인권위원회는 국회의장 및 국무총리에 주민등록번호 제도의 근본적 개편을 권고함.[56] 주민등록번호는 주민등록 관련 행정업무 등에 한정하여 사용하고, 그 외 영역에서는 조세번호와 같이 해당 분야에 고유한 목적 별 번호를 사용하도록 하고 주민등록번호를 변경할 수 있도록 허용하며 주민등록번호를 개인정보가 포함되지 않은 임의의 일련번호로 변경할 것을 권고하였음.
- 2015 년 12 월 23 일, 헌법재판소는 주민등록번호의 변경을 허용하지 않는 것은 그 자체로 개인정보 자기결정권을 침해하는 것으로 판시하며, 현행 주민등록법에 대해 헌법불합치 결정을 내림. 2017 년 12 월 31 일까지 주민등록법을 개정할 것을 권고함.[57]
- 주민등록번호 제도는 크게 3 가지의 문제점을 가지고 있음. 첫째, 공공 및 민간 영역에서 광범하게 수집되어 서로 다른 개인정보의 통합 및 개인에 대한 추적, 혹은 프로파일링을

54 작성단체: 진보네트워크센터

55 A/HRC/8/40, para 63.13.

56 국가인권위원회(2014). 주민등록번호 제도 개선 권고.

57 헌법재판소 2015 년 12 월 23 일 결정. 2014 헌마 449 2013 헌바 68(병합)

가능하게 하는 기반이 되고 있음. 둘째, 원칙적으로 주민등록번호의 변경이 불가능하여, 주민등록번호로 유출로 인한 잠재적 피해를 야기할 수 있음. 셋째, 주민등록번호 자체가 생년월일, 성별, 출생지 등을 포함하고 있어 정보주체가 원하지 않아도 개인정보가 노출될 수 있으며 차별의 근거로 활용될 수 있음.

- 개인정보의 수집을 제한하기 위해 2014 년 8 월부터 법령에 근거가 없이는 주민등록번호를 수집할 수 없도록 하였지만, 여전히 많은 법령에서 주민등록번호의 수집을 허용하고 있음. 2014 년 1 월, 안전행정부가 발표한 자료에 따르면 866 개의 법령에서 주민등록번호의 수집을 허용하고 있으며, 민간 부문인 금융, 통신 영역에서도 주민등록번호를 수집하고 있음. 또한 법이나 시행령이 아니라, 서식에 근거하여 주민등록번호를 수집하는 경우도 있음.
- 2015 년 12 월, 헌법재판소의 헌법불합치 결정에 따라, 2016 년 5 월 19 일, 주민등록번호를 변경할 수 있도록 허용하는 주민등록법 개정안(정부안)이 국회를 통과함.[58] 그러나 주민등록번호를 변경할 수 있는 대상자를 유출로 인해 생명·신체 및 재산, 성폭력 등과 같은 피해를 입거나 입을 우려가 있는 경우로 한정하였음. 현실적으로 대다수 피해자가 주민등록번호 유출로 인한 직접적인 피해를 입증하기는 곤란함. 또한, 주민등록번호 13 자리 중 뒤의 6 자리만 변경해주기 때문에, 새 주민등록번호 역시 생년월일과 성별 정보를 포함하고 있어 전체 주민등록번호의 유추가 가능함. 이에 국가인권위원회 위원장도 환영과 함께, 제한적 변경에 아쉬움을 표하는 성명을 발표하여 목적별 번호, 임의번호의 도입을 요구한 바 있음.[59]
- 주민등록번호에 생년월일, 성별, 출생지 정보를 포함하여 의도하지 않게 개인정보가 노출되고 연령, 성별, 지역에 따른 차별을 조장.[60] 또한, 개인정보로 주민등록번호를 추정할 수 있음.
  - 2014 년 서울과학기술대학교 연구, 페이스북에 공개된 개인정보를 이용하여 11 만 5615 명 중 45%의 주민번호 조합성공[61]
  - 2015 년 미국 하버드대학교 연구, 미국 IMS 헬스에 팔린 한국인 주민번호 모델로 2 만 3163 개 재식별 성공[62] "생년월일, 성별, 지역, 검증번호 덕분에 수월했다"

---

58 시민사회공동입장(2016) *19 대 통과된 주민등록법에 대한 시민사회단체 입장-미완으로 끝난 주민번호 개선, 20 대 국회서 바꿔야!*. http://act.jinbo.net/wp/9538/ [2019.5.14].

59 국가인권위원회 (2016). *<주민등록법> 일부개정법률안 의결에 대한 위원장 성명*. https://www.humanrights.go.kr/site/program/board/basicboard/view?&boardtypeid=24&currentpage=55&menuid=001004002001&pagesize=10&boardid=611785 [2019.5.14].

60 시민사회공동 기자회견(2016) *주민번호 성별 표시 항의 기자회견 및 인권위에 진정서 제출 - 주민등록번호 성별표시 국가인권위 차별 진정*. http://act.jinbo.net/wp/9228/ [2019.5.14].

61 채널 A. (2014). *[단독]페이스북 내 주소 치면 주민번호 좍*. http://www.ichannela.com/news/main/news_detailPage.do?publishId=61503088-1 [2019.5.14]

62 한겨레. (2019). *[단독] 복지부 빅데이터의 위험성…개인정보 암호화해도 풀 수 있다*. http://www.hani.co.kr/arti/society/society_general/762609.html [2019.5.14].

- ❍ 2009 년 인식조사, 국민의 77.2%는 주민번호를 통해 성별, 생년월일 등을 알 수 있다는 사실에 "원하지 않는데도 내 정보가 노출되어서 신경이 쓰인다"고 응답함.
- ❍ 주민등록번호의 성별은 남, 여의 구분만 하고 있고 남자는 1 (2000 년 이후 출생자는 3), 여자는 2 (2000 년 이후 출생자는 4)로 되어 있어, 남성 우위의 인식을 반영한다는 비판이 있으며, 성소수자를 차별하는 요인이 되고 있음.

- 2014 년 국가인권위원회의 권고에도 불구하고, 주무부처인 행정안전부는 아직 주민등록번호를 임의의 일련번호로 변경할 의사가 없는 상황임.

나. 권고사항

- 주민등록번호의 수집 및 이용은 서식이 아니라, 법령에 근거가 있어야 함.
- 주민등록번호는 행정 및 사법 목적으로만 엄격하게 제한하고, 공공부문의 다른 분야에서는 해당 목적에 고유한 별도의 식별번호(예를 들어, 조세번호)를 사용.
- 법에 근거가 없이는 서로 다른 분야의 식별번호가 주민등록번호와 연계되지 않도록 함.
- 주민등록번호를 개인정보를 포함하지 않는 임의의 일련번호 체계로 변경하도록 함.
- 일정한 요건만 갖추면 주민등록번호의 변경이 가능하도록 함.

다. 담당 부처 및 기관

- 행정안전부 주민과
- 총리실

2) 강제적 지문날인 제도[63]

가. 배경 및 문제점

- 지문은 모든 사람에게 고유한 생체인식정보로서 민감정보(특별한 보호를 필요로 하는 정보)로 보호받을 필요가 있음.
- 한국에서 지문날인 제도는 1968 년 주민등록증 발급과 함께 도입되었으며, 17 세 이상 전 국민의 열손가락 지문날인을 하고 있음. 현재 전 국민의 지문은 전자적으로 관리되며 경찰청이 지문자동검색시스템(AFIS)를 통해 수사 목적으로 활용하고 있음. 행정안전부는 엄지 손가락 지문정보를 보유하고 있으며, 신원확인 목적으로 활용하고 있음.
- 17 세 이상 전 국민의 열손가락 지문날인을 강요하고 이를 범죄수사 목적으로 활용하는 것은 전 국민을 잠재적 범죄자로 취급하는 것임.
- 1999 년 사회단체 활동가들이 구체적인 법률적 근거 없이 경찰이 17 세 이상 전국민의 열손가락 지문날인 정보를 수집하여 데이터베이스 시스템으로 구축, 운영하는 데 대하여

63 작성단체: 진보네트워크센터

헌법소원을 제기하였음. 2004 년 17 세에 달한 청소년 3 인도 국가의 지문날인 제도가 위헌이라는 취지로 헌법소원을 제기하였음. 그러나 헌법재판소는 2005 년 경찰법 및 경찰관직무집행법에 경찰의 직무에 "치안정보의 수집, 작성 및 배포"가 포함되어 있다는 이유로 기각하였음.[64] 2011 년 또다시 청소년 지문날인 거부자들이 헌법소원을 제기하였으나 마찬가지 이유에서 합헌으로 결정되었음.

나. 권고사항

- 강제적인 지문날인 제도를 폐지할 것을 권고함.

다. 담당 부처 및 기관

- 행정안전부 주민과

3) 본인확인기관제도[65]

가. 배경 및 문제점

- 정부는 과거부터 계속되어 왔던 개인정보 대량유출 사태에 대한 대응으로 그러한 유출공작의 핵심대상이 되는 주민등록번호가 정보통신망을 통해 수집되는 것을 2012 년부터 금지했음. 그러나 정보통신망법상[66] 본인확인기관은 예외적으로 주민등록번호 수집 권한이 있음
- 본인확인을 요구하는 수많은 법령들이 본인확인기관이 제공하는 본인확인 방법을 이용하도록 하고 있어 청소년보호법, 공직선거법, 게임산업진흥법 등에 따라 본인확인의무를 가진 인터넷업체들은 정보통신망 상의 본인확인을 계속해야만 했고, 각종 본인확인 시행령들은 본인확인방법을 한정적으로 열거하였으며, 인터넷업체들은 그중 유일하게 보편성이 있는 이동통신사 본인확인서비스에 의존할 수밖에 없게 되었음
  - ❍ 이동통신사들이 제공하는 SMS 방식의 본인확인 서비스는 이미 독점적인 지위를 유지하고 있으며, 최명길 국회의원이 방송통신위원회로부터 제공받은 자료에 따르면 이동통신 3 사는 2015 년 한 해에만 본인인증 서비스에서 258 억 원 정도의 수익을 올린 것으로 보도되기도 함
- 정보통신망법 상 본인확인기관 제도의 도입취지는 본인확인기관에게 주민등록번호를 대체하는 본인확인 수단을 개발하라는 것이었으나, 휴대폰 가입자의 주민등록번호를

---

64 헌법재판소 2005. 5. 26. 99 헌마 513 등

65 작성단체: 오픈넷

66 정통망법 제 23 조의 2(주민등록번호의 사용 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제 23 조의 3 에 따라 본인확인기관으로 지정받은 경우

수집하는 이통 3 사가 모두 본인확인기관으로 지정되어, 휴대폰 번호가 휴대폰 가입자의 주민등록번호와 1 대 1 로 연결되어 있는 상황에서는 사실상 전자주민등록증 방식의 본인확인 서비스를 가능케하고 있음

- 2014 년 3 월 이통 3 사 중 하나인 KT 가 해킹을 당해 약 1200 만명의 가입자의 주민등록번호를 포함한 개인정보가 유출됨. 이러한 대규모 유출사태가 발생한 것은 이통사들이 본인확인기관으로 지정되어 주민등록번호를 수집할 수 있었기 때문임
- 또한 이통사들은 가입자들이 인터넷에서 본인확인을 했는지에 대한 기록을 보관하게 되어 있어, 성인 인증 웹사이트나 실명제 웹사이트에 접속한 기록 등이 이통사에게 남게 됨. 이와 같이 사생활의 비밀에 해당하는 정보가 이통 3 사에 집중되면 이통사는 자연스럽게 가입자들의 취향을 프로파일링할 수 있게 되며, 빅브라더가 될 것이라고 해도 과언이 아닐 것임
- 2014 년 6 월 오픈넷은 헌법재판소에 본인확인기관 지정 제도가 국민의 개인정보자기결정권을 침해한다는 이유로 헌법소원을 제기한 바 있음

나. 권고사항

- 주민등록번호 및 가입자의 사생활의 비밀에 해당하는 민감한 정보가 특정 사업자에게 집중적으로 보관될 것을 강요하는 정보통신망법 상의 본인확인기관 지정 제도를 폐지할 것

다. 담당 부처 및 기관

- 방송통신위원회

4) 연계정보(CI)[67]

가. 배경 및 문제점

- 연계정보(CI, Connecting Information)는 서비스 연계를 위한 웹사이트간 공동 식별자로 88byte 로 암호화된 정보를 의미함. 이는 주민등록번호를 기반으로 인터넷 본인확인 기관이 생성하며 사이트간 제휴서비스 제공 시 고객 식별 용도로 활용됨. 즉, 연계정보란 가명처리 된 주민등록번호라고 볼 수 있음. CI 는 전국민 주민등록번호와 1:1 로 매칭되기 때문에 온라인 어디서나 개인을 고유하게 식별할 수 있는 '온라인 주민등록번호'인 셈임.
- 주민등록번호로 모든 행정서비스 및 민간 업체의 본인확인 및 실명확인이 이루어지다보니 주민등록번호의 수집·활용에 대한 문제가 지속적으로 발생해 왔음. 이에 대한 지속적인 문제제기의 결과 주민등록번호의 수집·활용을 제한적인 경우에만 할 수 있도록 법이

67 작성단체: 진보네트워크센터

개정되면서, 주민등록번호 대신 온라인 상에서 본인확인을 위한 수단으로 도입된 것이 CI 임.

- 국내 주요 인터넷 업체들은 필요이상으로 이용자에게 본인확인을 요청할 뿐 아니라, CI 를 주민등록번호 만큼 보호하지 않는다는 법의 헛점을 이용해 이용약관을 통해 포괄동의를 받고 CI 를 활용해 왔음. 수사기관 역시 CI 를 통해 이용자의 온라인 행적을 추적해 왔음.
- 결국 주민등록번호와 연계된 CI 를 통해, 개인의 온·오프라인 행적이 고스란히 추적 가능 한 상태에 놓이게 됨으로써 익명을 기반으로 한 온라인 표현의 자유를 침해하고 있음.
- CI 를 이용한 본인확인제도는 인터넷 실명제와 연결됨. 즉, 익명성을 기반으로 한 온라인 환경에서 본인인증을 하지 않아도 사용자 각각을 식별하고 범죄 등 문제 발생시 차단 및 처벌할 방법이 있음에도 불구하고, 실명인증과 함께 본인확인을 함으로써 해당 이용자의 발언권을 제약하는 위축효과(chilling effect)를 낳게됨.
- 2012 년 8 월 23 일, 헌법재판소[68]는 게시판 이용자가 본인확인절차를 거쳐야만 게시판을 이용할 수 있도록 하는 것은 인터넷 게시판 이용자의 표현의 자유, 개인정보자기결정권 및 인터넷게시판을 운영하는 정보통신서비스 제공자의 언론의 자유를 침해한다고 판단한 바 있음.
- 실제 CI 가 암호화되어 CI 만으론 개인을 식별할 수 없다고 하더라도, 전화번호나, 성명, 휴대전화번호 등과 결합하면 주민등록번호처럼 개인의 식별이 가능해짐.
- 2019 년 2 월 14 일, 과학기술정보통신부는 '정보통신 진흥 및 융합 활성화 등에 관한 특별법'을 근거로 첫 ICT 규제 샌드박스 사업으로 카카오 페이와 KT 가 신청한 <메신저·문자 기반 행정·공공기관 고지서 모바일 전자고지 서비스>에 임시허가 조치를 내린 바 있음. 이 조치를 통해 행정·공공기관의 모바일 전자고지를 위해 본인확인기관이 주민등록번호를 연계정보로 일괄 변환하여 사용할 수 있도록 했음.
- 공공기관이 주민등록번호를 처리하기 위해선 "법령상 구체적으로 주민등록번호 처리를 요구하거나 허용하는 근거가 있는 사무"[69]여야 함. 하지만 현재 문자, 이메일 등 동의에 의한 통지를 수행하는 행정기관은 당사자의 휴대전화 번호, 이메일 주소 등이 자주 바뀌기 때문에 전국 어디서나 추적하여 알리기 위해 CI 기반 알림톡이 필요하다는 입장임. 그러나 정부가 활용하고자 하는 알림톡 서비스는 국민식별번호가 민간 및 공공영역에서 범용적으로 수집, 활용되는 한국에서만 가능한 기형적 구조의 서비스라 할 수 있음. 정부기관이 CI 를 통해 온라인에서 국민을 식별하고 추적할 수 있도록 하는 것은 행정권력의 남용이라 할 수 있음.
- 이처럼 정부가 나서서 특정 기업의 서비스를 활용하여 민감한 개인정보인 주민등록번호를 활용하는데 적극적으로 나서는 것은 분명한 개인정보자기결정권 침해임.

나. 권고사항

68 헌법재판소 2012.8.23. 2010 헌마 47·252(병합).

69 개인정보보호법 제 24 조

- 정보통신망법 상의 본인확인기관 지정 제도를 폐지되어야 하며, 따라서 온라인 주민등록번호인 CI 역시 폐지되어야 함.
- 온라인에서 불필요한 본인확인은 개인정보 자기결정권 침해이며, 따라서 개인정보 감독기구는 불필요한 본인확인이 이루어지지 않도록 계도할 필요가 있음.

다. 담당 부처 및 기관

- 과학기술정보통신부
- 방송통신위원회
- 개인정보보호위원회

4. 통신의 익명성[70]

1) 휴대전화 실명제

가. 배경 및 문제점

- 2014 년 10 월 신설된 전기통신사업법 제 32 조의 4[71]는 전기통신사업자가 전기통신역무 제공에 관한 계약을 체결하는 과정에서 부정가입방지시스템 등을 이용하여 계약 상대방의 본인 여부를 확인해야만 하는 일명 '휴대폰 실명제'를 규정하고 있음. 즉 이통사는 휴대폰 계약 체결시 계약 상대방의 본인 여부를 확인해야 하며, 본인이 아니거나 본인 여부 확인을 거부하는 경우에는 계약의 체결을 거부할 수 있음
- 휴대폰 실명제는 이용자의 익명통신의 자유, 사생활의 비밀과 자유, 개인정보자기결정권을 침해하며, 이에 대해 오픈넷은 2017 년 11 월 헌법소원을 청구하여 현재 심리중
  - 익명통신의 자유 침해: 표현의 자유에 대해 헌법재판소는 익명표현의 자유가 포함된다는 점을 분명히 한 바 있으며, 이와 마찬가지로 통신의 비밀보호 대상에는 통신의 내용뿐만 아니라 통신의 당사자(수신인과 발신인), 수신지와 발신지, 발신횟수 등 통신과 관련된 일체를 포괄하며, 이에는 상대방 및 제 3 자에게 신원을 밝히지 않고 익명으로 통신할 자유인 '익명 통신의 자유'를 당연히 포함함. 그런데 휴대폰 실명제는 익명 통신을 전면적으로 불가능하게 하므로 익명 통신의 자유를 명백히 침해함
  - 프라이버시 침해: 오늘날 온라인에서 이루어지는 모든 통신과 표현행위는 기록을 남기기 때문에 국가에 의한 감시와 추적이 매우 용이해졌음. 그런데 휴대폰 실명제는 모든 통신기기를 이용자의 실제 신원과 강제적으로 연계시킴으로써 비단 국가에 의해서뿐만 아니라 기업과 사인에 의한 프라이버시 침해 위험을 훨씬 가중시킴
  - 개인정보자기결정권 침해: 휴대폰 실명제는 전기통신사업자가 정보주체의 이름, 주민등록번호, 주소 등 본인확인정보를 조사하고 수집·보관하게 할 의무를 지우고

---

70 작성단체: 오픈넷

71 제 32 조의 4(이동통신기기 부정이용 방지 등) ① 생략

② 전기통신역무의 종류, 사업규모, 이용자 보호 등을 고려하여 대통령령으로 정하는 전기통신사업자는 전기통신역무 제공에 관한 계약을 체결하는 경우(전기통신사업자를 대리하거나 위탁받아 전기통신역무의 제공을 계약하는 대리점과 위탁점을 통한 계약 체결을 포함한다) 계약 상대방의 동의를 받아 제 32 조의 5 제 1 항에 따른 부정가입방지시스템 등을 이용하여 본인 여부를 확인하여야 하고, 본인이 아니거나 본인 여부 확인을 거부하는 경우 계약의 체결을 거부할 수 있다. 전기통신역무 제공의 양도, 그 밖에 이용자의 지위승계 등으로 인하여 이용자 본인의 변경이 있는 경우 해당 변경에 따라 전기통신역무를 제공받으려는 자에 대하여도 또한 같다.

③ 제 2 항에 따라 본인 확인을 하는 경우 전기통신사업자는 계약 상대방에게 주민등록증, 운전면허증 등 본인임을 확인할 수 있는 증서 및 서류의 제시를 요구할 수 있다.

④ 제 2 항에 따른 본인 확인방법, 제 3 항에 따른 본인임을 확인할 수 있는 증서 및 서류의 종류 등에 필요한 사항은 대통령령으로 정한다.

있는데, 본인확인정보는 개인의 동일성을 식별할 수 있게 하는 정보로서 개인정보에 해당하므로, 당연히 이용자의 개인정보자기결정권을 침해함

- 휴대폰 실명제는 개인정보의 과도한 집적으로 해킹 등을 통한 유출 위험성을 높이며, 실제로 1 년이 멀다 하고 대규모의 정보 유출 사고가 지속적으로 발생하고 있는 것이 현실임. 특히 이통사는 수차례 개인정보 유출 사고의 근원이 되었음에도 불구하고, 휴대폰 실명제는 이통사의 개인정보 수집을 제한하기는커녕 더욱 광범위한 수집 권한을 인정하고 있음

나. 권고사항

- 익명통신의 자유, 사생활의 비밀과 자유, 개인정보자기결정권을 침해하는 휴대폰 실명제를 폐지할 것

다. 담당 부처 및 기관

- 과학기술정보통신부

2) 인터넷 실명제: 공직선거법, 청소년보호법, 게임산업법

2-1) 공직선거법상 실명제

가. 배경 및 문제점

- 공직선거법 제 82 조의 6[72]은 인터넷 언론사가 선거운동기간 중 자사 홈페이지 게시판、대화방 등에 정당·후보자에 대한 글을 게시할 경우 실명을 확인해야 한다고 하고 있고, 그 방법 중 하나로 정보통신망법 제 44 조의 5 에 따른 본인확인조치를 열거하고 있음
- 인터넷 언론사에는 네이버 등 인터넷 포털사이트도 그 대상이 됨. 또한 법은 본인확인조치 의무의 대상으로서 "정당·후보자에 대한 지지·반대의 글을 일반 이용자들이 게시할 수 있도록 하는 경우"라고 하여 지지, 반대의 글이 게시될 '가능성'만 있으면 규제대상이

72 제 82 조의 6(인터넷언론사 게시판·대화방 등의 실명확인) ① 인터넷언론사는 선거운동기간 중 당해 인터넷홈페이지의 게시판、대화방 등에 정당、후보자에 대한 지지、반대의 문자、음성、화상 또는 동영상 등의 정보(이하 이 조에서 "정보등"이라 한다)를 게시할 수 있도록 하는 경우에는 행정안전부장관 또는「신용정보의 이용 및 보호에 관한 법률」제 2 조제 4 호에 따른 신용정보업자(이하 이 조에서 "신용정보업자"라 한다)가 제공하는 실명인증방법으로 실명을 확인받도록 하는 기술적 조치를 하여야 한다. 다만, 인터넷언론사가「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제 44 조의 5 에 따른 본인확인조치를 한 경우에는 그 실명을 확인받도록 하는 기술적 조치를 한 것으로 본다.

되도록 하고 있는 바, 사실상 일반 이용자가 글을 게시할 수 있도록 하는 게시판, 댓글 등의 서비스를 제공하는 경우라면 모두 규제대상이 됨

- 공직선거법상 실명제는 익명표현의 자유를 침해할뿐만 아니라 익명통신의 자유도 침해함

나. 권고사항

- 익명통신의 자유를 침해하는 공직선거법상 실명제를 폐지할 것

다. 담당 부처 및 기관

- 중앙선거관리위원회

2-2) 청소년보호법상 실명제

가. 배경 및 문제점

- 2012. 9. 16. 부터 시행 중인 청소년보호법 제 16 조[73]는 청소년유해매체물을 제공하려는 자에게 '연령확인' 외에도 '본인확인' 의무를 부과하고 있음
- 청소년유해매체물에 접근하려는 사람의 연령확인에만 그치는 것이 아니라 청소년 및 성인을 포함한 모든 사람들에 대한 본인확인 의무화는 익명 통신의 자유, 개인정보자기결정권, 익명 표현의 자유, 알 권리를 침해함
- 특히 청소년보호법상 본인확인을 위해서는 본인확인을 하는 기관이 이용자의 개인정보를 항상 확보하고 있어야 하는데, 이처럼 본인확인기관에 개인정보가 집적되고 사업자의 본인확인 요청에 따라 발생하는 본인확인정보가 집적되면 필연적으로 개인정보 유출위험에서 자유로울 수 없음
- 오픈넷은 2013 년 5 월 해당 조항에 대해 헌법소원을 제기한 바 있음

나. 권고사항

- 익명 통신의 자유와 개인정보자기결정권을 침해하는 청소년보호법상 실명제를 폐지할 것

다. 담당 부처 및 기관

- 여성가족부

---

73 제 16 조(판매 금지 등) ① 청소년유해매체물로서 대통령령으로 정하는 매체물을 판매ㆍ대여ㆍ배포하거나 시청ㆍ관람ㆍ이용하도록 제공하려는 자는 그 상대방의 나이 및 본인 여부를 확인하여야 하고, 청소년에게 판매ㆍ대여ㆍ배포하거나 시청ㆍ관람ㆍ이용하도록 제공하여서는 아니 된다.

3-3) 게임산업법상 실명제

가. 배경 및 문제점

- 2012. 9. 16. 부터 시행 중인 게임산업법 제 12 조의 3[74]은 게임 과몰입 및 중독 예방을 위하여 온라인 게임물 회원가입시 온라인 게임물 관련사업자에게 가입자의 본인여부를 확인하도록 하고 있고, 18 세 미만 청소년의 경우 친권자 등 법정대리인의 동의확보의무를 부여하고 있음
- 온라인 게임물 회원가입시 청소년 및 성인을 포함한 모든 사람들에 대해 본인확인을 하는 것은 익명 통신의 자유, 개인정보자기결정권, 익명 표현의 자유를 침해함
  - ❍ 특히 본인확인을 위해서는 본인확인을 하는 기관이 이용자의 개인정보를 항상 확보하고 있어야 하는데, 이처럼 본인확인기관에 개인정보가 집적되고 사업자의 본인확인 요청에 따라 발생하는 본인확인정보가 집적되면 필연적으로 개인정보 유출위험에서 자유로울 수 없음
- 오픈넷은 2013 년 7 월 해당 조항에 대해 헌법소원을 제기한 바 있음

나. 권고사항

- 익명 통신의 자유와 개인정보자기결정권을 침해하는 게임산업법상 실명제를 폐지할 것

다. 담당 부처 및 기관

- 문화체육관광부

---

74 제 12 조의 3(게임과몰입、중독 예방조치 등) ① 게임물 관련사업자[「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제 2 조제 1 항제 1 호의 정보통신망(이하 "정보통신망"이라 한다)을 통하여 공중이 게임물을 이용할 수 있도록 서비스하는 자에 한한다. 이하 이 조에서 같다]는 게임물 이용자의 게임과몰입과 중독을 예방하기 위하여 다음 각 호의 내용을 포함하여 과도한 게임물 이용 방지 조치(이하 "예방조치"라 한다)를 하여야 한다.

1. 게임물 이용자의 회원가입 시 실명、연령 확인 및 본인 인증
2. 청소년의 회원가입 시 친권자 등 법정대리인의 동의 확보
3.-7. 생략

5. 개인정보의 보호

1) 빅데이터와 개인정보보호법제[75]

가. 배경 및 문제점

- 정부는 빅데이터 산업 활성화를 명분으로 정보주체의 동의없는 개인정보의 산업적 활용을 허용함으로써 정보주체의 개인정보 자기결정권을 침해하고 있음.
- 2016 년 6 월, 박근혜 정부는 관계부처 합동(국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부)으로 <개인정보 비식별조치 가이드라인>을 발표함. 이에 따르면, 개인정보를 가이드라인에 따라 비식별 조치를 할 경우 "개인정보가 아닌 것으로 추정"하여 정보주체의 동의없이 수집 목적 외로 활용할 수 있도록 함. 또한, 한국인터넷진흥원(KISA) 등 공공기관을 전문기관으로 지정하여, 기업 간에 비식별 처리된 개인정보의 결합을 지원하고 결합된 개인정보를 원 데이터 보유기업에 제공함.
- 2017 년 국정감사에서 드러난 바에 따르면, 비식별조치 가이드라인에 따라 2016 년 8 월부터 2017 년 9 월까지 26 차례에 걸쳐 약 3 억 4 천여만건의 민간 기업의 데이터가 결합되었음. 정보주체는 자신의 개인정보가 결합을 위해 활용되었는지에 대해 통지 받지 못했으며, 해당 기업에 열람권을 요청해도 답변 받지 못함.
- 시민단체는 2017 년 11 월 9 일, 4 개의 비식별 전문기관과 20 개의 기업을 개인정보보호법 위반 등의 혐의로 고발하였으나, 검찰은 2019 년 3 월 25 일, 이 고발에 관하여 혐의 없음으로 불기소 처분하였음.
- 문재인 정부는 2018 년 11 월 15 일, 개인정보보호법 개정안(인재근 의원 대표발의) 발의하였는데, 이에 따르면 통계작성, 과학적 연구 목적으로 가명정보를 정보주체의 동의없이 애초 수집 목적 외로 활용하거나 제 3 자에게 제공할 수 있도록 하고 있음. (제 28 조의 2). 그런데 여기서 과학적 연구는 데이터를 기반으로 하는 새로운 기술·제품·서비스의 개발 등 기업의 내부적인 R&D 를 포함하고 있음. 또한, <개인정보 비식별조치 가이드라인>과 유사하게, 지정된 전문기관을 통해 서로 다른 기업의 개인정보를 결합하고, 결합된 개인정보를 가명 혹은 익명처리하여 원래의 데이터 보유기업 혹은 제 3 의 기업에 제공할 수 있도록 하고 있음. (제 28 조의 3) 가명정보에 대해서는 열람권, 보관 기간의 제한, 유출 통지 등 정보주체의 권리도 제한됨.
- 시민사회는 정부의 개인정보보호법 개정안은 기업들이 가명처리된 개인정보를 정보주체의 동의 없이 판매, 공유, 결합하도록 허용함으로써 소비자(이용자) 개인정보 권리를 침해하고 있다고 비판하고 있음.
- 정부가 2018 년 11 월 15 일 발의한 신용정보법 개정안(김병욱 의원 대표발의)은 위의 개인정보보호법 개정안과 같이 개인신용정보를 가명처리를 하면 기업의 영리적인 연구 목적으로 정보주체의 동의없이 활용할 수 있도록 하고 있을 뿐만 아니라, SNS 정보를

75 작성단체: 진보네트워크센터

정보주체의 동의없이 신용평가 목적으로 활용할 수 있도록 허용하고 있음. 공개된 SNS 정보라고 할지라도 정보주체의 의사와 무관하게 자유롭게 활용할 수 있는 것은 아니며, SNS 정보를 신용평가에 활용하는 것은 이용자의 SNS 를 통한 표현의 자유를 침해하게 될 우려가 있음.

나. 권고사항

- 가명처리된 개인정보의 동의 없는 활용은 한 사회의 학술적 기반을 강화할 수 있는 학술 연구로 제한되어야 하며, 단지 기업 내부적인 연구를 위해 기업 간에 판매, 공유, 결합되어서는 안됨. 학술 연구 목적으로 개인정보를 제공하더라도 가능한 익명처리하는 등 충분한 안전조치가 마련되어야 하며, 해당 목적 달성을 저해하지 않는 한 정보주체의 권리를 보장해야 함.
- 빅데이터의 경제적 활용에만 매몰된 정부의 개인정보보호법 개정안 및 신용정보법 개정안은 폐기해야 하며, 적어도 유럽 GDPR 수준의 개인정보보호 제도를 마련해야 할 것임.

다. 담당 부처 및 기관

- 행정안전부, 방송통신위원회, 금융위원회, 개인정보보호위원회

2) 개인정보감독기구[76]

가. 배경 및 문제점

- 유엔 전산처리된 개인정보파일의 규제 지침(1990)은 모든 국가들은 열거된 원칙들의 준수를 감시할 독립된 기관을 설치하도록 하고 있음. 또한, 유럽평의회의 <감독기구와 국경간 정보이동과 관련한 개인정보의 자동처리에 관한 개인 보호 협약의 추가의정서>(2001 년)는 조사권, 명령권, 의견제시권, 사법소추권 등 개인정보 감독기관의 구체적인 권한을 명시하고 있음.
- 한국의 경우 개인정보 보호법제가 개인정보보호법, 정보통신망법, 신용정보법 등으로 분산되어 있고, 개인정보 감독기구 역시 행정안전부, 방송통신위원회, 금융위원회, 개인정보보호위원회 등으로 분산되어 있음. 행정안전부는 정부부처로서 독립성이 없으며, 방송통신위원회와 금융위원회는 빅데이터 산업 육성을 명분으로 개인정보 보호 완화 정책을 추진하고 있음. 개인정보보호위원회는 인사 및 예산의 독립성이 없고, 조사권, 시정조치권 등 감독기구로서 집행 권한을 가지고 있지 않음. 또한, 감독기구가 분산되어 있어 통일된 개인정보 보호정책의 추진 및 효율적인 감독이 저해되고 있음.

76 작성단체: 진보네트워크센터

- 2018 년 11 월 15 일, 정부가 발의한 개인정보보호법 개정안(인재근 의원 대표발의)은 행정안전부와 방송통신위원회의 감독권한을 개인정보보호위원회로 일원화하고 있음. 그러나 금융위원회의 감독권한은 여전히 분리되어 있으며, 개인정보보호위원회의 일부 권한(권리침해에 대한 조사 및 처분, 분쟁조정 등)에 대해서만 국무총리의 지휘, 감독권을 배제하고 있어, 개인정보보호와 관련된 법령의 개선, 정책·제도·계획 수립·집행 등 개인정보보호위원회의 중요한 기능에 대해서 독립성을 보장하지 않고 있음.

나. 권고사항

- 개인정보 감독기구를 개인정보보호위원회로 일원화하고 완전한 독립성을 보장할 것.

다. 담당 부처 및 기관

- 행정안전부, 방송통신위원회, 금융위원회, 개인정보보호위원회

3) 소비자 개인정보[77]

가. 배경 및 문제점

- 홈플러스는 보험회사에 유상판매할 목적으로 개인정보 약 712 만건을 수집하면서 판매사실을 고지하지 않았으며, 개인정보 동의사항을 1mm 크기로 기재하여 사실상 읽을 수 없도록 하였음. 또한 생년월일, 자녀수 등 불필요한 항목에 대해서 동의하지 않을 수 없도록 함.
- 한편 홈플러스는 제 3 자 제공 동의없이 보험회사들에게 개인정보를 넘기면 보험회사들이 필터링을 하여 보험계약 체결 가능성이 있는 사람들만 추린 후 홈플러스가 그 사람들을 대상으로 사후적으로 제 3 자 제공 동의를 받은 후 다시 보험회사에 넘김.
- 한국소비자단체협의회에서 소비자 683 명을 원고로 하여 피고 홈플러스, 라이나생명보험, 신한생명보험에 제기한 손해배상청구소송에서 항소심 법원은 홈플러스는 고객 사은행사의 일환으로 경품을 지급하는 것처럼 기망적인 광고행위를 한 점, 개인정보의 수집·이용 목적 등의 사항을 약 1mm 크기의 읽기 어려운 작은 글씨로 기재한 점, 경품추첨 사실을 알리는 데 필요한 개인정보와 관련 없는 사생활의 비밀에 관한 정보와 고유식별정보까지 수집함으로써 목적에 필요한 범위 외의 정보까지 수집한 점 등을 지적하며 개인정보보호법, 표시광고법 등을 위반하였다고 봄. 그리고 이러한 홈플러스의 불법행위로 피해자들이 정신적 고통을 받았을 것임이 인정되므로 홈플러스는 위자료 200,000 원을 지급하라고 판시함. 또한 홈플러스가 제 3 자인 보험회사들에게 미동의 개인정보를 제공한 행위는 개인정보보호법을 위반한 것이라고 봄. 패밀리카드 회원들로서는 자신들의 개인정보를 제 3 자가 알게 될 수 있다는 불안감 또는 이를 영업에 활용함으로써 자신들이 영리행위의

77 작성단체: 한국소비자단체협의회

대상으로 취급되고 있다는 불쾌감을 느꼈을 것이므로 홈플러스와 보험회사들은 공동하여 정신적 손해에 대한 배상으로 각 50,000 원을 지급해야한다고 판시함.

- 한편 재판부는 특별법상 불법행위책임에 있어서도 고의·과실 요건에 한해 입증책임을 전환하고 있으므로 개인정보가 보험회사에 제공되었다는 사실의 입증책임은 소비자에게 있다고 봄. 소비자가 입증하지 못하는 한 불법행위의 피해자로 볼 수 없다고 판단하여 형사절차에서 개인정보가 제공되었음이 명확히 밝혀지지 않은 패밀리카드 회원 222 명의 청구를 전부 기각함. 현재 원고 222 명에 대하여 상고심절차가 진행 중임.
- 집단소송제의 부재로 소비자피해에 대하여 민사소송법상 손해배상청구의 소만을 제기할 수 있음. 그러나 민사소송은 다수의 피해가 있었음에도 공동소송에 참여한 소비자만이 구제받을 수 있음. 또한 기업이 모든 증거를 가지고 있는 상황에서 소비자에게 입증책임 있으며, 소비자는 소송에 소요되는 긴 시간과 높은 비용을 감내해야함. 설령 이를 감내하더라도 구제금액은 피해액수에 비해 현저히 낮음. 따라서 소비자 피해에 적용하는데 분명한 한계가 있음.

나. 권고사항

- 홈플러스는 개인정보 약 600 만 건을 판매하고 약 119 억 원이라는 막대한 수익을 얻었음에도 불구하고 피해구제액은 1%에도 못 미칠 만큼 적다는 점은 집단소송제의 부재로 인한 소비자 피해구제의 한계라고 할 수 있음. 따라서 집단소송제의 빠른 도입이 필요함.
- 소액, 다수의 피해를 구제할 수 있는 가장 효율적인 방법은 '소비자 집단소송제'의 도입임. 소비자 피해 특성에 맞는 절차와 입증책임의 완화, 증거개시제도, 징벌적 손해배상 등 법의 실효성을 높일 수 있는 장치가 마련된 '소비자 집단소송제'의 도입이 필요함.
- 재판부는 패밀리카드 회원의 개인정보가 보험회사들에게 제공되었을 가능성이 적지 않고, 증거의 편재 등으로 인해 피고가 증명에 용이한 위치에 있음을 인정하면서도 법해석의 원칙만을 고수하면서 소비자에게 입증책임을 지움. 소비자가 기업의 불법행위 사실을 입증하는 것은 사실상 불가능에 가까운 바, 입증책임의 전환이 필요함.

다. 담당 부처 및 기관

- 행전안전부, 개인정보보호위원회 (개인정보보호법 소관부처)

4) 건강정보와 프라이버시권[78]

4-1) 의료 정보의 목적 외 이용 및 제공

78 작성단체: 건강과 대안

가. 배경 및 문제점

- 진료 과정에서 의료기관에서 수집된 정보는 원칙적으로 의료기관이 개인의 의료적인 목적 달성을 위해서만 수집, 이용될 수 있음
- 그러나 현대 의료는 점차 디지털화되면서 다양한 의료 정보 처리 주체들이 개입되게 되었고(전자처방전 업체, 전자의무기록 유지보수 업체, 의무기록 보유, 저장업체, 의료기기 업체, 약국 등), 이들 각각이 환자의 명시적 동의와 법적 근거 없이 의료기관에서 수집된 환자의 의료 정보를 처리하고 있는 상황이 벌어지고 있음
- 관련현황
- 2010 년 SK 텔레콤이 전자처방전 형태로 제공된 의료기관의 환자 정보를 환자의 동의 없이 자체 서버에 저장해 처리하고 관련 업무로 이득을 취하였음: 현재 형사재판 진행 중
  - 2010 년 약학정보원이 의료기관이 처방전 형태로 약국에 제공한 의료정보를 가공하여 환자 동의 없이 IMS Health 에 제공하여 이득을 취하였음: 현재 형사재판 진행 중
  - 의료기관이 클라우드 서비스를 제공하는 IT 기업과 합작하여 환자 의료정보를 관련 IT 기업의 클라우드에 집적하고 이를 환자 동의 없이 다양한 용도로 활용하려는 시도를 보이고 있음
  - 아산병원, 현대중공업, 카카오 합작 회사 관련 보도: “카카오, AI 의료 빅데이터 사업 진출”[79]
  - 분당 서울대병원, 대웅제약, 네이버 합작 회사 관련 보도: “헬스케어 산업에 손 뻗는 IT 기업들…” [80]
  - 정부는 모바일 어플리케이션을 통해 개인의 의료정보를 보험회사에 손쉽게 제공할 수 있는 방안을 추진: 정부, 보험사에 개인 진료·건강정보 ‘빗장 풀기’ 논란[81]
  - 건강보험심사평가원, 개인의 의료정보를 비식별화했다는 이유로 민간보험사에 52 건(총 6420 만명분) 표본데이터 제공[82]

나. 권고사항

- 정보 주체의 동의 없이 의료정보에 대한 목적 외 이용, 제공을 엄격히 규제하고 극히 예외적인 경우에 한해 법제도를 명확히 하여 규제와 관련된 회색 지대를 없앰

다. 담당 부처 및 기관

- 보건복지부

79 https://m.yna.co.kr/view/AKR20180829078700017
80 http://it.chosun.com/site/data/html_dir/2019/03/15/2019031501989.html
81 http://www.hani.co.kr/arti/society/health/864560.html#csidx119c26a3c4298f98c71f39970351d23
82 http://www.hani.co.kr/arti/society/health/816649.html#csidxfcfd021d8be8866ba9fdf73ca91fb78

4-2) 건강 정보의 저장

가. 배경 및 문제점

- 건강 관련 개인 정보는 목적을 달성하기 위한 필요를 다한 후에는 폐기하는 것이 원칙임
- 그러나 건강보험공단, 건강보험심사평가원, 개별 의료기관 등은 연구 목적 사용 등의 이유로 명확한 법적 근거 없이 관련 정보를 반영구적으로 보유하고 있는 실정임[83]

나. 권고사항

- 의료기관 및 건강정보를 처리하는 공공기관에 건강정보 보유기간을 명시하는 법 제도 개선 권고

4-3) 의료기관의 개인정보 보호 의무 해태: 의료 정보 보안 부실

가. 배경 및 문제점

- 건강 정보는 개인정보 중에서 특히 민감한 개인정보이므로 개인정보 보호법에서 정하는 보안 관련 기준을 넘어 더욱 철저히 보안 조치가 필요한 정보임
- 그럼에도 불구하고 한국의 의료기관은 개인 의료정보에 대한 보안 수준이 낮아 의료 정보 유출 및 개인정보보호법 위반 사례가 빈번히 발생하고 있음
- 행정안전부가 2015 년~2016 년까지 분야별로 행정처분한 결과를 보면 전체 위반 건수(30 개 기관)는 73 건이었고, 이 가운데 의료분야 위반 건수는 22 건(6 개 기관)으로 나타났다.(2015 년 1 개 기관 4 건, 2016 년 5 개 기관 18 건)[84]

나. 권고사항

- 의료기관의 개인정보 보호 의무 이행에 대한 지도, 감독 강화

4-4) 개인 건강 정보의 오픈 데이터화

가. 배경 및 문제점

- 건강 정보는 민감정보이므로 그 자체는 물론이거니와 가명화된 형태로도 오픈 되어서는 안됨

---

83 정보인권연구소, 데이터 연계·결합 지원제도 도입방안 연구, 2017. 개인정보보호위원회

84 "의료기관서 개인정보보호법 자주 위반하는 것은?"
https://www.doctorsnews.co.kr/news/articleView.html?idxno=124752

- 그러나 건강보험공단은 2017 년 이전에는 가명화하였다는 이유로 표본 데이터셋을 누구나 내려 받아 이용할 수 있도록 하였고, 현재도 연구자들에게 일정한 절차를 거쳐 표본 데이터셋을 내려 받아 이용할 수 있도록 하고 있음 (건강보험공단 홈페이지 참고[85])

나. 권고사항

- 건강정보는 가명화되었다고 하더라도 오픈 데이터 형태로는 제공하지 않도록 관련 제도를 명문화할 것을 권고함

4-5) 건강 정보의 연구 목적 활용

가. 배경 및 문제점

- 건강정보는 개인의 동의 없이 연구 목적으로 활용될 수 있으나, 그 목적이 본래의 수집 목적과 비례하여야 하고 최대한의 안전 조치를 취한 상태에서 활용되어야 함
- 그러나 한국의 경우 개별 의료기관 및 공공기관(건강보험공단 등)이 보유하고 있는 개인 의료정보를 가명화하고 일정한 절차를 충족하였다는 조건 하에 법적 규정이 미비한 상태에서도 연구자들이 활용할 수 있도록 하고 있음
- 그리고 이러한 경우 개인정보 주체에게 개인 정보 활용 사항을 통지하고
- opt-out 할 권리를 주어야 함에도 불구하고 이러한 절차가 지켜지지 않고 있음 (건강보험공단 홈페이지 참고[86])

나. 권고사항

- 개인의 동의 없이 수행할 수 있는 과학적 연구의 범위, 절차, 보안 조치 등에 대해 법제도를 명문화할 것을 권고

5) 공공기관 개인정보의 정보수사기관 제공[87]

가. 배경 및 문제점

- 현행 개인정보보호법에 따르면, "범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우" 개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공할 수 있음(제 18 조 제 2 항 제 7 호). 다만 "정보주체 또는 제 3 자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고" 있지만 구체적인 요건을 부여하고 있지 않음.

85 https://nhiss.nhis.or.kr/bd/ab/bdaba001cv.do
86 https://nhiss.nhis.or.kr/bd/ab/bdabd003cv.do
87 작성단체: 진보네트워크센터

- 현행 개인정보보호법에 따르면, “국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보”에는 개인정보보호법의 주요 규율을 적용하지 아니함(제 58 조 제 1 항 제 2 호).
- 이에 한국사회에서는 개인정보처리자, 특히 공공기관이 보유하고 있는 개인정보가 정보 및 수사기관에 광범위하게 제공되는 데 대한 논란이 커져 왔음. 특히 수사기관의 경우, 공공기관이 보유한 개인정보를 대량으로 제공받아 비혐의자를 대상으로 저인망식(dragnet)으로 수사하는 일이 증가하고 있고, 건강정보(health-related information) 등 민감정보마저 무영장으로 제공받고 있음
- 2013 년, 경찰은 파업으로 수배중인 철도노조원들의 요양급여내역을 국민건강보험공단에서 무영장으로 제공받음. 이때 무영장으로 경찰에 제공된 철도노조원 정보는 국민건강보험공단 외에도 국민연금관리공단, 교육청 등 여러 공공기관을 아우름. 철도노조원들은 불법파업 혐의로 2014 년 3 월 11 일 기소되었으나 이후 무죄판결을 받음. 철도노조원들은 요양급여내역 제공에 대해 헌법소원을 제기하여 2018 년 헌법재판소에서 위헌으로 결정됨[88].
- 2014 년, 경찰은 건물에 “박근혜 정권 물러가라” “국정원 불법 선거개입” 등의 글귀로 정부를 비판한 낙서범을 잡겠다며 지방자치단체들로부터 무영장으로 3000 명의 기초생활수급자 정보를 제공받음[89].
- 2016 년, 경찰은 장애인 활동보조인 600 명의 개인정보를 지방자치단체에서 무영장으로 제공받아 이들의 과거 휴대전화 발신위치 등을 추적하는 방식으로 장애인 수급 부정을 일제히 수사함. 이처럼 장애인 활동보조인을 대상으로 한 저인망식 수사기법은 여러 지역 경찰에서 사용해 옴. 활동보조인들이 헌법소원을 제기하였으나 2018 년 기각됨[90]
- 2014 년 국회 국정감사에 따르면, 특히 건강정보의 경우 검찰과 경찰이 연평균 96 만 7 천건, 하루 평균 2 천 649 건의 건강보험 의료정보를 열람함.[91]
- 2013 년 정부의 반대에도 불구하고 국가정보원장을 공직선거법 위반으로 기소한 검찰총장에 대하여 청와대와 국가정보원이 그 사생활에 대하여 사찰함. 이 과정에서 구청 가족관계정보, 경찰 전산망, 건강보험시스템, 학교행정시스템(NEIS, National Education Information System) 등 전자정부 시스템이 불법조회되어 관련자들이 재판을 받고 있음.
- 그러나 헌법재판소의 위헌 결정을 비롯하여 논란이 계속되고 있음에도 정보 및 수사기관의 개인정보 수집을 통제 및 감독하기 위한 제도개선이 이루어지고 있지 않음
- 한국의 헌법재판소는 공공기관이 보유한 개인정보를 수사기관에 제공하는 것은 영장이 불필요한 임의수사라고 보았음. 다만 철도노조원의 헌법소원에 대해서는, 질병명을 포함한

88 헌법재판소 2018. 8. 30. 결정 2014 헌마 368.

89 허프포스트코리아. (2014). *정부 비판 낙서범, 기초수급자 중에 찾아보자?*. https://www.huffingtonpost.kr/2014/10/15/story_n_5987854.html [2019.5.15].

90 헌법재판소 2018. 8. 30. 결정 2016 헌마 483.

91 연합뉴스. (2014). <*기관에 퍼주고, 엿보고…건보 개인정보관리 '엉망'*> https://www.yna.co.kr/view/AKR20141016161100017 [2019.5.15].

민감한 요양급여내역에 대해 2~3 년에 걸친 장기간 내역을 제공받은 것이 불가피하지 않았다는 이유로 위헌으로 보았음. 그러나 장애인 활동보조인의 헌법소원에 대해서는, 수급부정 범죄의 공익이 매우 크기 때문에 지방자치단체의 대규모 개인정보 제공이 과잉하지 않다는 취지로 기각하였음.

- 수사기관의 개인정보 수집에 대해서는, 1987 년에 유럽평의회(CoE)의 경찰권고가 제정된 이래로, 2016 년 유럽이 이른바 'police directive'(DIRECTIVE (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA)를 제정하기까지 수사기관 또한 개인정보보호원칙을 준수할 것을 요구하는 국제규범이 강화되어 옴
- 정보기관의 개인정보 수집(data collection)에 대해서는, 에드워드 스노든 사건 이후로 유엔 총회의 디지털 프라이버시 결의안(A/RES/68/167) 등 국제적으로 적절한 통제와 감독에 대한 요구가 계속되어 옴

나. 권고사항

- 경찰 등 수사기관의 개인정보 수집에 대하여 개인정보 보호원칙을 준수하도록 통제하고 독립적인 제 3 의 기관으로부터 감독을 받을 수 있도록 제도를 개선할 것. 비혐의자를 포함하는 대규모 개인정보를 수집하기 위해서는 그 요건과 절차를 구체적으로 규정하는 등 법률에 따른 통제를 받을 것. 특히 건강정보 등 민감정보의 수집시 영장 등 법원의 통제를 받도록 할 것.
- 정보기관의 개인정보 수집에 대하여 필수적이고 비례적인 경우로 통제하기 위하여 독립적인 제 3 의 기관으로부터 감독을 받을 수 있도록 제도를 개선할 것. 정보기관이 개인정보를 수집하기 위해서는 그 요건과 절차를 구체적으로 규정하는 등 법률에 따른 통제를 받을 것.

다. 담당 부처 및 기관

- 행정안전부/개인정보보호위원회 (개인정보보호법 소관부처)
- 경찰청/국가정보원

6) 사회보장정보시스템[92]

가. 배경 및 문제점

92 작성단체: 민주 사회를 위한 변호사 모임

- 2010 년 보건복지부는 여러 복지급여사업을 하나의 전자정보시스템으로 관리하는 사회보장정보시스템 구축(2013 년 한차례 확충하여 현재 22 개 부처의 360 여 가지 복지사업 관리)
- 사회보장정보시스템은 사회보장급여나 서비스를 받는 모든 사람을 개인별, 가구별로 등록하여 자격과 이력을 관리하는 시스템으로, 2015. 12.기준 등록된 복지대상자는 17,140,887 명(중복포함)
- 사회보장정보시스템의 중요한 기능 중 하나는 신청자 및 수급자의 재산과 소득조사를 위한 자료 수집 및 관리
- 재산 및 소득조사를 위해 복지급여 또는 서비스신청자로부터 일괄 동의를 받아 납세정보 등 24 개 공공기관이 가지고 있는 77 종의 정보(2017. 12. 기준)와 140 여개 금융기관으로부터 금융거래 정보수집. 수집되는 정보 중 출입국기록도 있음. 이 중 상당수의 자료는 자동으로 갱신됨. 연 2 회 소득、재산 변동여부 확인조사 실시
- 2014 년 경제적 어려움을 이유로 한 60 대 모와 30 대 두 딸의 자살이 사회적으로 큰 반향을 일으키자 정부는 도움이 필요한 사람들을 적극적으로 찾아서 발굴하겠다고 선언하고 「사회보장급여의 이용、제공 및 수급권자 발굴에 관한 법률」(사회보장급여법)을 제정하여 단전、단수、건강보험료 체납 등의 정보를 당사자의 동의 없이 수집할 수 있도록 함. 빅데이터를 활용한 위기가정 “발굴”로 사회보장 사각지대를 해소하겠다는 것이 목적
- 이렇게 해서 발굴된 대상자의 수집된 정보 중 일부는 지방자치단체에는 본인 동의 없이 제공되며, 본인 동의 있으면 민간 자선단체에 제공될 수 있음
- 2017 년 사회보장급여법을 개정하여 대출금, 신용카드대금 연체 등 개인신용정보를 사회보장정보시스템으로 수집할 수 있도록 함
- 그러나 사회보장 비수급 빈곤층의 근본적 원인은 사회보장제도 특히 공공부조제도를 지배하는 잔여주의(residualism)에 있음. 예를 들어 사회보장정보시스템에 등록된 부양의무자의 소득、재산이 일정한 수준을 넘으면 공공부조에서 배제하는 식이다. 이처럼 엄격한 수급요건으로 인해 공공부조가 필요하지만 급여를 받지 못하는 인구는 2015 년 기준 93 만명에 달함(정부추정치). 사회보장정보시스템 도입으로 오히려 수많은 탈락자가 양산되어 그로 인해 적지 않은 자살이 발생함.
- 정부자료에 따르면 2018 년 1~11 월 사이 빅데이터를 활용하여 “발굴”한 243647 명 중 33.4%인 81354 명만이 어떠한 지원이라도 연계받았고, 그 중 28932 명만이 공공서비스를 연계받았으며 나머지는 민간 자선사업으로 연계됨. 즉 “발굴”된 취약계층 중 12% 미만이 공공서비스 연계로 이어짐.
- 2019 년 4 월 보건복지부는 3,560 억원을 들여 ‘차세대 사회보장정보시스템’ 구축하겠다고 발표. ‘차세대 사회보장정보시스템’으로 구현하겠다는 기능 중 하나는 전국민을 대상으로 하는 ‘복지멤버십’ 제도로서, 등록된 사람이 동의한 가구, 소득, 재산 관한 정보를 토대로 사회보장급여、서비스의 지원기준에 맞추어 정보시스템이 주기적으로 잠정적 판정을 하여 받을 가능성이 높은 사업 목록을 “맞춤형으로” 안내하는 것을 내용으로 함.

- 즉, 사회보장정보시스템에 '멤버'로 등록된 사람에 대해 현재 실제로 사회보장급여나 서비스를 받지 않더라도 가구, 재산, 소득에 관한 정보를 수집하고, 주기적으로 변동사항까지 반영하겠다는 것임. 전국민을 대상으로 하고 있고, 공공기관, 금융기관 등 수백 개의 기관에서 수집하는 정보의 방대함을 고려할 때 본인의 동의를 전제로 하고 있다 하더라도 개인정보 보호와 프라이버시권에 대한 잠재적 위협이 상당함
- 이처럼 사회보장급여나 서비스의 잠재적 제공을 내세우며 개인의 프라이버시에 속하는 방대한 정보를 수집하며 사회보장 전달체계를 전산시스템으로 대체하겠다는 발상은 정보의 집중을 통한 통제력 강화를 지향하는 것임
- 서로 내용과 요건이 제각각이고 분절되어 있는 복지급여 수급자격에 대한 입증책임을 당사자에게 부여하고 있어 정작 욕구가 높은 취약계층은 적합한 도움에 접근하기 어려운 배제적 구조를 그대로 둔 채 광범위한 정보수집으로 적합한 급여를 안내하겠다는 접근은 기본권을 보장하겠다는 효과보다 과도한 개인정보 침해의 위험성 큼

나. 권고사항

- 사회복지급여와 서비스의 빈약성과 신청자에게 배제적인 구조를 방치한 채 사회보장급여나 서비스가 필요한 사람들을 찾아내어 안내한다는 명목으로 취약계층을 대상으로 하는 본인의 동의 없는 정보수집을 중단하고 제도개선과 예산 확충을 통해 비수급 빈곤층 문제를 해결할 것
- 사회보장정보시스템으로의 과도한 정보집중을 가져올 것으로 예상되는 '복지멤버십' 계획을 폐기하고 신청자의 욕구에 맞는 급여가 보장될 수 있도록 전달체계를 개혁하여 복지급여와 서비스에 대한 접근성을 높일 것

다. 담당 부처 및 기관

- 보건복지부

7) DNA 데이터베이스[93]

가. 배경 및 문제점

- 점거 및 농성을 행한 철거민, 노동조합원, 노점상 활동가 등이 DNA 채취대상이 되어 국가 디엔에이신원확인정보데이터베이스(DNA identification database)에 디엔에이신원확인정보(DNA identification information, known as 'profile')가 보관됨
- 2011 년 용산철거민과 쌍용노동자들이 제기한 헌법소원에 대해서는 2014 년 기각.각하가 결정되었음. 피채취자들의 경우 디엔에이신원확인정보가 다른 개인정보나 지문 등 타

93 작성단체: 민주 사회를 위한 변호사 모임

생체정보와 달리 가족들과 공유하는 유전정보를 포함하고 있으며 국가데이터베이스의 수록으로 인한 침해가 자녀 등 가족구성원에게 확장된다는 점을 호소함

- 2016 년 KEC 노동조합 조합원들이 헌법소원을 제기함. 2010 년 공장점거 파업농성 중 "다중의 위력으로써 타인의 건조물에 침입했다는 죄"로 유죄판결 선고 후 영장이 발부되어 2015 년부터 2016 년 사이에 디엔에이감식시료(DNA sample)를 채취당함. 2017 년 민주노점상전국연합 활동가들이 헌법소원을 제기함. 2013 년 아울렛상가 점거 집회과정에서 "다중의 위력으로써 매장 안에 침입했다는 죄"로 유죄판결 선고 후 영장이 발부되어 2017 년 디엔에이감식시료를 채취당함. 2018 년 8 월 30 일 위 두 사건을 병합하여 헌법불합치가 결정됨[94]. DNA 법 영장절차 조항이 채취대상자의 의견진술권, 불복청구권, 구제절차 등을 결여하고 있다는 이유임
- 그러나 헌법재판소의 헌법불합치 결정을 비롯하여 논란이 계속되고 있음에도 정부는 제도개선을 위한 법개정안을 제출하지 않고 있으며, 피해자들의 DNA 정보 삭제청구를 거부하였음
- 2010 년 제정된 디엔에이신원확인정보의 이용 및 보호에 관한 법률(ACT ON USE AND PROTECTION OF DNA IDENTIFICATION INFORMATION)의 경우, 11 종의 열거된 범죄에 해당하는 소년범을 포함한 형확정자 및 구속피의자에 대하여 개별적으로 재범여부를 평가하지 않고 모두 DNA 를 채취하여 그 디엔에이신원확인정보(DNA identification information, known as 'profile')를 데이터베이스에 보관후 수사에 활용하고 있음.
  - 이 DNA 법은 디엔에이감식시료의 채취 요건으로 재범의 위험성을 명시하고 있지 않고 영장발부 절차 규정에서도 영장발부의 요건을 명시하지 아니하여 채취대상범죄에 해당하면 획일적으로 채취하고 있다는 문제가 있음.
  - 이로 인하여 디엔에이신원확인정보데이터베이스에는 실형을 선고받은 형확정자는 23%에 불과함.[95]
  - 또 채취대상으로 "단체 또는 다중의 위력을 보인" 폭력행위를 포함하면서 항의과정에서 점거 및 농성을 행한 철거민, 노동조합원, 노점상 활동가 등이 채취대상이 됨.
- DNA 법은 다음의 경우에 한해 데이터베이스에서 신원확인정보를 삭제할 수 있음. 즉, 무죄 등 특별한 사유가 없으면 대상자가 사망한 경우 직권 또는 본인의 신청이 있어야만 신원확인정보를 삭제할 수 있음.
  - 이는 대상자가 재범하지 않고 상당 기간을 경과하는 경우에도 디엔에이신원확인정보의 보존기간이 지나치게 길다는 점에서 문제의 심각성이 있음.

---

94 헌재 2018. 8. 30. 2016 헌마 344·2017 헌마 630. 위 법률조항은 2019. 12. 31.을 시한으로 입법자가 개정할 때까지 적용됨.

95 <디엔에이신원확인정보 데이터베이스 연례 운영보고서>에 따르면 수록된 전체 137,519 명의 형 확정자 중 실형범은 37,636 명이고 벌금·집행유예·조건부선고유예 등을 받은 '수형인외 형 확정자'는 99,883 명임.

- ❍ 특히 소년범의 경우 매우 가혹한 측면이 있음.
- ❍ 헌법재판소도 디엔에이법 삭제조항에 대한 보충 및 반대의견[96]에서 국민의 기본권 제한을 최소화하기 위해 일정 기간 재범하지 않은 적절한 범위의 대상자의 경우에는 디엔에이신원확인정보를 삭제할 수 있도록 개선할 필요가 있다고 반복적으로 지적한 바 있음.

제 13 조(디엔에이신원확인정보의 삭제) ① 디엔에이신원확인정보담당자는 수형인등이 재심에서 무죄, 면소, 공소기각 판결 또는 공소기각 결정이 확정된 경우에는 직권 또는 본인의 신청에 의하여 제 5 조에 따라 채취되어 데이터베이스에 수록된 디엔에이신원확인정보를 삭제하여야 한다.
② 디엔에이신원확인정보담당자는 구속피의자등이 다음 각 호의 어느 하나에 해당하는 경우에는 직권 또는 본인의 신청에 의하여 제 6 조에 따라 채취되어 데이터베이스에 수록된 디엔에이신원확인정보를 삭제하여야 한다.
1. 검사의 혐의없음, 죄가안됨 또는 공소권없음의 처분이 있거나, 제 5 조제 1 항 각 호의 범죄로 구속된 피의자의 죄명이 수사 또는 재판 중에 같은 항 각 호 외의 죄명으로 변경되는 경우. 다만, 죄가안됨 처분을 하면서 「치료감호법」 제 7 조제 1 호에 따라 치료감호의 독립청구를 하는 경우는 제외한다.
2. 법원의 무죄, 면소, 공소기각 판결 또는 공소기각 결정이 확정된 경우. 다만, 무죄 판결을 하면서 치료감호를 선고하는 경우는 제외한다.
3. 법원의 「치료감호법」 제 7 조제 1 호에 따른 치료감호의 독립청구에 대한 청구기각 판결이 확정된 경우
③ 디엔에이신원확인정보담당자는 수형인등 또는 구속피의자등이 사망한 경우에는 제 5 조 또는 제 6 조에 따라 채취되어 데이터베이스에 수록된 디엔에이신원확인정보를 직권 또는 친족의 신청에 의하여 삭제하여야 한다.

나. 권고사항

- 국가 디엔에이신원확인정보 데이터베이스 수록대상에 있어, 개별 대상자의 재범위험성에 대하여 신중히 판단할 수 있도록 사법심사절차를 보완하고 대상자가 의견을 진술하거나 불복할 수 있는 구제절차를 둘 것
- 대상자가 재범하지 않고 상당 기간을 경과하는 등 데이터베이스 운영목적이 달성된 경우, 수록된 사람의 신원확인정보에 대한 삭제권을 보장할 것

다. 담당 부처 및 기관

- 법무부 (법률 소관부처)
- 대검찰청 (형확정자 데이터베이스 운영사무)

96 헌법재판소 2011 헌마 28; 헌법재판소 2016 헌마 344, 2017 헌마 630(병합)

- 경찰청 (구속피의자, 범죄현장 데이터베이스 운영사무)

6. 노동감시[97]

가. 배경 및 문제점

- 최근 사용자가 폐쇄회로 텔레비전(이하 'CCTV')과 휴대전화 어플리케이션 등 전자기기를 이용하여 근로자를 감시하는 것이 사회적으로 큰 문제가 되고 있음.
- 대기업 KT 는 근로자들에게 특정 어플리케이션 설치를 지시하였는데, 그 어플리케이션을 설치할 경우 회사 관리자가 개인 휴대전화에 있는 연락처, 문자 메시지는 물론 현재 위치, 달력일정, 계정과 사진정보 등에 접근할 수 있음. 회사는 근로자가 설치를 거부하자 해당 근로자에게 정직 1 개월 징계 처분을 내리는 등 실질적으로 어플리케이션 설치를 강제하였음. CCTV 영상자료를 근로자 징계에 사용한 사례는 사기업뿐만 아니라 교사, 경찰관 등 공무원까지 다양한 업종에서 문제가 제기되고 있으며, 일부 사기업은 노동조합 설립 후 280 여명이 근무하는 공장에 직원 휴게실 등 CCTV 를 200 여대 설치하여 문제가 되기도 하였음.
- 개인정보보호법[98]은 1)법령에서 구체적으로 설치를 허용한 경우, 2)범죄의 예방 및 수사를 위하여 필요한 경우, 3)시설안전 및 화재 예방을 위하여 필요한 경우, 4)교통단속을 위하여 필요한 경우, 5)교통정보의 수집·분석 및 제공을 위하여 필요한 경우 이외에 공개된 장소에 영상정보처리기기[99]를 설치·운영 하여서는 아니 된다고 정하고 있음. 따라서 근로자를 감시할 목적으로 CCTV 를 설치하는 것은 법에서 정한 목적 외로 수집된 정보를 사용하는 것으로 법률에 근거가 없음.
  한편, 근로자참여 및 협력증진에 관한 법률 제 20 조 제 1 항 제 14 호는 '사업장 내 근로자 감시 설비의 설치'를 노사협의회 협의사항으로 정하고 있어 근로자와 협의한 경우 근로자 감시의 여지를 두고 있지만, 개인 휴대전화의 내부정보를 임의로 습득할 수 있는 어플리케이션 설치를 강제하는 것은 어떠한 법률적 근거도 없음.
- 국가인권위원회는 CCTV 를 이용한 노동감시를 중단할 것[100]과 고용노동부에 사업장 전자감시로부터 근로자 개인정보 보호를 강화할 방안을 마련할 것을 권고하였으나 현장에서는 여전히 각종 전자기기를 이용한 감시가 만연한 상황이며, 새로운 매체를 이용한 노동감시에 대하여 어떠한 대책도 없는 실정임.

---

97 작성단체: 민주 사회를 위한 변호사 모임

98 개인정보보호법 제 25 조(영상정보처리기기의 설치, 운영 제한)

99 "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서, 폐쇄회로 텔레비전(CCTV)과 네트워크 카메라를 의미합니다(개인정보보호법 제 2 조 제 7 호 및 동법 시행령 제 3 조).

100 16 진정 0464200, 16 진정 0585300 등 다수

나. 권고사항

- ‘전자기기를 이용한 노동감시’를 막기위해 정부부처 차원에서 어떠한 노력을 하고 있는지 밝히라.
- 2013 년 인권위가 실시한 「정보통신기기에 의한 노동인권 침해 실태조사」에 따르면, 사업장 전자감시로 인해 자신의 개인정보가 침해되어도 이를 공식적으로 문제 제기하는 경우는 응답자의 28.4%에 불과하고, 개인정보보호법에 근거한 개인정보침해 신고센터가 운영되고 있다는 사실을 아는 경우도 29.4%에 그쳤다. 2019 년 관련 인식이 개선되었는지 수치를 밝히고, 인식개선을 위한 방안을 제시하라.

다. 담당부처 및 기관

- 고용노동부
- 개인정보보호위원회

7. 사회적 약자의 프라이버시권

1) 성소수자와 프라이버시[101]

1-1) 군대 내 합의에 의한 동성 간 성적행위의 범죄화와 프라이버시권

가. 배경 및 문제점

- 군형법 제 92 조의 6[102]은 군내 남성 간 합의된 동성 성행위를 처벌하고 있으며, 국내에서 유일하게 합의된 동성 성행위를 형사처벌하는 조항임
- 많은 유엔 기구들이 위 조항의 폐지를 권고하였음[103]
- 헌법재판소에서 위 조항에 대한 위헌 심사가 지난 14 년 간 이루어졌는데, 헌법재판소는 2016 년 7 월 세 번째 위헌심사에서 구 군형법 제 92 조의 5(위 조항의 구법)을 합헌으로 결정했음.[104]
- 정부는 UPR 에서 위 조항이 성적 지향에 대한 처벌이 아닌 군대 내 기강을 확립하기 위한 것이라고 답변하며 권고 수용을 거부하였음
- 2017 년 언론은 군대 내 군형법 위반 혐의로 동성애자 군인 색출을 보도했음[105] 군 수사관들은 게이 데이트 앱이나 소셜 미디어를 이용하여 게이 군인들을 추적했음 군 수사관들은 피해자들의 휴대전화에 저장된 실시간 통신과 메시지 등 개인정보를 악용하여 동성애자로 의심되는 다른 사람의 신원을 파악하는 연쇄 수사를 벌였음
- A 대위로 알려진 한 군 장교는 기소돼 징역 6 개월에 집행유예 1 년을 선고받았음

나. 권고사항

- 합의에 의한 성적행위를 범죄화하는 군형법 제 92 조의 6 을 폐지할 것
- 군형법 제 92 조의 6 에 기초한 수사의 중단을 선언할 것

다. 담당 부처 및 기관

---

101 작성단체: 성소수자 차별반대 무지개행동

102 군형법 제 92 조의 6(추행) 제 1 조제 1 항부터 제 3 항까지에 규정된 사람에 대하여 항문성교나 그 밖의 추행을 한 사람은 2 년 이하의 징역에 처한다.

103 "위원회는 다음 사항들에 관하여 우려를 표명한다: …(b) 군대에서 남성 간 합의에 의한 동성 성관계를 처벌하는 군형법 92 조의 6…군형법 제 92 조의 6 을 폐지하고…." 유엔 인권위원회 (시민적 정치적 권리규약 위원회) 대한민국의 네번째 정기 보고서에 관한 최종 견해 (CCPR/C/KOR/CO/4, para. 14).

104 Hankyoreh, "Constitutional Court upholds military's ban on sodomy," August 8 2016. http://english.hani.co.kr/arti/english_edition/e_national/755208.html

105 CNN, "Dozens arrested as South Korean military conducts 'gay witch-hunt'," June 12, 2017. http://edition.cnn.com/2017/06/11/asia/south-korea-lgbt-military/index.html

- 국방부

1-2) 주민등록번호

가. 배경 및 문제점

- 한국인은 출생신고를 할 때 13 자리 숫자로 구성된 주민등록번호를 부여받고 있음
- 이 숫자에는 생년월일과 성별과 같은 정보가 포함되어 있음. 1900 년대에 태어난 남성의 경우 뒷자리가 1 로 시작하고, 여성의 경우 뒷자리가 2 로 시작함. 2000 년 이후에 태어난 사람들의 경우, 남성은 3, 여성은 4 로 시작함
- 주민등록번호는 만능 식별번호로 활용되고 있기 때문에, 한국인의 경우 부동산 거래부터 투표까지 모든 업무에서 신분증과 주민등록번호 공개가 요청됨
- 이와 같이 다목적으로 사용되는 주민등록번호는 엄격하고 침해적인 요건으로 인하여 법적 성별을 바꾸지 못한 트랜스젠더들에게 큰 어려움을 주고 있음
- 신분증 제시가 어렵기 때문에 구직, 휴대전화 계약, 투표 등 다양한 상황에서 포기하게 되는 것임

나. 권고사항

- 주민등록번호를 개인의 정보를 담지 않는 무작위 임의 번호 방식으로 변경할 것

다. 담당 부처 및 기관

- 행정안전부

1-3) HIV/AIDS 와 프라이버시권

가. 배경 및 문제점

- 후천성면역결핍증 예방법이 의료 관계자에 의한 HIV 프라이버시권 침해를 예방하기 위한 법률조항을 규정하고 있지만,[106] 의료 분야 또는 교도 환경에서 HIV 에 감염인의 프라이버시권이 침해되는 경우가 많음

---

106 후천성면역결핍증 예방법 제 7 조(비밀 누설 금지) 다음 각 호의 어느 하나에 해당하는 사람은 이 법 또는 이 법에 따른 명령이나 다른 법령에서 정하고 있는 경우 또는 본인의 동의가 있는 경우를 제외하고는 재직 중에는 물론 퇴직 후에도 감염인에 대하여 업무상 알게 된 비밀을 누설하여서는 아니 된다.
1. 국가 또는 지방자치단체에서 후천성면역결핍증의 예방ㆍ관리와 감염인의 보호ㆍ지원에 관한 사무에 종사하는 사람
2. 감염인의 진단ㆍ검안ㆍ진료 및 간호에 참여한 사람

- 일반적으로 회사는 노동자의 건강검진결과가 노동자에게 직접 통보되기 때문에 그 결과를 알 수 없음. 그러나 기업이 특정 의료기관을 의료진단으로 지정하는 경우, 의료 관계자가 노동자 HIV 감염여부를 기업에 유출할 수 있음. 일부 회사들는 직원들에게 건강검진결과를 직접 제출할 것을 요구하고 있음
- 3 인의 HIV 감염인이 국가인권위원회에 진정을 제기하였음. 3 명의 진정인은 2018 년경 대구교도소 수감 중 교도관들에 의한 프라이버시권 침해를 주장하였음
- 진정인들은 '특별한 환자'라고 표시된 방에 분리 수용되었음. 경비원들은 진정인들을 '특별한 환자' 또는 때로는 '에이즈'라고 큰 소리로 불렀으며, 다른 수용자들과 운동하지 못했고, 간혹 교도관들은 운동장에 선을 그어놓고 진정인들에게 넘어가지 못하게 하였음
- 후천성면역결핍증 예방법 제 19 조[107]는 HIV 감염인을 여전히 불명확한 AIDS 전파매개체로 규정화하여 범죄집단으로 규정하고 있음

나. 권고 사항

- HIV/AIDS 감염인의 프라이버시권 침해를 막기 위해 필요한 조치를 취할 것
- 후천성면역결핍증예방법 제 19 조에 따른 수사, 기소, 처벌을 중지할 것

다. 담당 부처 및 기관

- 보건복지부
- 질병관리본부

1-4) 트렌스젠더의 신체의 자율성을 보장받을 권리와 프라이버시권

가. 배경 및 문제점

- 2006 년 대법원 판결으로,[108] 인해 법원의 지침은 트랜스젠더의 성별정정 허가 심리를 위한 '조사 사항'을 규정하였음[109]
- '조사사항'이라는 말은 재량권을 내포하고 있으나, 법원은 사실상의 전제조건으로 받아들이고 있음

---

3. 감염인에 관한 기록을 유지ㆍ관리하는 사람

107 제 19 조(전파매개행위의 금지) 감염인은 혈액 또는 체액을 통하여 다른 사람에게 전파매개행위를 하여서는 아니 된다.

108 대법원 2006. 6. 22. 자 2004 스 42 결정

109 성전환자의 성별정정허가신청사건 등 사무처리지침 (출처: 성전환자의 성별정정허가신청사건 등 사무처리지침 (개정 2015. 1. 8. [가족관계등록예규 제 435 호, 시행 2015. 2. 1.]). SOGI 법정책연구회가 번역한 가이드라인의 영문 번역본은 http://annual.sogilaw.org/review/law_list_en

- 위 지침에 따르면, 신청인은 19 세 이상이어야 하고, 불임수술과 성전환 수술을 했는지 여부, 혼인 중인지 여부, 미성년 자녀가 있는지 여부 등을 밝혀야 함
- 신청인이 성인이지만 부모의 동의를 요구하는 관행이 있음
- 일부 법원은 2013 년 이후 외부 성기 수술을 요구하지 않지만, 여전히 다른 일부 법원에서 외부 성기 수술을 포함한 성전환 수술을 요구하고 있음

나. 권고사항

- 성별정정을 위해 성기 제거, 재건 수술 등 외과적 수술절차를 강제하는 것을 금지할 것

다. 담당부처 및 기관

- 대법원

2) HIV/AIDS 와 프라이버시[110]

2-1) 의료현장에서의 HIV 감염인 프라이버시 침해

가. 배경 및 문제점

- 한국에는 후천성면역결핍증 예방법에 프라이버시 침해를 막는 조항[111]이 존재함.
- 그러나 법 조항의 유무와 관계없이 의료현장에서 HIV 감염인의 프라이버시가 침해되는 상황이 빈번하게 발생되고 있음.
- 아래와 같은 상황·행위가 발생하고 있음.
  - ❍ 병원이 HIV 감염인의 동의 없이 다른 병원에 진료회신서를 보내는 행위
  - ❍ 병원이 HIV 감염인의 동의 없이 진료의뢰서 혹은 증명서 등의 서류에 HIV 감염사실을 기재하는 행위
  - ❍ 병원이 HIV 감염인의 동의 없이 가족에게 HIV 감염사실을 알리는 행위
  - ❍ 병원에서 HIV 감염인에게 아무런 고지 없이 HIV 검사를 실시하는 행위
  - ❍ 병원의 HIV 검사결과에 대한 부주의한 통보 행위

---

110 작성단체: HIV/AIDS 인권활동가 네트워크

111 후천성면역결핍증 예방법 제 7 조(비밀 누설 금지) 다음 각 호의 어느 하나에 해당하는 사람은 이 법 또는 이 법에 따른 명령이나 다른 법령에서 정하고 있는 경우 또는 본인의 동의가 있는 경우를 제외하고는 재직 중에는 물론 퇴직 후에도 감염인에 대하여 업무상 알게 된 비밀을 누설하여서는 아니 된다.

1. 국가 또는 지방자치단체에서 후천성면역결핍증의 예방·관리와 감염인의 보호·지원에 관한 사무에 종사하는 사람
2. 감염인의 진단·검안·진료 및 간호에 참여한 사람
3. 감염인에 관한 기록을 유지·관리하는 사람

❍ 병원에서 의료진이 HIV 감염인이 이용하는 물품에 별도의 표식을 달아 구분, 분리하여 다른 사람이 알게 되는 상황

[참고] 2016 국가인권위원회 HIV 감염인 의료차별 실태조사

	매우/대체로 그렇다			
	경과기간(년)			
	<5	5~9	10+	합계
검사/수술 순서 밀림	6 9.7%	15 23.8%	28 35.4%	49 24.0%
타과 진료 시 차별	10 16.4%	13 20.6%	31 38.8%	54 26.5%
간호사가 차별	7 11.3%	9 14.3%	17 21.5%	33 16.2%
방사선과나 검사실 직원의 차별	3 4.8%	4 6.3%	10 12.7%	17 8.3%
행정직원의 차별	3 4.8%	6 9.5%	11 14.1%	20 9.9%
HIV 감염인에 대해 수군거림	6 9.7%	13 20.6%	21 26.9%	40 19.7%
차트 등에 감염인 표식	8 13.1%	19 30.2%	29 37.2%	56 27.7%
다른 질병으로 병원 방문 시 감염인임 밝히기 어려움	43 69.4%	51 82.3%	60 76.9%	154 76.2%
치료를 위한 병원 방문 불편하여 대도시로 이사(희망)	18 29.0%	18 28.6%	37 46.8%	73 35.8%
내 의사 반하여 처방전 등에 HIV 명시	11 17.7%	14 22.2%	29 36.7%	54 26.5%

나. 권고사항

- 후천성면역결핍증 예방법의 제 7 조(비밀누설금지)가 실질적 효력을 발휘할 수 있도록 조치
- 의료관계자들에 대한 의무적 교육

다. 담당부처 및 기관

- 보건복지부

2-2) 구금시설 내 HIV 감염인의 프라이버시 침해[112]

가. 배경 및 문제점

- 후천성면역결핍증 예방법에 비밀 누설 금지 조항[113]이 있음에도, 구금시설 내에서 HIV 감염인의 감염사실이 타인에게 동의 없이 알려지는 상황이 빈번함. 또한 교도소 수감 중의 일체의 활동에서 HIV 감염을 이유로 분리, 배제, 차별 행위를 한 것은 「헌법」 제 10 조의 인간존엄과 가치, 행복추구권 및 「헌법」 제 11 조 평등권을 침해하고, 「국가인권위원회법」 및 「형의 집행 및 수용자의 처우에 관한 법률」에서 금지하고 있는 병력(病歷)을 이유로 한 명백한 차별행위임.
- 구금시설 내 HIV 감염인들이 기거하는 방에 특이환자라는 표식을 해두어 감염사실이 노출될 수밖에 없게 되는 상황(예: 거실 출입문에 특이환자라고 크게 표기해 놓아 감염사실이 노출됨)
- 운동 시간을 별도로 배정하고, 함께 운동을 하는 경우에도 운동장에 선을 그어 분리·배제하는 행위
- 일체의 취미활동, 교정 프로그램 참여에 대해 배제하는 행위
- HIV 감염 수용인을 감염사실이 이미 알려진 수용인과 같이 거주하게 배정하며 격리 수용시키는 행위
- 호명할 때 큰소리로 특이환자라고 호명하는 행위
- 다른 수용인들이 알게 될 수 있는 상황에서 HIV 병명을 언급하여 감염사실이 알려지게 되는 상황(예: 통로에 세워두고 병명을 말함 / 보안검사 도중 교도관끼리 '에이즈 방이니 들어가지 말라'는 얘기를 함 / 교도관이 동료수용인들이 보는 앞에서 HIV 라는 표식이 되어있는 박스에서 손톱깎기를 꺼내 전달하게 함)
- HIV 감염 수용인과의 접촉에서만 마스크 등을 사용하는 행위

---

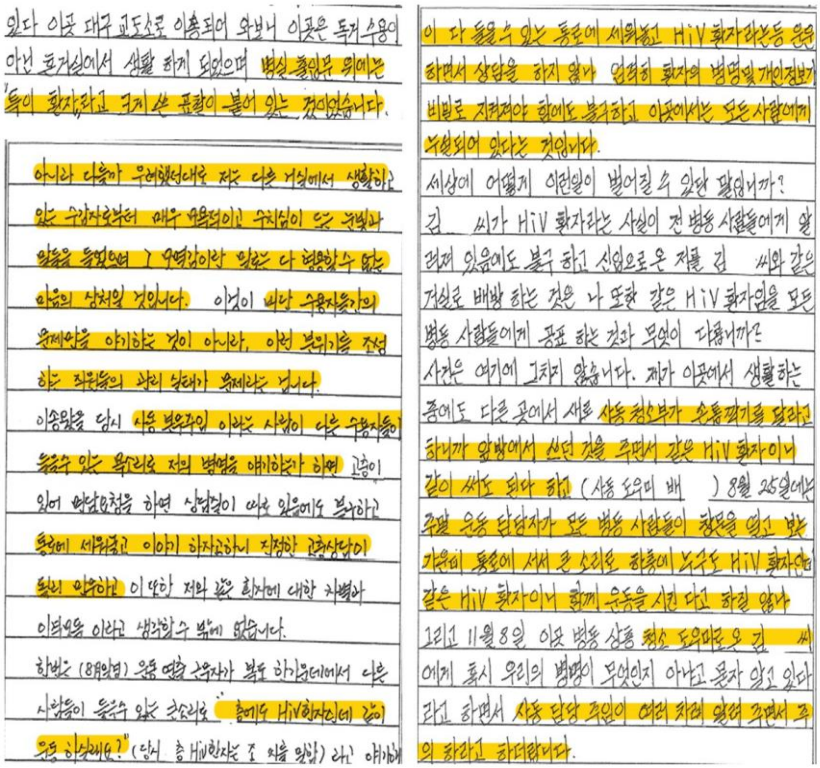
112 본 내용은 피해당사자 2 명과 인권단체 2 곳이 국가인권위원회에 진정을 제기한 상황

113 제 7 조(비밀 누설 금지) 다음 각 호의 어느 하나에 해당하는 사람은 이 법 또는 이 법에 따른 명령이나 다른 법령에서 정하고 있는 경우 또는 본인의 동의가 있는 경우를 제외하고는 재직 중에는 물론 퇴직 후에도 감염인에 대하여 업무상 알게 된 비밀을 누설하여서는 아니 된다.

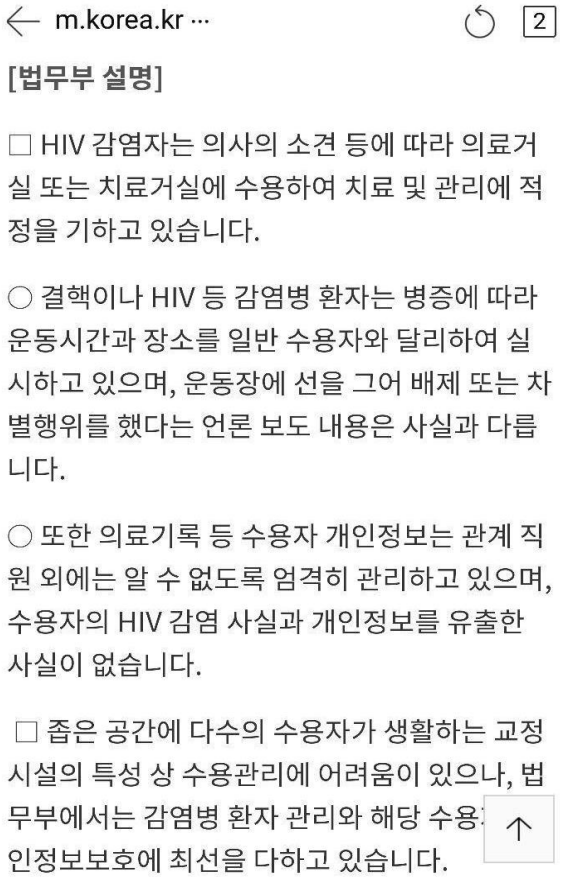
1. 국가 또는 지방자치단체에서 후천성면역결핍증의 예방·관리와 감염인의 보호·지원에 관한 사무에 종사하는 사람
2. 감염인의 진단·검안·진료 및 간호에 참여한 사람
3. 감염인에 관한 기록을 유지·관리하는 사람

- 교정 행정 시스템 '보람이'를 통해 HIV 감염사실이 광범위하게 노출된 상황
- 법무부 및 교정본부가 민원 서신의 답변공문에 실명으로 감염인이라고 명기하여 감염사실을 노출한 행위

[참고] 대구교도소 수감 중인 HIV 감염인의 피해사실이 담긴 서신



[참고] 2019.02.15 법무부의 정책브리핑(인권침해 사실을 부정하는 내용으로 이는 당사자 조사 한번 없이 대구교도소의 답변만을 근거로 발표한 것임)



나. 권고사항

- 입소·수용 생활 중 동의되지 않은 HIV 강제검사 중지
  - 수용자의료관리지침 제 3 조(신입자 건강진단의 실시) 5 항은 '모든 신입 수용자에 대해 신속히 관할 보건소 또는 검사 전문기관에 의뢰하여 매독 및 후천성면역결핍증검사를 실시'하도록 규정하고 있음. 이 과정에서 수용자에게 HIV 검진사실조차 고지되지 않고 있는 상황. 본인의 동의 없이 채혈을 하거나 검사를 하는 것 자체가 인권침해이기 때문에 이러한 행위가 시도조차 되어서는 안 됨.
- 미흡한 비밀 보장 규정(의료정보시스템 & 보람이 시스템) 개선
  - 교도 행정 시스템의 환자 정보 유지·기록·관리에 대한 구체적인 가이드라인 및 지침상의 비밀누설금지 규정의 부재. 의료정보시스템이 교정정보시스템(보람이 시스템)과 연동되어 있으며, 타 구금시설에서도 개인 수용자의 병력 정보를 조회할 수 있어서, 광범위하게 HIV 감염 수용자의 병력정보가 노출되고 있음.

- 감염인 건강권 제한 금지
  - 수용자의료관리지침 제 20 조(이송대상 혈액투석환자)는 에이즈 감염 등 감염병에 이환되지 않은 자만이 혈액 투석을 받을 수 있도록 하여 HIV 감염 수용인의 의료접근성을 제한하고 있음. 그러나 혈액투석이 필요한 HIV 감염 수용인에 대한 의료 접근 제한 조치는 의학적으로 근거가 없으며, 질병관리본부와 대한병원감염관리학회가 발간한「투석실에서의 감염관리 표준지침」(2010)에 의하면 "혈액매개감염검사에 있어 투석환자들이 HIV 검사를 정기적으로 할 필요가 없으며, HIV 예방과 관리를 위해 HIV 에 감염된 환자를 다른 환자들로부터 격리하거나 투석기계를 분리하거나 담당 의료인을 구분하지 않아도 된다. 또한 투석기를 재사용해도 된다." 라고 규정하고 있음.
- 당사자 감염인의 요구수렴을 위한 재발방지 시스템 도입
  - 처우개선 요청에 조사도 없이 응대를 하는 바람에 "대구교도소는 물론이고 교정본부 및 대구교정청에 수용자들이 아무리 진정을 하고 청원을 해도 묵살해 버리고 들은 채도 않기 때문에" 심리적 고통이 극심하며 이를 아래와 같이 개탄하고 있음. "어떻게 수용자의 진정내용을 현장조사 한 번 없이 대구교도소 직원들의 허위 보고만을 믿고 고통 속에 시달리며 생활하고 있다는 수용자의 진정을 묵살하고 있는지 개탄하지 않을 수 없습니다."
- HIV 감염인 인권침해 재발방지를 위한 법무부 산하 교정청 교도관 대상 교육 실시
- 법무부 소속 전국 교정청에 수감 중인 HIV 감염인 인권침해 상황 전수조사
- 구금시설 내 HIV 감염 수용인의 건강 및 인권/프라이버시 보장을 위한 지침 마련

다. 담당 부처 및 기관

- 법무부

2-3) 청소년 HIV 감염인의 프라이버시

가. 배경 및 문제점

- 청소년 HIV 감염인의 수가 늘어나고 있는 데에 비해, 청소년 HIV 감염인의 심리적 안정, 인권 등을 보장하기 위한 법제도적 장치가 없는 상황임.
- 청소년의 HIV 감염사실이 당사자의 동의 없이 법[114]에 의해 가족 등의 법정대리인에게 통보될 수 있는 상황

114 후천성면역결핍증 예방법 제 8 조의 2(검진 결과의 통보) ① 후천성면역결핍증에 관한 검진을 한 자는 검진 대상자 본인 외의 사람에게 검진 결과를 통보할 수 없다. 다만, 검진 대상자가 군(軍), 교정시설 등 공동생활자인 경우에는 해당 기관의 장에게 통보하고, 미성년자, 심신미약자, 심신상실자인 경우에는 그 법정대리인에게 통보한다.

나. 권고사항

- HIV 감염인의 인권 및 에이즈에 대한 올바르고 정확한 정보가 포함된 포괄적 성교육 실시
- 청소년의 HIV 감염사실을 당사자의 동의 없이 법정대리인에게 통보하게 하는 법조항 폐지
- 청소년 HIV 감염인의 실질적 인권보장을 위해 국가적 지원체계 마련

다. 담당부처 및 기관

- 보건복지부
- 여성가족부

2-4) HIV 감염인의 노동현장에서의 프라이버시

가. 배경 및 문제점

- 후천성면역결핍증 예방법 제 8 조의 2 3 항[115]의 내용과는 달리 노동현장에서 HIV 감염사실이 알려질 수 있는 상황이 빈번함.
- 취업 시 채용검진에 HIV 검진가 강제로 포함되어 있는 상황
- 취업 후 정기적인 직장 내 건강검진 항목에 HIV 검진이 강제로 포함되어 있는 상황

나. 권고사항

- 노동권의 침해를 막기 위해 법(제 8 조의 2 3 항)이 제대로 효력을 발휘할 수 있도록 조치
- 채용검진 및 직장 내 건강검진에서 HIV 검진을 강제로 하지 않도록 제도적 장치 마련

다. 담당 부처 및 기관

- 고용노동부
- 보건복지부

115 후천성면역결핍증 예방법 제 8 조의 2(검진 결과의 통보) ① 후천성면역결핍증에 관한 검진을 한 자는 검진 대상자 본인 외의 사람에게 검진 결과를 통보할 수 없다. 다만, 검진 대상자가 군(軍), 교정시설 등 공동생활자인 경우에는 해당 기관의 장에게 통보하고, 미성년자, 심신미약자, 심신상실자인 경우에는 그 법정대리인에게 통보한다.
② 제 1 항에 따른 검진 결과 통보의 경우 감염인으로 판정을 받은 사람에게는 면접통보 등 검진 결과의 비밀이 유지될 수 있는 방법으로 하여야 한다.
③ 사업주는 근로자에게 후천성면역결핍증에 관한 검진결과서를 제출하도록 요구할 수 없다.

2-5) HIV 감염 군인 및 준군인의 프라이버시

가. 배경 및 문제점

- 군인 및 준군인 등 군 관계자가 HIV 감염인일 경우에는 기관의 장에게 통보가 됨[116]. 또한 군 내에서 HIV 감염사실이 동의 없이 다른 이들에게 알려지는 상황이 발생하고 있음. HIV 감염인은 군면제에 해당되기에 대부분의 상황은 군입대 후 HIV 감염사실을 알게 되었을 때 발생하게 됨.
- 군에서 HIV 감염사실이 동의 없이 다른 이들에게 알려지는 상황
- HIV/AIDS 에 대해 공포스러운 분위기를 조성하며 배제하는 분위기의 형성(예: 머무른 곳을 락스로 청소하라고 명령하는 등)

나. 권고사항

- 질병관리본부가 홍보하고 있는 것과 같이, 공동생활에서 감염될 우려가 없으므로 통보조항 폐지
- 올바르고 정확한 HIV/AIDS 의 정보와 HIV 감염인의 인권에 대해 관련자들을 교육

다. 담당부처 및 기관

- 국방부
- 병무청
- 경찰청

2-6) 국가에 의한 HIV 감염인의 사적영역(성행위) 통제 및 개입

가. 배경 및 내용

- 후천성면역결핍증예방법 상 19 조 전파매개행위금지조항은 HIV 감염인의 '콘돔없는 성행위'를 처벌하고 있음. U=U 캠페인으로 꾸준한 치료를 받는 HIV 감염인의 전파가능성이 0%라는 것이 입증된 지금, 19 조 전파매개행위금지조항은 HIV 감염인이 '콘돔없는 성행위'를 했다면, 상대방에게 감염사실을 미리 알리고 사전에 동의를 구했어도, 성행위 결과 상대방이 HIV 에 감염되지 않았다 하더라도 HIV 감염인을 형사처벌하고 있음. 이는 명백한 국가에 의한 사생활 침해임.

---

116 후천성면역결핍증 예방법 제 8 조의 2(검진 결과의 통보) ① 후천성면역결핍증에 관한 검진을 한 자는 검진 대상자 본인 외의 사람에게 검진 결과를 통보할 수 없다. 다만, 검진 대상자가 군(軍), 교정시설 등 공동생활자인 경우에는 해당 기관의 장에게 통보하고, 미성년자, 심신미약자, 심신상실자인 경우에는 그 법정대리인에게 통보한다.

나. 권고사항

- 후천성면역결핍증예방법 상 19 조 전파매개행위금지조항 폐지.

다. 담당 부처 및 기관

- 법무부

3) 북한이탈주민의 프라이버시권 침해[117]

가. 배경 및 문제점

- 2016. 4. 중국의 북한식당에서 근무하던 종업원 12 명과 지배인 1 명이 집단 입국하였고, 입국 직후 통일부의 긴급브리핑으로 입국 사실이 공개됨.
- 북한이탈주민이 대한민국에 입국하는 경우, 당사자의 신원, 입국 사실 및 입국 경위에 대하여 공개하지 않고, 국가정보원에서 조사를 진행하고 이후 보호 및 정착지원을 결정하면 통일부에서 보호 및 지원 내용을 결정함.
- 그러나 2016. 4. 입국한 종업원들에 대해서는 입국 직후 입국사실을 공개하였고, 당사자들이 북한이탈주민보호센터에 들어가는 모습을 촬영한 사진을 언론을 통해 공개함. 촬영자의 신원은 알 수 없으나, 당시 종업원을 촬영한 사진이 언론에 보도되도록 하였고 현재까지도 관련 기사에 인용되고 있음. (첨부 1 사진)
- 해당 종업원들은 사진이 언론에 공개될 것이라는 사실을 전혀 알지 못하였고, 어떤 경위로 자신들을 촬영한 사진이 보도되었는지 알지 못하고 있음. 해당 종업원들을 아는 사람이라면 사진을 통해 신원을 구별할 수 있을 정도이고 실제 종업원들이 관련 질문을 받기도 함.
- 북한이탈주민보호센터를 국가정보원이 운영, 관리하고 있는데 관계법령상 북한이탈주민에 대한 조사의 권한만 있고 원칙적으로 북한이탈주민의 보호 및 정착지원업무는 통일부의 소관임. 그럼에도 불구하고 북한이탈주민의 신원 확인 및 조사에 관한 권한을 국가정보원이 광범위하게 보유하면서 자의적으로 북한이탈주민에 관한 정보의 공개여부 및 그 내용을 결정하고 있음(첨부 2 관련 법령).
- 북한이탈주민을 보호하고 정착을 지원하겠다는 법과 제도의 목적과 달리, 국가정보원이 북한이탈주민보호센터를 운영, 관리하면서 북한이탈주민의 신상정보를 수집하고 이를 활용하는 과정을 통제하기 어려움. 또한 국가정보원장이 보호여부를 결정하는 '국가안전보장에 현저한 영향을 줄 우려가 있는 사람'에 대한 판단기준이 모호하여 누가 국가정보원의 관리대상이 될 것인지 예측하기 어렵고 이 또한 국가정보원의 판단에 맡겨져 있음. 위 종업원들의 경우, 중국 소재 북한식당에서 근무한 이력이 '국가안전보장에 현저한

117 작성단체: 민주 사회를 위한 변호사 모임

영향을 줄 우려가 있는 경우’라고 보기 어려움에도 불구하고, 국가정보원이 해당 종업원들을 북한이탈주민보호센터에서 계속 관리함.

나. 권고사항

- 국가정보원이 북한이탈주민보호센터를 운영, 관리하면서, 구체적인 기준 없이 북한이탈주민에 대한 조사를 실시하고 관련 정보를 수집, 관리하는 것은 적절하지 아니함. 북한이탈주민의 신상정보를 포함한 관련 정보에 대한 일률적인 관리 체계를 마련하고, 이를 북한이탈주민의 보호 및 정착지원 업무의 소관부처인 통일부에서 담당하도록 할 필요가 있음.

다. 담당 부처 및 기관

- 국가정보원
- 통일부

[첨부 1] 언론에 보도된 입국 당시 사진

[첨부 2] 관계 법령

북한이탈주민의 보호 및 정착지원에 관한 법률
제 10 조(정착지원시설의 설치)

① 통일부장관은 보호대상자에 대한 보호 및 정착지원을 위하여 정착지원시설을 설치·운영한다. 다만, 제 8 조제 1 항 단서에 따라 국가정보원장이 보호하기로 결정한 사람을 위하여는 국가정보원장이 별도의 정착지원시설을 설치·운영할 수 있다.

제 8 조(보호 결정 등)
① 통일부장관은 제 7 조제 3 항에 따른 통보를 받으면 협의회의 심의를 거쳐 보호 여부를 결정한다. 다만, 국가안전보장에 현저한 영향을 줄 우려가 있는 사람에 대하여는 국가정보원장이 그 보호 여부를 결정하고, 그 결과를 지체 없이 통일부장관과 보호신청자에게 통보하거나 알려야 한다.

제 7 조(보호신청 등) ① 북한이탈주민으로서 이 법에 따른 보호를 받으려는 사람은 재외공관이나 그 밖의 행정기관의 장(각급 군부대의 장을 포함한다. 이하 "재외공관장등"이라 한다)에게 보호를 직접 신청하여야 한다. 다만, 보호를 직접 신청하지 아니할 수 있는 대통령령으로 정하는 사유가 있는 경우에는 그러하지 아니하다.
② 제 1 항 본문에 따른 보호신청을 받은 재외공관장등은 지체 없이 그 사실을 소속 중앙행정기관의 장을 거쳐 통일부장관과 국가정보원장에게 통보하여야 한다.
③ 제 2 항에 따라 통보를 받은 국가정보원장은 임시 보호나 그 밖의 필요한 조치를 한 후 지체 없이 그 결과를 통일부장관에게 통보하여야 한다.

북한이탈주민의 보호 및 정착지원에 관한 법률 시행령
제 12 조 (임시 보호 등의 내용) ① 법 제 7 조제 3 항에 따른 임시보호나 그 밖의 필요한 조치는 보호신청 이후 보호신청자에 대한 일시적인 신변안전 조치와 보호 여부 결정 등을 위한 필요한 조사로 한다.
② 국내에 입국한 보호신청자에 대한 제 1 항에 따른 일시적인 신변안전 조치와 조사의 기간은 해당 보호신청자가 국내에 입국한 날부터 90 일을 초과할 수 없다. 다만, 입국 인원 증가 등 불가피한 사유가 있는 경우에는 협의회의 심의를 거쳐 그 기간을 1 회에 한정하여 30 일의 범위에서 연장할 수 있다.
③ 제 1 항에 따른 임시 보호나 그 밖의 필요한 조치의 내용·방법과 필요한 조치를 위한 시설의 설치·운영 등에 대해서는 국가정보원장이 정한다.

4) 외국인 피의자의 프라이버시권 침해[118]

가. 배경 및 문제점

118 작성단체: 민주 사회를 위한 변호사 모임

- 2018. 10. 7. 경기 고양시 화전동 대한송유관공사 경인지사의 옥외 휘발유 탱크 14 기 중 하나가 폭발하는 화재사고가 발생하였음(이하 '고양저유소 화재'라 함). 고양저유소 화재는 매우 큰 화재였고, 휘발유 화재였기 때문에 진화에 난항을 겪었음. 경찰은 화재 몇 시간 전 외국인노동자가 날린 풍등을 고양저유소 화재의 원인으로 지목하였고, 2018. 10. 8. 외국인노동자 A 를 긴급체포하였음. 경찰은 A 를 긴급체포하자마자 언론에게 A 의 실명, 국적, 나이, 직업, 수입, 검거장소 등을 알려주었음.
- 고양저유소 화재는 언론의 큰 관심을 받는 사건이었기 때문에 많은 언론 보도가 되었음. 언론들은 관련 기사에서 A 의 국적을 중요하게 다루었고, "OOOO 인"이라는 표현이 지속적으로 사용하였음. 어떤 언론은 스리랑카인의 나이와 일터, 거주지 등 신상정보를 자세히 보도하기도 했으며, 심지어 A 의 얼굴을 공개한 언론도 있었음. 경찰은 이후에도 언론에게 A 의 진술과 수사내용을 공개하였고, 이는 실시간으로 보도되었음.
- 경찰의 문제점
  - '인권보호를 위한 수사공보준칙(법무부훈령 제 761 호)'에 의하면, 수사사건을 공보함에 있어서는 목적 달성에 필요한 최소한의 사항만을 정확하게 공개하여야 하고 사건관계인의 명예 등 인권을 침해하거나 수사에 지장을 주지 아니하도록 유의하여야 함(제 13 조). 따라서 공소제기 전 수사사건에 대한 혐의사실 및 수사상황 등 수사관련 내용 일체를 원칙적으로 공개하지 못하며(제 9 조), 부득이하게 사건관계인을 공개하는 경우 익명사용을 원칙으로 하고, 사건 관계인의 인격 및 사생활, 범죄 전력, 진술 내용, 증거 관계 등도 특별한 사정이 없는 한 공개를 금지하고 있음(제 19 조). 또한 합리적 이유 없이 성별, 종교, 나이, 장애, 사회적 신분, 출신지역, 인종, 국적, 정치적 의견 등을 이유로 한 차별을 금지하고 있음(제 6 조).
  - 경찰은 수사사건의 내용을 공개할 수 있는 예외적 사유에 해당하지 않음에도, 고양저유소 화재 사건의 수사 내용을 공개하였으며, A 의 실명, 실명, 국적, 나이, 직업, 수입, 검거장소 등을 공개하였음. 경찰의 공개 행위는 인권보호를 위한 수사공보준칙위반이며, A 의 개인정보자기결정권을 침해한 행위임.
  - 특히 경찰은 A 의 국적과 외국인노동자라는 신분을 강조하였고, 언론 역시 이를 강조하여 보도하였음. 이는 출신지역, 인정, 국적, 사회적 신분을 이유로 한 차별임.
  - 국가인권위원회는 2019. 5. 17. 경찰이 A 의 사생활을 침해하였음을 인정하는 내용의 결정을 하였음.
- 언론의 문제점
  - 언론은 경찰이 공개한 A 의 신상정보를 무분별하게 보도하여 A 의 개인정보자기결정권을 침해하였음.
  - 국가인권위원회와 한국기자협회가 공동으로 작성한 인권보도준칙에 의하면, 언론은 고정관념이나 사회적 편견 등에 의한 인권침해를 방지하기 위해 용어 선택과 표현에 주의를 기울여야 함(인권보도준칙 총강 6 항). 또한 언론은 이주민에 대해 희박한 근거나 부정확한 추측으로 부정적인 이미지를 조장하거나 차별하지 않아야 함(인권보도준칙 분야별 요강 5 장). 하지만 언론은 A 의 국적과 외국인노동자라는

신분을 집중적으로 보도하였음. 단적인 예로, A 가 날린 풍등은 전날 B 초등학교의 행사에서 사용된 풍등이었는데, B 초등학교의 이름은 거의 보도되지 않았지만, A 의 국적은 1000 번이 넘게 보도되었음. 결국 언론은 고양저유소화재와 관련 없는 A 의 국적과 외국인노동자라는 신분을 집중적으로 보도함으로 인해, 이주민에 대한 부정적인 이미지를 조장하였음.

나. 권고사항

- 경찰은 인권보호를 위한 수사공보준칙을 준수해야 함. 또한 수사공보준칙을 위반한 공보에 대해 제지를 가할 수 있는 실질적인 방법을 모색할 필요가 있음.
- 언론이 인권보도준칙을 엄격하게 준수하도록 강제하는 방법을 모색할 필요가 있음.

다. 담당 부처 및 기관

- 경찰,언론중재위원회

5) 아동의 프라이버시권 침해[119]

5-1) 생활기록부와 나이스(NEIS)

가. 배경 및 문제점

- 학생에 대해 의무적으로 작성하게 되는 학생생활기록부에 담기는 내용이 과도하기 때문에 학생의 세밀한 개인정보까지 수집되어 기록되고 있음
  1. 인적사항 – 본인의 성명, 성별, 주민등록번호, 주소 / 가족의 성명, 생년월일 / 특기사항
  2. 학적사항 – 언제 어느 학교를 졸업하고, 언제 어느 학교에 입학했는지
  3. 출결상황 – 수업일수, 결석일수, 지각, 조퇴, 결과 (질병/무단/기타)
  4. 수상경력
  5. 자격증 및 인증 취득상황 – 자격증 및 인증 취득상황, 국가직무능력표준 이수사항
  6. 진로희망사항
  7. 창의적 체험활동상황 – 자율활동, 봉사활동, 동아리활동, 진로활동, 자치활동, 특별활동 등
  8. 교과학습발달상황 – 내신 등급(성적) / 과목별 세부능력특기사항
  9. 독서활동상황(2016 년까지는 책 제목과 간단한 감상을, 2017 년부터는 책 제목만 적음)
  10. 행동특성 및 종합의견(각 학년 담임의 의견)
- 이러한 학생생활기록부에 담기는 내용은 학생의 별도의 동의절차 없이 수집되고 기록됨. 입력과정에 학생이 관여할 수 있는 제도적인 통로는 존재하지 않음

119 작성단체: 청소년인권행동 아수나로

- 이렇게 만들어진 학생생활기록부는 NEIS 라는 온라인 교육정보시스템에 저장되는데, 그 결과 정부가 모든 학생들의 개인정보를 동의절차 없이 일괄적으로 수집하는 것이 됨. 또한 NEIS 에 저장된 학생정보는 학생의 의사에 반하더라도 학부모 또는 관리자 등이 열람이 가능함.
- NEIS 에 저장된 학생생활기록부는 반영구적으로 보존됨. 동의절차를 거치지 않고 수집한 학생의 개인정보를 폐기 기한을 정하지 않은 채 국가가 보관하고 있는 것임

나. 권고사항

- 생활기록부 작성을 위해 수집하는 정보의 범위를 축소할 필요가 있음
- 생활기록부 내용에 대한 이의 신청, 대처 절차 등을 마련하는 등 생활기록부 작성 과정에 대해 학생이 제도적으로 참여할 수 있는 방안이 마련되어야 함
- 학생의 의사에 반하는 NEIS 개인정보 수집 및 학부모 등 제 3 자의 열람을 제한할 수 있는 절차가 마련되어야 함
- 학생의 의사에 따라 NEIS 에 수집된 개인정보가 폐기될 수 있는 절차가 마련되어야 함

다. 담당 부처 및 기관

- 교육부

5-2) 학교의 학생생활규정이나 관습적으로 이루어지는 개인정보 침해

가. 배경 및 문제점

- 학교 내 생활규정, 관행 등으로 명찰 부착, 소지품 검사, 일기장 검사가 이루어지고 있음
- 많은 학교에서는 학교생활규정으로 교복에 고정명찰을 부착하도록 하고 학교에 등하교할때 교복을 입도록 함. 이에 따라 재학중인 학교, 학년, 이름이라는 정보가 원하지 않더라도 등하교 과정에서 불특정다수에게 공개되게 됨. 2010 년 인권위에서 인권침해라는 지적을 받으며 잠시 감소했지만 최근 다시 학교 차원에서 고정명찰을 유도하며 다시 증가하는 추세
- 2016 년 인권위에서 실시한 '학교생활에서 학생의 인권보장 실태조사'에 의하면 실태조사에 참여한 학생의 17.6%가 사전 동의 없는 소지품 검사를 당했다고 응답 -> 학생인권조례가 제정되어 있는 곳에서는 금지되어 있지만 제정되어 있지 않은 곳에서는 학생생활규정이나 관행에 따라 이루어지는 경우가 많다
- 강제로 일기를 쓰게 하고, 일기장 검사를 하는 관행이 초등학교 내에서는 강하게 남아 있음. 2008 년부터 인권위에서는 이를 두고 인권침해라는 결론을 도출하였지만 잘 개선되지 않고 있음

나. 권고사항

- 소지품 검사 금지, 일기장 검사 금지, 부착용 명찰 금지 등 아동의 프라이버시권을 보호하기 위한 내용이 실효성 있는 기본 법률로 규정될 필요가 있음
- 학생들의 생활에 대한 규정을 제·개정할 때 학생들이 참여할 수 있는 절차적 권리가 보장되어야 하고, 참여가 배제된 경우 이의를 제기할 수 있는 절차 또한 마련되어야 함

다. 담당 부처 및 기관

- 교육부

5-3) 어린이집 CCTV

가. 배경 및 문제점

- 2015 년 4 월, 어린이집 CCTV 의무화를 포함한 영유아보육법이 국회를 통과하였음
- 아동과 어린이집 직원의 모든 행동이 촬영됨에 따라 아동과 교사의 일상생활 전반이 기록되어 아동의 사생활을 침해하는 결과로 나타남
- 아동 학대 관련 언론 보도에 수집된 CCTV 영상이 목적 외로 활용되는 경우, 아동의 사생활 침해가 광범위하게 발생할 우려가 있음
- 어린이집 아동학대 건수와 전체 아동학대 사건에서 어린이집 아동학대 사건 비중은 증가하고 있기 때문에 (보건복지부 전국아동학대현황보고서) CCTV 설치 의무화 조치와가 필수불가결의 조치인지 불분명함
- 더불어 부모와 교사의 동의 아래 CCTV 설치를 하지 않은 경우에도 부모의 어린이집 참여권 증진 등을 통해 아동의 사생활을 침해하지 않는 방식으로 아동의 안전을 확보할 수 있음

나. 권고사항

- 어린이집 CCTV 설치 의무를 폐지할 필요가 있음
- 보육교사 처우 향상, 아동 당사자 의사에 부합하고, 프라이버시권이 확보될 수 있는 보육환경 개선 대책을 강구할 필요가 있음

다. 담당 부처 및 기관

- 행정안전부
- 교육부

5-4) 성에 관한 프라이버시 침해

가. 배경 및 문제점

- 아수나로에서 2010 년 9~11 월에 진행한 '사랑은 19 금이 아니야 - 청소년 연애탄압조사'에 따르면 서울 관악구의 중학교, 고등학교 중 81.3%, 경기도 화성시 중학교, 고등학교 중 86.7%의 학교가 학칙에 "불건전한 이성교제", "남녀간의 파렴치한 행위", 이성간 혹은 동성간의 연락, 관심표현, 만남, 이성간 혹은 동성간의 신체접촉, 혼숙, 성관계 자체를 처벌하는 조항을 두고 있었음. 이처럼 학생의 성적 사생활을 침해하는 연애탄압규정은 여전히 많은 중,고등학교에 존재하고 있음
- 나아가 학교에서 학생 성소수자를 색출하려는 시도가 보고된 바도 있음

나. 권고사항

- 학생의 성적자기결정권 행사에 학교가 관여하는 것과, 성적지향 및 성별정체성에 따른 차별을 실효성 있게 금지할 수 있는 기본법의 제정이 필요함
- 학생들의 생활에 대한 규정을 제·개정하는 경우, 학생들의 동의를 받고, 학생들이 실질적으로 참여할 수 있는 절차가 마련되어야 함

다. 담당 부처 및 기관

- 교육부

5-5) 만 14 세 미만의 개인정보 자기결정권

가. 배경 및 문제점

- 개인정보보호법 제 22 조 제 6 항은 개인정보처리자가 만 14 세 미만 아동의 개인정보를 법정대리인의 동의를 받아 처리할 수 있도록 하고 있음
- 그리고 위 조항과 같은 법 시행령 제 17 조 제 4 항은 개인정보처리자가 법정대리인의 동의를 받지 않고, 아동에게 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있도록 하고 있음
- 위 조항들로 인하여, 만 14 세 미만의 아동은 자신의 의사와는 관계없이 자신의 정보의 처리여부가 결정되고 있음
- 가령 조선대학교가 2017 년경 정부 예산을 지원받아 진행하기로 결정한 청소년 범죄와 유전자 연관성에 관한 연구는 국내 중학교 학생 800 명의 구강상피세포 등 생체, 유전정보를 수집하고, 5 년 간 해당 학생들의 발달과정을 추적하는 등 대상 학생들의 프라이버시권을 현저하게 침해할 우려가 존재함. 그럼에도 불구하고 조선대학교는 학생들의 의사와는 관계없이 법정대리인의 동의만을 받아 연구를 진행하고자 하였음. 이에

시민단체들은 국가인권위원회에 위 연구가 아동의 프라이버시권 등을 침해한다는 내용의 진정을 제기하였음

나. 권고사항

- 만 14 세 미만의 아동의 개인정보 자기결정권을 보장하기 위해 법정대리인의 동의와 함께 아동의 의사를 확인할 수 있는 절차를 마련해야 함. 개인정보처리에 관한 설명 및 의사 확인 방식은 아동의 연령과 발달 정도가 고려되어야 함
- 아동의 의사를 확인할 수 없는 경우, 법정대리인의 동의권 행사가 아동의 의사가 반하는지 여부를 아동의 최상의 이익 원칙에 따라 판단할 수 있는 절차가 필요함

다. 담당 부서/기관

- 행정안전부

5-6) 청소년 스마트폰 감시법과 스마트폰 감시앱[120]

가. 배경 및 문제점

- 2015 년 4 월 16 일부터 시행된 전기통신사업법 제 32 조의 7[121]은 이통사가 청소년과 전기통신서비스 제공에 관한 계약을 체결하는 경우 청소년유해매체물 및 음란정보에 대한 차단수단을 제공하여야 한다고 하고 있으며, 동 법 시행령 제 37 조의 8[122]는 이통사가 계약 체결 시 차단수단의 종류와 내용 등을 고지하고 차단수단을 설치하도록 강제하고 있고,

---

120 작성단체: 오픈넷

121 제 32 조의 7(청소년유해매체물 등의 차단) ① 「전파법」에 따라 할당받은 주파수를 사용하는 전기통신사업자는 「청소년 보호법」에 따른 청소년과 전기통신서비스 제공에 관한 계약을 체결하는 경우 「청소년 보호법」 제 2 조제 3 호에 따른 청소년유해매체물 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 44 조의 7 제 1 항제 1 호에 따른 음란정보에 대한 차단수단을 제공하여야 한다.

122 제 37 조의 8(청소년유해매체물등의 차단수단 제공 방법 및 절차) ① 법 제 32 조의 7 제 1 항에 따라 「청소년 보호법」에 따른 청소년과 전기통신서비스 제공에 관한 계약을 체결하는 전기통신사업자는 해당 청소년이 전기통신서비스를 통하여 「청소년 보호법」 제 2 조제 3 호에 따른 청소년유해매체물 및 불법음란정보(이하 "청소년유해매체물등"이라 한다)에 접속하는 것을 차단하기 위하여 해당 청소년의 이동통신단말장치에 청소년유해매체물등을 차단하는 소프트웨어 등의 차단수단을 제공하여야 한다.
② 제 1 항에 따라 차단수단을 제공하는 경우에는 다음 각 호의 절차에 따른다.
1. 계약 체결 시
가. 청소년 및 법정대리인에 대한 차단수단의 종류와 내용 등의 고지
나. 차단수단의 설치 여부 확인
2. 계약 체결 후: 차단수단이 삭제되거나 차단수단이 15 일 이상 작동하지 아니할 경우 매월 법정대리인에 대한 그 사실의 통지

계약 체결 후에는 차단수단이 삭제되거나 차단수단이 15 일 이상 작동하지 아니할 경우 법정대리인에게 통지하도록 하고 있음

- 차단수단이라 함은 스마트폰 애플리케이션을 말하는데, 현재 시중에 나와 있는 차단 앱 중 다수는 유해정보 차단을 넘어 스마트폰 사용 모니터링, 위치 조회 등 청소년의 사생활을 과도하게 침해하고 개인정보를 수집하는 기능들을 갖추고 있음
  - ❍ 이렇게 감시 내지 모니터링 기능을 갖춘 앱은 보안이 취약한 경우가 많아 해커들의 표적이 되며, 청소년을 개인정보 유출, 해킹 등의 보안 위험에 노출시킴. 특히 정부가 개발, 보급한 "스마트보안관"은 무려 26 건의 보안 취약점을 갖고 있음이 시티즌랩의 보고서에 의해 밝혀져 큰 파장을 불러일으켰음. 또한 3 대 이통사인 KT 와 LGU+가 무상으로 제공하고 있는 차단수단도 보안에 매우 취약한 것으로 밝혀짐
- 청소년 스마트폰 감시법은 이통사가 청소년의 스마트폰에 차단수단을 의무적으로 설치하고 청소년이 어떤 정보를 검색하고 접근하는지를 상시 감시하게 하여 스마트폰을 사용하는 청소년의 사생활의 비밀과 자유를 침해하고, 청소년과 법정대리인의 개인정보를 수집, 보관, 이용하기 때문에 개인정보자기결정권도 침해함. 또한 차단수단에 의해 유해정보뿐만 아니라 합법적이고 교육적인 정보도 차단되어 청소년의 알 권리를 침해하며, 차단수단 설치 여부에 대해 청소년 및 법정대리인의 선택권을 인정하지 않아 부모의 자녀교육권을 침해함
- 오픈넷은 청소년 및 청소년의 법정대리인(부모)을 대리해 2016 년 8 월 청소년 스마트폰감시법에 대해 헌법소원을 청구하여 현재 심리중
- 청소년 스마트폰 감시법은 유해정보로부터 청소년을 보호하자는 좋은 취지로 도입되었으나, 이통사가 청소년이나 부모의 의사와 상관없이 차단수단을 의무적으로 설치해야 하며, 차단수단의 삭제 또는 비활성화 여부를 확인해서 부모에게 통지해야 함. 이러한 감시 앱 강제설치법은 전 세계적으로 유례가 없으며 매우 국가후견주의적인 제도임
- 특히 보호가 필요한 아동과 청소년이 무조건 사용해야 하는 앱에는 더욱 엄격한 보안기준이 적용되어야 함에도 불구하고 정부는 이에 대한 고려는 전혀 하지 않고 오히려 보안에 취약한 앱을 권장하고 있으며 이는 더 많은 청소년을 보안 위험에 노출시키는 결과를 초래함

나. 권고사항

- 청소년의 프라이버시를 과도하게 침해하는 청소년 스마트폰 감시법을 폐지하라.
- 청소년을 보안 위험에 노출시키는 스마트폰 감시 앱(관리 앱)에 대한 보안심사기준을 마련하고, 현재 제공되고 있는 앱들의 보안성 심사를 추진하라.

다. 담당 부처 및 기관

- 방송통신위원회
- 한국인터넷진흥원

6) 성범죄 보도로 인한 피해자 등의 프라이버시권 침해와 피의사실공표의 문제[123]

가. 배경 및 문제점

- 현재 우리 사회의 성범죄 보도로 인한 프라이버시권 침해 상황
  - 최근 우리 사회 각계각층에서 성범죄 보도와 관련하여 많은 문제점이 발생하고 있음. 언론은 보도 과정에서 피의자, 피해자와 그 가족 등의 인적 사항을 공개하거나, 보도 대상과 관련 없는 사적 영역을 선정적으로 보도하기도 함
  - 일반인이든 유명인이든 이름을 그대로 사용하여 '○○○ 사건'으로 보도하여 사회적 낙인을 찍는 경우도 존재함.
  - 사실관계가 왜곡되는 경우가 있고, 인터넷과 소셜미디어를 통해 빠르게 유포됨
  - 이때 피의자, 피해자 또는 그 가족 등 주변인들에게 발생하는 프라이버시권 침해는 매우 심각함
- 피해자의 민사소송을 통한 구제
  - 성범죄 보도로 인한 프라이버시 침해 당사자가 직접 언론사 또는 유포자를 상대로 민사소송(손해배상, 기사삭제 등) 제기도 가능하나 피해자가 적시에 구제받기 어려움. 프라이버시권 침해는 또한 대부분의 경우 사적인 정보가 광범위하게 유포된 상태이기 때문에 피해자의 회복이 어려움
  - 2012 년 나주시에서 초등학생을 상대로 발생하였던 강간 사건이 있었음. 위 사건에서 보도의 대상이 된 피해자 및 피해자 가족들은 언론사를 상대로 법원에 민사소송을 제기하여 손해배상 및 기사의 일부 내용 삭제를 인정 받음
  - 위 사례에서 법원은 해당 언론사가 아래와 같은 내용을 동의없이 보도하여 피해자의 사생활을 과도하게 침해했다고 인정하였음
    ① 위성 사진, 집 외부, 창으로 된 문을 통한 집 내부의 어지러운 모습 등을 촬영하여 방송, ② 피해자 어린이의 상처난 얼굴, 가해자에게 물린 이빨 자국과 같은 폭력의 흔적 등을 방송, ③ 사건과 무관한 피해자의 그림 일기장, 독서록, 노트 그림 등을 피해자 부모의 동의 없이 촬영하고 방송
  - 그러나 제 1 심이 2014 년 선고되고 제 2 심이 2015 년 선고되는 등 법원의 최종선고에 많은 시간이 소요되었음
- 제재조치 및 시정권고 등을 이용한 규제
  - 방송법 및 방송심의에 관한 규정에 근거한 방송통신심의위원회의 방송심의, 언론중재 및 피해구제 등에 관한 법률에 근거한 언론중재위원회의 시정권고가 있음
  - 위 조치들은 피해자가 직접 법원에 제기하는 민사소송에 비하여 신속한 제재 및 권고가 이루어지나 역시 사후적인 한계가 있으며 피해자 권리 회복이 완전하지 못함
  - 유투브 등을 이용하는 1 인 미디어에 대하여는 민사, 형사 상 절차 외 다른 규제 수단이 없음

123 작성단체: 민주 사회를 위한 변호사 모임

- 국외 사업자 및 플랫폼 사업자가 프라이버시권 침해를 야기하는 경우의 규제책에 대해서도 고민할 필요가 있음

- 언론사의 자율규제 및 수사기관의 피의사실 공표
  - 언론의 보도 자체를 사전에 법률로 규제하고 제한함은 표현의 자유를 침해할 우려가 존재하므로 사전적으로는 언론사의 자율 규제를 기대해야 함
  - 각 언론사는 자율규제를 위한 개별의 취재준칙, 방송강령, 윤리규범 등을 마련하고 있지만, 자율규제의 특성상 지켜지지 않는 경우가 있음
  - 한편 수사기관의 기소 전 피의사실 공표는 법률이 아닌 행정규칙 등에 이루어지고 있고, 이로 인하여 피의사실 공표가 광범위하게 이루어져 성범죄피의자를 포함한 피의자 전반의 인격권 등 침해가 발생하고 있음.
  - 형법은 피의사실공표죄를 규정하고 있지만, 법무부가 국회에 제출한 자료에 따르면 2013 년부터 2018 년 8 월까지 접수된 약 200 건의 피의사실 공표 관련 사건 중 기소된 건은 없음

나. 권고사항

- 언론사의 자율규제가 실패하여 발생하는 프라이버시권 침해를 방지하기 위한 구체적인 계획에 관한 정보를 제공할 것
- 1 인 미디어에 의한 프라이버시권 침해 문제를 해결하기 위한 구체적인 계획에 관한 정보를 제공할 것
- 국외 사업자 및 플랫폼 사업자에 의한 프라이버시권 침해를 방지하기 위한 구체적인 계획에 관한 정보를 제공할 것
- 수사기관의 부당한 피의사실 공표로 인한 피의자의 인격권 등 침해를 방지할 수 있는 구체적인 계획에 관한 정보를 제공할 것

다. 담당부처 및 기관

- 방송통신위원회
- 언론중재위원회
- 문화체육관광부
- 법무부

7) 여성의 프라이버시[124]

온라인 공간의 젠더 폭력과 프라이버시

124 작성단체: 한국 사이버 성폭력 대응센터

프라이버시권에 젠더적 관점을 적용해야 함. 누군가 여성의 프라이버시를 침해하면 그 '누구'가 정부든 기업이든 개인이든 상관없이 중대한 기본권 침해가 이루어진 것으로 받아들여져야 함. 프라이버시권의 보호 원칙을 여성이 경험하는 일에도 적용해야 함. 그러나 한국에서 그동안 이루어진 프라이버시권 보호에 대한 논의는 개인의 사생활에 '여성'을 제외시켜 온 측면이 있음.

한국사이버성폭력대응센터가 다루는 '사이버성폭력'은 온라인 공간에서 발생하는 젠더 폭력으로서 피해경험자의 여러 권리를 침해하는데, 그중 하나가 프라이버시권임. 온라인 공간에서의 여성 대상 프라이버시권 침해 수준은 매우 심각함. 사이버성폭력 사례를 살펴보면 대부분의 경우가 그 자체로 프라이버시권에 대한 심각하고 중대한 침해 행위임을 알 수 있음.

온라인 공간의 '남성'에 의한 여성의 프라이버시권 침해 사례에서, 여성의 정보는 적법하고 정당한 절차에 의해 여성의 인지나 동의를 얻은 후 수집되고 있지 않음. 여성은 자신의 정보가 어떠한 용도와 방식으로 이용되고 있는지 쉽게 확인할 수 없음. 여성은 자신의 사적인 정보에 대해 열람, 정정, 삭제를 요구할 권리를 가지고 있지 않음. 온라인 플랫폼 사업자, 정부는 여성의 프라이버시권을 보호하기 위한 제반조치를 취하고 있지 않음.

여성의 프라이버시권 침해 상태는 즉각적으로 구제되기는커녕 아주 오랜 시간 동안 '남성의 권리','어쩔 수 없는 일'로 인식되어 왔음. 2019 년인 지금도 사이버성폭력 대응 활동 중 여성의 프라이버시권 침해 상황을 해결하려는 시도가 '표현의 자유 침해', '남성 프라이버시권의 침해'로 받아들여지는 경우가 존재함.

예를 들어, 중대한 프라이버시 침해 행위가 명백하게 발생하는 불법촬영물 유포 플랫폼에 접근할 수 없도록 접속차단 차단 조치가 이루어졌을 때, '표현의 자유 침해', '프라이버시 침해'라는 반발이 돌아옴. 접속차단 조치는 해당 사이트에 접속하는- 주로 남성인- 인터넷 유저의 사생활을 침해할 가능성이 있으니 절대 허용해선 안 된다는 것임. '침해될 가능성'으로만 존재하는 단계부터 절대적으로 보장되어야 한다는 프라이버시 보호 원칙이 남성에게는 적용되는 반면 이미 그 사이트에 사적인 촬영물이 유포되어 심각한 프라이버시권 침해를 경험하고 있는 여성에게는 적용되지 않는 것임.

또한 여성 대상 프라이버시권 침해 행위는 성차별적인 사회 문화 구조 안에서 경제적 이득을 창출하는 행위가 되기도 함. 대표적으로, 한국 사회는 여성의 사생활을 동의 없이 촬영하고, 동의 없이 유포한 영상물을 별다른 문제의식 없이 하나의 포르노 장르로 인식해 온 역사가 있음. 그와 같은 영상을 재화로 하는 산업 구조까지 만들어짐. 2018 년에는 여성의 프라이버시권을 침해함으로써 돈을 버는 사업체 간의 유착 구조가 '웹하드 카르텔'이라는 이름으로 드러남.

지금 당장 한국에서 일어나고 있는 여성 대상 프라이버시권 침해와 위협을 좀 더 가시화하고, 여성이 포함된 프라이버시권 개념을 재정립할 필요가 있음. "성별에 따른 프라이버시에 대한 위협과 특유의 혜택 및 경험, 그리고 프라이버시와 인권 원칙을 인식하는 상호교차적 접근방식을 채택하라"는 권고를 적극적으로 실행해야 함.

온라인 공간의 여성폭력 문제에 있어서는 개인 대 개인, 개인 대 기업의 프라이버시권 침해에 개입할 수 있는 공권력의 역할이 중요함. 거대 기업과 국가권력을 중심으로 다뤄져 왔던 기존의

프라이버시권 침해를 강간 문화로 확장해야함. 여성에게, 강간 문화는 빅브라더의 다른 이름임. 기업과 국가권력이 그를 방관하거나 용인할 때, 여성 개인이 자신의 프라이버시를 지키기 위해 싸워야 할 상대는 기업, 국가, 인터넷 유저 개개인으로 더욱 확장될 수밖에 없음.

단순한 임시적 조치로는 이 문제를 해결할 수 없음. 국가는 온라인 공간에 대하여 해당 공간이 치외법권이 아니며, '누구든' 해당 공간에서 프라이버시 침해를 경험하지 아니할 권리가 있다는 관점을 공고하게 확립할 필요가 있음. 온라인 공간에 대한 이해를 바탕으로 해당 공간 자체에 대한 국가 차원의 비전을 수립하여 온라인 공간에서 이루어지는 여성에 대한 폭력과 혐오를 종식하기 위한 체계적이고 포괄적인 대책을 마련해야 함.

7-1) 남성 인터넷 유저에 의한 여성의 프라이버시권 침해

가. 배경 및 문제점

- 성적 촬영물을 이용한 프라이버시권 침해
- 대검찰청 통계에 따르면 카메라등이용촬영죄는 성폭력 범죄 발생건수의 구성비 중 지난 10 년간 가장 급증한 범죄. 2008 년 전체 성폭력범죄에서 차지하는 비중이 4.6%수준이었으나 이후 지속적으로 증가해 2015 년에는 24.9%의 비중을 보임. 2016 년 17.9%로 축소됐다가 2017 년에는 20.2%로 증가함. 카메라등이용촬영죄 통계는 불법촬영과 유포가 통합되어 집계된 것임. 불법촬영에는 화장실, 대중교통 등의 일상적 공간에서 촬영하는 유형과 성관계 등 성적 장면을 촬영하는 유형이 있음.
  - 2018 년 4 월 30 일부터 12 월 31 까지 여성가족부산하 한국여성인권진흥원의 디지털 성범죄 피해자 지원센터의 피해 지원 통계에 따르면 피해 건수 5,687. 그중 온라인 공간에 불법촬영물 유포가 이루어진 건이 2,267 건. 불법 촬영물 게시물 중 해당 센터가 삭제 지원한 2 만 8879 건에 이름.
  - 2 만 8879 건의 삭제 지원 게시물 분석을 통해 `2018 년 디지털 성범죄 피해자 지원 보고서`가 작성됨. 유포 게시글 5 건 중 1 건 이상은 피해자를 특정할 수 있는 신상정보가 담겨 있었음. 센터가 삭제한 불법 촬영물 중 개인정보 유출 피해가 확인된 것은 6700 건으로 전체의 23.2%를 기록함. 전체 개인정보 유출 피해 확인 건의 47.8%가 피해자의 이름이 알려지는 경우로, 가장 많았음. 이어 별칭(23.7%) 주소(9.3%) 순. 피해자가 소속된 집단과 전화번호가 함께 유포된 경우는 각각 8%, 3.1%에 달함.
  - 센터의 지원을 받은 피해자의 절반 이상이 불법촬영, 유포, 유포협박, 사이버 괴롭힘 등의 피해를 중복으로 경험함. 특히 피해자를 통제할 목적으로 성적 촬영물을 활용하는 유포협박의 경우 전체의 14.1%에 해당하는 803 건의 유포협박 피해가 접수되었음. 압수수색영장, 구속 영장 발부가 잘 이루어지지 않아 가해자가 증거를 인멸하거나 촬영물을 유포해버리는 경우 생김.

- ❍ 유포협박을 경험하는 피해자는 어떤 대응 방법을 선택하더라도 유포될 수 있다는 불안감을 느낌. 가해자가 촬영물을 소지하고 있다는 이유 때문에 가해자의 협박을 무효화하기 어려움. 피해자는 타인이 소지하고 있는 자신의 성적 촬영물을 통제할 수 있는 형법적 권한이 없으며 가해자에게 삭제를 강제할 수 없음.
- ❍ 아동·청소년의 경우 랜덤 채팅 어플 등을 통해 쉽게 온라인 그루밍 피해에 노출되어 스스로 자신의 신체나 성적인 장면을 촬영해 가해자에게 건네주기도 함. 아동·청소년이 피해 지원 기관에 연락했을 때, 이미 200 개 넘는 신체 촬영물 및 자위 영상 등을 가해자에게 건네 준 경우도 존재함. 온라인 그루밍을 통해 촬영물을 얻어낸 가해자는 이를 추가 촬영물을 얻어내기 위한 협박 수단으로 활용하거나, 해외 서버 사이트를 통해 촬영물을 판매하기도 함. 현행법 상 온라인 그루밍 행위 자체에 대한 처벌법이 없음. 성적 촬영물을 유포하겠다고 협박하거나 유포하는 등 추가 피해가 발생했을 때 이에 해당하는 법률로 처벌이 가능함.
- ❍ 여성가족부 산하 '디지털성범죄 피해자 지원센터'는 법적대리인의 동의를 받지 않은 미성년자에게 삭제 지원을 제공하지 않음. 즉, 온라인 그루밍 등을 통해 성적 촬영물이 유포되면, 미성년자는 유포된 촬영물을 삭제하기 위해 부모님께 피해 사실을 알려야 하는 것임. 본인의 피해를 부모님 등 보호자에게 알리기 어려운 사례는 국가 차원의 피해지원을 받을 수 없음.
- ❍ 국가가 가해자를 특정하여 처벌하지 못하기 때문에 사이버 범죄가 용인됨. 수사기관에서 '피해자 스스로 가해자를 특정해 오지 않으면 검거할 수 없다'며 피해자에게 수사의 책임을 전가하는 경우가 있음. 이렇게 피해자의 신고를 반려하여 입건 자체를 하지 않는 경우가 있음에도, 2018 년 1~8 월 동안 집계된 불법촬영물 유포 피해 신고 164 건 가운데 검거 건수는 52 건(검거인원 66 명)뿐임.

사례 1. 한 성인 남성이 랜덤채팅 어플리케이션에서 15 세 여성 청소년에게 접근하여 친분을 쌓음. 처음에는 이름과 나이, 학교 이름을 묻고 얼굴이 나오도록 섹시한 사진을 찍어 보내달라고 요구하다가 갈수록 요구하는 사진의 수위가 심해짐. 남성은 15 세 여성 청소년에게 성기 사진을 보내달라고 요구함. 여성이 이를 거절하자 성기 사진을 보내주지 않으면 이전에 보내주었던 가슴사진을 유포하겠다고 협박함. 남성은 '네가 사진을 보내주기 시작했으니 고소할 수도 없다'며 겁을 주었고, 여성은 어쩔 수 없이 가해자가 원할 때 마다 성기 사진을 보내줄 수밖에 없었음.

사례 2. 한 여성이 전 남자친구와 성관계 영상을 찍었고 헤어질 때 지우기로 약속하였음. 그러나 얼마 후 지인으로부터 여성의 성관계 영상이 유포되고 있음을 전해 듣게 됨. 이미 여러 사이트에 유포되었고 조회수가 몇만 회에 달했음. 피해자를 조롱하거나 모욕하는 댓글들도 수백개씩 달리며 끊임없이 영상이 전파되었음. 여성은 자신의 성관계 영상을 삭제하기 위해

애썼지만 아무리 지워도 또 유포되는 것을 경험하며 무력감과 절망감을 느꼈고 자신의 피해가 종결되지 않을 것이라는 좌절을 느끼게 됨.

- 성적 합성 및 편집 후 유포를 통한 프라이버시권 침해
  - ❍ 여성이 SNS 나 메신저 프로필 등에 올린 일상 사진을 당사자의 동의 없이 수집해 성적으로 합성함. 다른 여성의 나체와 합성하는 경우, 여성의 얼굴에 정액이 표현되도록 편집하는 경우, 성적 쾌감을 느끼는 표정으로 합성하는 경우 등 다양한 유형이 있고, 대개 남성 지인이 가해자이기 때문에 '지인능욕'이라고 부르기도 함. 합성된 이미지를 유포할 때 피해 여성의 신상정보를 함께 공개하며 성적으로 모욕하거나 허위사실을 유포하는 경우도 많기 때문에 사이버상 괴롭힘의 성격을 띠며, 게시물이 업로드되면 댓글과 공유를 통해 불특정 다수에 의한 성적 모욕이 추가로 이루어짐.
  - ❍ 2018 년 4 월 30 일부터 12 월 31 일까지 디지털성범죄피해자지원센터의 지원현황에 따르면 총 5,687 건의 피해 건수 중 사진 합성은 2.7%에 해당하는 153 건, 사이버상 괴롭힘은 4.4%에 해당하는 251 건의 피해가 접수되었음.
  - ❍ 주로 남성들끼리 공유되는 오픈 채팅방 링크 등 여성의 접근이 어려운 공간에서 유포가 이루어지기 때문에 피해자는 자신의 사생활 정보가 어디에 얼마나 유포되었는지 파악하기도 어려운 현황. 프라이버시권 침해가 아예 피해자의 인지 범위 밖에서 일어나기 때문에 성적 합성 및 편집 후 유포가 2.7%밖에 일어나지 않는 게 아니라 인지할 수 있는 부분이 2.7%인 것으로 봐야 함.
  - ❍ 이미지를 합성하거나 편집하는 행위는 성폭력처벌법에 해당하지 않음. 사례에 따라 사이버명예훼손이나 모욕죄를 적용할 수 있음. 따라서 성폭력처벌법에 해당하는 경우에 보장받을 수 있는 성폭력 피해자로서의 권리를 보장받지 못하고 본인의 실제 촬영물이 아니라는 이유로 피해가 사소화됨.

사례 1: 어느 '지인능욕' 텔레그램 방에서는 300 여명정도의 사람들이 지인 사진을 가져다가 성적으로 합성, 편집하고 피해자를 '능욕'하고 있었음. 한 남성이 지인 사진을 텔레그램 방에 올리면 다른 사람들이 사진에 자신의 성기를 들이댄 모습을 찍어 올리거나 정액을 뿌린 지인의 사진을 올림. 학교에 몰래 들어가 여학생의 체육복에 정액을 묻히고 이를 인증하기도 하였음. 서로 지인의 사진을 성적으로 합성해주기로 하기도 하고 지인의 얼굴 사진에 정액을 뿌리는 영상을 교환하거나 구매하자는 제안도 오고 감.

- 사이버스토킹을 통한 프라이버시권 침해
  - ❍ 온라인 공간에서의 스토킹은 피해자의 신상정보나 촬영물이 피해자의 동의 없이 수집되어 무단으로 활용되는 방식으로 나타남. 스토킹은 인터넷 게시판, 대화방,

이메일 등 정보통신망을 통하여 상대방이 원하지 않는 접촉을 지속적으로 시도하거나 욕설, 협박 내용을 담고 있는 메일 송신 행위를 지속적으로 하는 것뿐만 아니라, 피해자의 개인정보를 도용하거나 사칭하는 경우도 포함함.

❍ 사이버범죄 수사에 대한 수사기관의 의지와 전문성 부족으로 익명의 가해자를 특정하기 어려움. 촬영물을 도용하고 개인을 사칭하는 행위에 대한 처벌법 역시 부재함.

사례 1: 익명의 가해자가 SNS 메신저를 이용하여 피해자에게 지속적으로 음란한 문자 메세지와 음란물을 전송함. 가해자의 계정에는 피해자의 일상을 몰래 촬영한 이미지가 게시되어 있었음. 가해자는 피해자가 SNS 플랫폼에 해당 계정을 신고해도 계속 새로 계정을 만들어 피해자를 괴롭힘. 뿐만 아니라, 피해자의 사진을 도용해 성매매 사이트에 글을 게시함. 피해자를 사칭하며 성매매 여성인 척 글을 올렸고 피해자의 신상 정보까지 유포함. 피해자의 불법촬영물과 개인정보들이 온라인 공간에 계속 유포되는 것과 성적인 문자가 오는 것을 막을 수 있는 방법이 없었음.

나. 권고사항

- 사이버범죄 수사의 전문성을 높이기 위한 대대적인 자원 투입과 수사 역량강화 대책이 필요함.
- 소지죄 신설 및 삭제 지원 보장 등, 피해자가 자신의 촬영물을 통제할 수 있는 권리를 보장하기 위한 대책을 마련해야 함.
- 부모의 동의를 받지 않기를 원하거나 받을 수 없는 미성년자의 촬영물 삭제를 보장하는 국가 차원의 지원 체계를 마련해야함.
- 성적 합성 및 편집 후 유포, 유포협박을 성폭력 처벌법으로 처벌할 수 있도록 성폭력처벌법을 개정 및 신설해야함
- 인지범위 밖에서 일어나는 프라이버시권 침해 사전 차단하는 조치가 필요함.이는 목차 2) 온라인 플랫폼의 여성 거래로 이어짐.

다. 담당 부처 및 기관

- 경찰청
- 법무부
- 여성가족부
- 과학기술정보통신부
- 방송통신위원회

7-2) 온라인 플랫폼의 여성 거래

가. 배경 및 문제점

- 한국은 성기나 항문이 등장하는 '음란물'의 제작 및 유통이 금지된 국가임. 그러나 '국산야동'이 존재함. 실제 연인간의 섹스를 당사자, 특히 여성의 동의 없이 촬영하고, 유통하여 시청하는 것이 하나의 '포르노' 취향과 장르로 한국 사회에 자리잡음. 한국 남성들은 동의 없이 유포된 여성의 사생활 촬영물을 '국산야동'이라고 부름.
- 2000 년대 이후, '국산야동'의 유통과 소비는 거대한 산업 구조를 만들어 냄. 태블릿, 스마트폰 등 다양한 디지털 기기 보급과 한국의 빠른 인터넷 기술 발전은 '국산야동' 산업화를 가속화함.
- 생산.유통.소비에 관여하는 이들에 의한 집단적 범죄인 성적촬영물 비동의 유포가 주 소비층인 남성들에게 '놀이문화'로 이해되면서, 남성들은 '국산야동'소비를 자신의 권리로 인식하게 됨. 본 단체는 유통플랫폼에 의해 '산업화'되어 국내법 체계 안에서 '국산야동'을 구매할 수 있게 된 사회적 배경이 이와 같은 인식의 토대를 만드는 동시에 더욱 심화시켰음 또한 짚고자 함.
- 한국의 이러한 분위기를 잘 드러내는 사례로 다음의 예를 들 수 있음; 포털 사이트, P2P 프로그램, 웹하드, SNS 등의 사업자인 온라인 서비스 제공자 (OSP)에게 '국산야동' 검색을 제한하는 필터링 시스템 구축을 의무화하고, 그것의 유통을 방치했을 경우 사업자의 처벌이 가능하도록 한 전기통신사업법 개정안이 2014 년 국회를 통과해 2015 년 시행되자, 남성 중심 온라인 커뮤니티들은 이 법률을 이른바 '딸통법'(자위 통제 법률)이라고 부르며 비판함.
- 인터넷의 발전으로 불법촬영물이 '민주화'되었는데, 국가가 시대에 역행하는 규제 정책을 펼침으로써 성적 쾌락의 추구라는 기본권을 침해할 뿐 아니라 그것의 소비에 있어 계급적 '불평등'을 심화시킨다는 것이 이들의 논리임. 이는 일찍이 게일 루빈(Gayle Rubin, 2011/2015)이 '여성－거래'(the traffic in Women)라 부른 것, 즉 남성 간 관계와 연대의 유지를 위해 여성이 교환의 대상으로 활용되는 모습과도 유사함. 유통 플랫폼을 통해 증폭된 촬영물을 이용한 사이버성폭력은 이미지를 통해 여성의 섹슈얼리티를 특정 이미지로 고착시키고, 남성들이 교환하는 여성의 범위를 대폭 확장함으로써 이 같은 '여성－거래'를 현대화하고 있음.
- 웹하드
  - 국내 파일 공유 플랫폼인 '웹하드'는 피해자가 존재하는 촬영물을 유통하며 수익을 얻는 구조를 만들었음. 드라마나 영화처럼 저작권이 있는 컨텐츠는 수익의 70%를 저작권자에게 주고 나머지 30%를 콘텐츠 업로더와 배분해야 하지만, 저작권이 없고 피해자가 존재하는 '국산야동'은 수익의 70%를 웹하드가 가져가고 30%를 업로더가 가져가기 때문에 큰 수익을 얻을 수 있는 '상품'이었음.

- ❍ 거기에 더해, 거의 모든 웹하드가 내부 직원들을 통해 콘텐츠를 모아 직접 업로드를 하거나 불법콘텐츠를 모아 업로드하는 헤비업로더를 고용하는 방식을 적용함. 콘텐츠 유통을 통한 거의 모든 수익을 업체 측에서 가져갈 수 있게 된 것임.
- ❍ 본 단체는 2017 년도 웹하드 전수조사 모니터링을 통해 하나의 웹하드 사이트에 많게는 10 만개 이상의 '국산야동'이 유통되었고, 각 웹하드 당 평균 몇 만개 단위의 '국산야동'을 유통했음을 확인함. 유통량에 있어 상위를 차지한 모 웹하드 업체는 국가에 신고한 수익만 일년에 300 억이 넘었음. 상위 웹하드 사업체의 경우 연간 수익이 천억을 넘는 경우도 있었음.
- ❍ 웹하드 업체들은 동의 없이 유포된 여성의 성적촬영물 삭제 요청을 거부하거나 해당 촬영물의 재유통 방지를 위한 기술적 조치가 가능한데도 조치하지 않은 채 요청받은 게시물만 삭제하곤 했음. 2017 년 5 월 한국사이버성폭력대응센터가 무료 삭제 지원을 시작하기 전까지, 피해 여성은 사설 온라인 평판관리 업체에 월 200~300 만원 정도의 비용을 장기간 지불하며 침해당한 자신의 프라이버시권을 자력구제 해야 했음.
- ❍ 2018 년, 업로더, 플랫폼, 플랫폼의 불법 정보 유통을 견제하기 위한 기술적 조치를 제공하는 업체, 사설 삭제 업체가 모두 한 사람의 소유로, 유착 구조를 이루어 비정상적인 수익을 얻어왔다는 사실이 '웹하드카르텔'이라는 이름으로 공론화됨.

- 해외 불법 포르노 사이트
  - ❍ 해외에 서버를 두고 국내법과 한국 수사기관을 피해 운영하는 불법 사이트로, 국내 사업자 보다 한층 더 대담하게 불법촬영물을 유통함. '국산야동', '일반인야동' , '유출야동', '영계야동'과 같은 키워드로 카테고리를 만들어 불법촬영물을 대량 유통함. 가장 대표적인 사이트는 '소라넷'임. 이용자가 100 만명이 넘는 대형 사이트로, 남성들이 자신의 여성 가족과 지인을 몰래 찍어 올리고 공유하는 게시판이 성행했음. 2016 년도에 국민들의 폐쇄 요구로 수사가 진행되어 폐쇄되었으나 이와 유사한 불법포르노사이트는 여전히 많이 남아 있음. 2017 년 기준 한국사이버성폭력 대응센터가 지원한 206 명의 피해자 영상이 유포된 사이트 중, 해외 불법 포르노 사이트만 300 여개 가량임.
  - ❍ 비트코인, 성매매, 성인용품이나 도박 광고를 통해 광고수익을 얻음. 소라넷의 경우 하루 1 억원의 광고 수익을 벌어들였던 시기가 존재함.

나. 권고 사항

- 온라인 사업자 "'인권과 기업에 관한 유엔 지침'을 이행하고, 자신의 활동의 성별 영향을 효과적으로 고려하여, 자신의 사업 관행에 영향을 받는 모든 사람의 인권을 침해하는 것을 피한다."는 권고를 적극적으로 실행해야 함.
- 플랫폼 사업자 대상 처벌법 강화: 현행법은 불법정보 유통 사실을 명백히 인지했으면서 의도적으로 조치를 취하지 않은 사업자에게 2000 만원 이하의 과태료 처분을 부과하기 때문에 해당 사업자에게 큰 타격이 되지 않음. 불법적인 온라인 플랫폼 사업자를 실효성 있게 규제할 수 있는 법 개정이 필요함.

- 플랫폼 사업자에 대한 사회적 책무 부과: 범죄화되지 않은 여성폭력과 여성혐오의 영역에서도 지속가능한 온라인 플랫폼을 위한 온라인 사업자의 책임이 강화되어야함.
- 피해 구제를 위해 불법정보를 유통하는 해외 인터넷사이트 차단 강화와 더불어 사이트 운영자를 검거하고, 사이트를 폐쇄할 수 있도록 하는 근본적 대책이 마련되어야 함.

다. 담당 부처 및 기관

- 법무부
- 과학기술정보통신부
- 방송통신위원회
- 방송통신심의위원회
- 경찰청

NGO Report on the Right to Privacy in the Republic of Korea

June 2019

Korean Civil Society Organization Network for the Official Visit of the Special Rapporteur on the Right to Privacy to the Republic of Korea

ASUNARO: Action for Youth Rights of Korea, Center for Health and Social Change, HIV/AIDS Activists Network Korea, Korea Cyber Sexual Violence Response Center, Korea National Council of Consumer Organizations, Korean Progressive Network Jinbonet, Rainbow Action Against Sexual-Minority Discrimination[125], MINBYUN-Lawyers for a Democratic Society, Open Net Korea, and People's Solidarity for Participatory Democracy

125 GongGam Human Rights Law Foundation, Korean Lawyers for Public Interest and Human Rights(KLPH), Labor Party-Sexual Politics Committee, Minority Rights Committee of the Green Party, Daegu Queer Culture Festival, Deajeon LGBTQ Human Rights Group Solongos, QUV; Solidarity of University and Youth Queer Societies in Korea, Social and Labor Committee of Jogye Order of Korean Buddhism, the Korean lesbian community radio group, Lezpa, Rainbow Jesus, Rainbow Solidarity for LGBT Human Rights of Daegu, QIP Queer In Pusan, Busan Queer Festival, Gruteogi : 30+ Lesbian commuity grocommunity, Seoul Human Rights Film Festival, Seoul Queer Culture Festival Organizing Committee, Korean Anglican Church's Youngsan House of Sharing (Social Minority Life and Human Rights Center), Yeohaengja : Gender non-conforming people's community, PFLAG Korea, Advocacy for LGBTQ's rights to knowledge, Northwest, Collective for Sexual Minority Cultures PINKS, The Korean Society of Law and Policy on Sexual Orientation and Gender Identity, Sinnaneuncenter: LGBT Culture, Arts & Human Rights Center, Unninetwork, Lesbian Human Rights Group 'Byunnal' of Ewha Womans University, Open Door in JB, Sexual Minority Committee of the Justice Party, Network for Glocal Activism, LGBTQ Youth Crisis Support Center 'DDingDong', Korean Transgender Rights Organization JOGAKBO, Trans Liberation Front, Chingusai – Korean Gay Men's Human Rights Group, Lesbian Counseling Center in South Korea, Korean Sexual-Minority Culture and Rights Center(KSCRC), Youth PLHIV Community of Korea 'R', Solidarity for LGBT Human Rights of Korea, Solidarity for HIV/AIDS Human Rights Nanuri+

Table of Contents

1. Intelligence/Investigation Agencies and Privacy

1) National Intelligence Service (NIS)

Inspection and Surveillance by NIS[126]

A. Background

1) Investigation of citizens

- According to the current National Intelligence Service Korea Act[127], the scope of domestic information that the NIS can handle is limited to security information, specifically, intelligence pertaining to anti-communism, counter-intelligence, anti-terrorism and the collection, writing, and distribution of data for compiling a list of international crime organizations. Therefore, inspections of private companies and civic groups fall beyond its mandate and so doing is illegal.
- Despite the limitations placed on its mandate, the NIS remains under suspicion of secretly surveilling South Korean citizens who have opposed or criticized the government.
  - During the dictatorial regime and authoritarian governments, the NIS, was originally established as the Korean Central Intelligence Agency (KCIA), before undergoing a reorganization and changing its name as the Agency for National Security Planning (ANSP). It employed a variety of surveillance and control tactics to suppress human rights and stifle political oppositions. In 1998, the Kim Dae-jung presidential administration (1998 – 2003) curtailed the Agency's activities, prohibiting it from engaging in domestic intelligence collection, and renamed it as the NIS.
  - However, in September 2002, ahead of the 16th presidential election (in December 2002), Grand National Party (GNP) Member Lee Seong-hun raised suspicions that Park Ji-won, the Chief Presidential Secretary at the time, may have intervened in Hanwha Group's acquisition of Korea Life Insurance. This accusation, along with further revelations from a National Assembly audit revealed that the NIS had indiscriminately and illegally intercepted the conversations of politicians, journalists, businesspersons, and civil groups.
  - In July 2005, the Chosun Ilbo (a major conservative newspaper) revealed that a secret unit for the ANSP had been involved in illegally wiretapping citizens during the Kim Dae-jung administration. Under the Roh Moo-hyun administration (2003 – 2008), then-NIS Chief Kim Seung-kyu ordered an investigation into the activities of the Mirim Team, a covert surveillance team employed to illegally intercept conversations among businesspersons, politicians, and journalists. The probe found the team active under both the Kim Dae-jung administration and the succeeding Kim Young-sam administration (1993 – 1998). Besides being involved in what became known as the X-file scandal, a political scandal that involved wiretapped conversations of politicians arranging bribes for the 1997 presidential election, the team also eavesdropped on conversations of civil society groups, religious figures and

126 Written by People's Solidarity for Participatory Democracy

127 National Intelligence Service Korea Act, Article 3 (1) The NIS shall perform each of the following services: 1. Collection, compilation and distribution of foreign intelligence and domestic security intelligence (anti-communism, subversion of the Government, counter-espionage, counter-terrorism and international criminal syndicate)

outside government group leaders under the Kim Dae-jung administration.

- In October 2008, a news agency reported that NIS officials demanded public corporations and private companies to provide data on donations to civic groups. This action falls beyond the scope of the NIS; therefore, constituting an abuse of authority. After the report, civil society groups strongly condemned such overreach by the NIS.
- In June 2009, Park Won-soon, a senior director at the Hope Institute, raised allegations that the NIS had urged companies to surrender their data and to suspend their sponsorship of the Hope Institute and the Beautiful Foundation. Suspicion around the surveillance of Park Won-Soon, then attorney-at-law, and his office by the NIS revealed a variety of illegal surveillance activities against civil society groups. The following allegations were raised against the NIS: urging the Seoul Metropolitan Government to suspend financial support for an environmental film festival; conducting investigations on a group of professors who opposed the Grand Canal Project; obstructing the group action of the Countermeasures Committee against the Four Major Rivers Restoration Project, placating local officials to secure agreement on legislation related to the New Capital City (Sejong City) of Korea; pressuring the Gwangju Metropolitan City Government to demolish art work that criticized the Four Rivers Restoration Project; requesting the cancellation of civil society event that was to be held at Jogyesa Temple.
- In May 2010, the UN Special Rapporteur on Freedom of Expression, Frank La Rue, was followed and video recorded by the NIS, and these actions prompted protests by him.
- In March 2011, it was found that an individual under investigation for violating the National Security Law had been subject to a network tapping known as “packet tapping” for years. Civil society organizations, along with the victim, filed a petition with the Constitution Court[128]. The NIS admitted its packet tapping on Gmail (@gmail.com) and insisted that it should continue, which revealed that NIS’ assertion that tapping Gmail had been impossible since its server was overseas was a lie.
- In December 2012, a former NIS official revealed that the NIS had organized and coordinated the manipulation of public opinion under the Lee Myung-bak administration (2008 – 2013). NIS cyber-team members, along with their civilian supporters, posted comments that defended the Lee administration while criticizing the opposition, including civil society organizations. This campaign, which attempted to monitor and control political expression online, violated the National Intelligence Service Korea Act[129], which prohibits the NIS from involvement in domestic politics.
- In May 2013, Jin Seon-mi, a Democratic Party Member of the National Assembly, reported that the NIS had engaged in domestic intelligence collection, including gathering information on policies related to half-price tuition, welfare policy expansion, dismissal reinstatement, and the conversion of temporary workers to full-time employees. One-hundred eleven civilians, including civil society groups, accused the NIS of violating the National Intelligence Service Korea Act.

- The NIS has been embroiled in constant controversy related to its illegal surveillance of private

128 Constitutional Court 2011 HUNMA 165
129 National Intelligence Service Korea Act, Article 9 (Prohibition of Involvement in Politics)

citizens for the following reasons:

- The NIS has the authority to investigate, arrest, and detain those crimes specified in the National Security Law. These powers remain separate from other investigative authorities.
- The scope of the NIS's legal authority is vague, and it exercises its power based on presidential decrees or rules, rather than on laws.
- Any expectation by investigative authorities or domestic human rights organizations for independent and impartial investigations on the NIS remain limited, even in cases where the NIS commits human rights violations, such as domestic surveillance activities.
- In June 2015, the media reported that in the course of fulfilling its role of conducting identity surveys on prospective civil servants, the NIS investigated judicial candidates' opinions on social issues. As these opinions did not pertain to national security, the NIS overextended its reach.
- Under Article 33(1) (Identification Survey) of the Presidential Decree, "Security Regulations", the NIS shall conduct an identity survey about prospective civil servants to investigate their loyalty, integrity, and credibility for national security.
- Despite other organizations being capable of assessing the qualifications of public officials, Article 33(1) remains in effect and the NIS continues to lead such investigations[130].
- On February 17, 2005, The National Human Rights Commission of Korea recommended addressing and improving on the lack of legal basis on which the NIS operates.

1) Purchase and Use of the Remote-Control System (RCS) Hacking Program

- In July 2015, HackingTeam, a Milan-based hacker, suffered a hacking resulting in the exposure of its customer list by WikiLeaks. Among its customers was the NIS, which had purchased and used HackingTeam's Remote Control System (RCS), a spyware program that infiltrates computers, smartphones, and monitors.
  - According to the information leaked from HackingTeam's site, the NIS attempted to: Infiltrate KakaoTalk, a mobile messaging application, and domestic models of the Samsung Galaxy 3 smartphone; bypass domestic antivirus programs (e.g. V3 Mobile 2.0); and plant malicious code in the alumni list of Seoul National University of Technology and in a Microsoft Word file questionnaire on the sinking of the Cheonanham, a Korean navy ship.
  - The use of RCS allows the NIS to monitor private citizens' computers and smartphones; thereby revealing not only an infringement of privacy but also violations of laws, including the Act on Promotion of Information and Communications Network Utilization and Information Protection, which prohibit hacking; the Protection of Communications Secrets Act, which prohibits unauthorized eavesdropping; and provisions of abuse of authority in the National Intelligence Service Korea Act.
  - On July 30, 2015, a total of 2,786 people and 41 civil society groups accused the NIS of hacking and this case remains under investigation

130 Security Regulations, Article 33(1) The chief of the National Intelligence Service conducts an identity survey to investigate the loyalty and credibility for national security.

- As the NIS has the authority and investigative powers to intervene in domestic affairs, it continues to engage in illegal hacking and surveillance activities. This can be addressed by separating the NIS' investigative authority and its authority to collect domestic intelligence and then transferring the latter powers to other bodies.

2) Act on Counter-Terrorism For The Protection Of Citizens And Public Security (also known as the Anti-Terror Law)

- In 2001, over a decade before the 19th National Assembly passed the Anti-Terrorism Act on March 2, 2016, an anti-terror bill had been proposed at each session of the National Assembly.
    - In 2001, the NIS submitted an anti-terrorism bill to the National Assembly Information Committee in advance of the 2002 World Cup; however, this failed to pass due to opposition from civil society organizations and the National Human Rights Commission.
    - In 2003, another bill was proposed and received support from the NIS, which was motivated by concerns over the surge in anti-Korea sentiment and the increased threat of terrorism from Korea's additional deployment of troops to Iraq. However, this bill was eventually abandoned due to continued opposition and the expiration of bill's the term.
    - In November 2015, following a terrorist attack in the Paris by an Islamic militant group, the Park Geun-hye administration (2013 – 2017) pressed for the passage of anti-terrorism legislation. In March 2016, despite the opposition of many citizens and civil society groups, an anti-terror bill passed during a National Assembly plenary session.
- The main contents of the Anti-Terrorism Act are to establish a "counterterrorism center" led by the NIS.
- The practical content of the law includes introducing a comprehensive concept of terrorism and authorizes the NIS to collect intelligence on people's financial records and communications. Thus, the law grants the NIS with comprehensive powers for unlimited national surveillance.
- After the Anti-Terror Law was passed on March 2, 2016, the Park administration moved to enact the law. In May 2016, Lee Chul-Woo, a member of the Liberal Korea Party, proposed a counter-terrorism bill, and this was followed by the National Cyber Security Bill in January 2017. The primary contents of the latter bill entail expanding NIS authority to include cyber security, as well as extending its scope to include the private sector, such as telecommunication companies and internet portals. This raises concerns regarding the possibility of the NIS engaging in surveillance and intelligence collection on the private sectors information and communication networks, including the gathering of personal information.

B. Recommendations

- Reorganize the NIS into an international intelligence collection body so that it may fulfill its original role of being an intelligence agency.
    - Abolish the planning and coordination authority of the NIS, which is its basis for exercising control over other government departments
    - Abolish the domestic information collection service of the NIS, which can provide the basis

for domestic political intervention

- Transfer criminal investigative authority to the police and prosecutors' office
- Abolish psychological warfare functions and psychological war
- Transfer cyber security authority to other departments

- Enhance the role of the National Assembly Information Committee, which is the sole organization with the authority to supervise the NIS.
- Repeal the Anti-Terror Law

C. Responsible ministries and agencies

- National Intelligence Service

Cyber Security Authority of NIS[131]

A. Background

- NIS has immense power over cybersecurity on the information and communications network.
  - Overall management and conciliation of national cybersecurity
  - Overall management of cybersecurity of major information and communications network infrastructure in the public area[132]
  - Prevention of cyber crisis and detection attacks of public information and communications network including major telecommunications infrastructures.[133]
  - Investigation of cyber intrusions and analysis of information on threats[134]
  - Security Verification Scheme: a system to verify the safety of the information protection system introduced to national and public institutions.[135]

131 Written by Korean Progressive Network Jinbonet
132 By following Act on the Protection of Information and Communications Infrastructure, NIS takes 'working committee in charge of public sector' under 'the committee for protection of information and communications infrastructure', and is checking whether a management organization implements measures to protect critical information and communications infrastructure of public sector (Article 5-2 (1)), establishing guidelines for formulating measure to protect (Article 6-4), providing technical support (Article 7-1), determining standards concerning the analysis and evaluation of vulnerabilities (Article 9-4), and others.
133 According to the homepage of National Intelligence Agency, it constantly monitors major national computer networks and conducts simulation training". http://eng.nis.go.kr/EAF/1_7.do
134 Investigation of cyber intrusions and analysis of information on threats. In the event of a cyber intrusion against a government/public organization, including an attack by hackers, the NIS investigates the incident, ascertains its cause. and conducts information analysis on cyber threats. The NIS also has established cooperative ties with relevant organs at home and abroad. (http://eng.nis.go.kr/EAF/1_7.do)
135 Article 56 of the Electronic Government Act and Article 5 of the Enforcement Decree of the Management of Archives by Public Agencies

- Korean Cryptographic Module Validation Program[136]

- However, it has no legal ground and is not appropriate as an intelligence agency that the NIS has authorities over the cybersecurity of the public information and communications network infrastructure. Viewed in a historical light of the NIS, such as civilian inspection by abusing their authority and methods of activities, which mainly characterized prowling, there is a huge risk of illegal information gathering and inspection through cyberspace.

- Cybersecurity authority of the NIS lacks legal grounds. There is no overt provision of that authority in the National Intelligence Security Korea Act. The Regulation on National Cyber Security is nothing more than a presidential directive without higher law. According to the Act on the Protection of Information and Communications Infrastructure, the NIS takes a part of 'working committee in charge of public sector' under 'the committee for the protection of information and communications infrastructure', but it is limited to cybersecurity tasks about public sector's information and communications infrastructure. Nevertheless, there is no reason that the NIS should take charge of these tasks as an intelligence agency.

- There is no regulation related to processing gathered personal data while the NIS is in charge of cybersecurity of public information and communications network.

- It is not appropriate that the NIS is in charge of everyday network surveillance task like preventing cyber crises and detecting attacks. Because there is no safeguard to control private surveillance and collecting information of the intelligence agency.

- The NIS is carrying out the mission of investigation of cyber intrusions and analysis of information on threats, but it is not enforced by a warrant requirement. Because the NIS verifies cryptographic module, companies should submit source codes. Through that, the NIS can have control power over the cryptographic market, but it could damage the reliability of code.

B. Recommendation

- Cybersecurity of the public information and communications network is necessary, but it is inappropriate that the NIS has a part of operating as an intelligence agency. The government should transfer authorities for cybersecurity of public information and communications network to other agencies.

C. Responsible ministries and agencies

- National Intelligence Service

- Cheong Wa Dae-the Blue House, Office of National Security

2) The Defense Security Command

136 A system for verifying cryptographic modules used in national and public information and communications network. Article 69 of the Enforcement Decree of the Electronic Government Act and the Cryptographic Module Testing and Validation Guidelines.

2-1) The illegal surveillance on the family members of the victims of Sewol-Ferry Disaster by Defense Security Command[137]

A. Background

- On 16 April 2014, a Korean ferry, Sewol, sank in the south-west sea of Korea, and 304 passengers, mostly students, died or were missing ('Sewol Ferry Disaster')
- The family members of victims of Sewol Ferry Disaster requested the government to investigate the truth of the disaster, but the clear causes of the disaster have not been clarified and the people allegedly responsible for the disaster have not been punished. Only one government official was punished.
- The formal Park-Geun-hye administration systematically obstructed the investigations on the disaster and punishments on allegedly responsible people, such as forcibly dissolving the special investigation committee compulsively.
- A joint probe team consisting of civilian and military officials, under the present administration, found that the Defense Security Commands ordered subordinates to spy on the situations of victims' families on 17 April 2014, a day after the disaster.
- The Defense Security Commands illegally gathered birth dates, cell-phone numbers, internet portal activities, personal blog addresses, email addresses, the list of goods purchased through the internet, the pictures of identification cards and bank books of the family members, and so on. The Defense Security Commands even ordered their subordinates who spied the families on the spot, to disguise as the member of families.
- The Defense Security Commands, in particular, have done national crimes such as classifying the family members as 'pro-North Korea' and spread false facts of the family members to the media.
- Nevertheless, according to the announcement of special investigation team of Ministry of Defense in 2018, only 5 suspects were officially prosecuted, but other remaining 4 were suspended.

B. Recommendations

- Conduct a thorough investigation on the illegal surveillance by the Defense Security Command and punish people who are allegedly responsible for the surveillance.
- Provide specific plans to prevent a recurrence of the illegal surveillance, such as establishing an independent supervisory system, and so on.
- The right to truth, justice, and reparation of the family members should be upheld.

C. Responsible ministries and agencies

- Defense Security Support Command (formerly the Defense Security Command)

137 Written by MINBYUN-Lawyers for a Democratic Society

- Ministry of National Defense

2-2) Illegal Wiretapping of the Defense Security Command[138]

A. Background

- The Defense Security Command is an intelligence investigation agency under the Ministry of National Defense, aimed at collecting information on military affairs, military security and counterintelligence, and criminal investigation. But, the inspection of the families of missing people by the agency right after the Sewol ferry sinking in 2014 at the time of Park Geun-hye regime, and its preparation of martial law in 2017 during the candlelight vigil calling for impeachment has been social controversy. With that controversial, the agency was disbanded in September 2018 and reorganized into the Defence Security Support Command.
- On April 8, 2019, when Chun Jung-bae, an assembly person of Party for Democracy and Peace, disclosed the daily report of <Sewol ferry TF> drawn up by the Defense Security Command, it was revealed that the agency wiretapped the phone conversation of ordinary citizens illegally and indiscriminately at the Park Geun-hye government.
- From June 10, 2014, to July 22, 2014, the agency illegally listened to and recorded the contents of private communication without court approval in Seoul, Hanam, Seongnam, Yongin and Anseong by using its own mobile surveillance equipment and radio monitoring facilities of Radio Management Service under Ministry of Science, ICT and Future Planning (currently the Ministry of Science and ICT). It turns out that private conversations at taxis, hospitals, playgrounds, and movie theaters were wiretapped indiscriminately.139
- Such an activity of the agency was aimed at investigating Yoo Byeong-eon, the owner of the Sewol ferry, but it is beyond the agency's scope of duty and wiretapping without court approval is illegal in violation of the Protection of Communications Secrets Act.
- The mission of the Radio Management Service is “to monitor radio waves to maintain radio order including removal of confusion according to articles 49 to 51 of the Radio Waves Act”, and recording other people's conversations for purposes beside radio management constitutes illegal wiretapping. The agency suggested wiretapping with the help of the Radio Management Service to the prosecution, and the Supreme Prosecutors' Office appears to have actually asked for the cooperation to the institution and carried it out, which means that the prosecution and the ministry were also involved in the illegal activities and abandoned their duty to crack down on them.
- On April 15, 2019, civil society organizations filed a complaint with the prosecution against those subject to illegal surveillance including the Defense Security Command.

B. Recommendation

138 Written by Korean Progressive Network Jinbonet
139 JTBC, right after the Sewol ferry disaster, illegal surveillance of civilians...indiscriminate wiretapping at movie theaters, restaurants, etc. 2019.4.8

- Conduct a thorough investigation into the illegal wiretapping by the Defense Security Command and punish relevant officers.
- Establish an independent supervisory system to prevent the agency from illegally inspecting and spying on civilians beyond its authority.

C. Responsible ministries and agencies

- Defense Security Support Command (formerly the Defense Security Command)
- Ministry of Science and ICT (formerly Ministry of Science, ICT and Future Planning)
- Radio Management Service

3) Police Agency

3-1) Investigative Information System[140]

A. Background

- According to data from an inspection of government offices in 2017, the police has almost 37 billion cases through 83 units of database systems.141 However, even the National Assembly cannot exactly figure out the present situation.
- Most of the database systems of the police such as gathered evidence system, have no specific legal ground for its establishment and operation. Only a few systems, such as the criminal justice information system and the identification information system of DNA have specific legal ground.
- These police systems are operated without a legal ground and personal data in that systems is vulnerable to be used for other purposes and connected to different systems, increasingly becoming the target of the automatic identification.
- As a result, there is no control on the personal information database system of police on a large scale and processing personal data. The public does not know what is collected by the policy system, and they cannot exercise the rights to access, correct, delete and demand the cessation of the processing their personal information.
- In 1999, activists from social organizations have been submitting constitutional petitions against establishing and operating ten-fingerprints database collected from all citizens over 17 years old without any legal ground. However, the Constitutional Court dismissed appeals in 2005 because the Police Act and the Act on the Performance of Duties by Police Officers include “Collection, preparation, and distribution of information on public security” as the scope of duties.142
- After that, the courts and the Constitutional Court have been holding that position to all kinds of police systems. In 2010, activists from social organizations brought an action for damages

140 Written by Korean Progressive Network Jinbonet
141 NEWSIS. (2017). Police, Securing 3.7 Billion Personal Information… 2.7 Billion Cases in Criminal Justice Information System. http://www.newsis.com/view/?id=NISX20170114_0000117579 [15 May 2019]
142 the Constitutional Court, May 26, 2005, 99Hun-ma513, etc.

against establishing and operating CIMS (Crime Information Management System) by collecting all information from suspects and testifiers including victims without a specific legal ground. However, the judge ruled against the plaintiff.143

- In 2018, the police reformation committee recommended the establishment of a separate and specific legal ground for establishing and operating the police information system concerning its grounds, procedures methods and controls. It further recommended prohibiting establishing and operating of an information system, which is not opened to inside and outside of the police. However, no improvement has been made.

B. Recommendations

- The purposes, procedures, methods, and controls of the personal information database system should be in accordance with specific provisions of relevant laws.
- An adoption of the supervision of independent third-party agency concerning the police personal information database system.

C. Responsible ministries and agencies

- National Police Agency

3-2) Vehicle search system of the police[144]

A. Background

- The vehicle search system is operated solely along with the police's own operating guidelines145 which were issued in October 2015. This system collects information on the driving routes of innocent people (more than 24 million per day) and retains these records for 30 days. Furthermore, the police have an MOU with CJ Korea Express, a courier company, which enables it to receive black box images from CJ. 146
- Although the police engage in the large-scale collection and accumulation of people's personal information, such data is only customarily processed in accordance with general regulations (e.g. collection, creation and distribution of police information147) or the police's own guidelines without legislative basis.
- Particularly in the case of emergency searches for wanted persons, the vehicle search system is designed to allow for 'similar searches' whereby one only needs to input two letters or numbers from a license plate. If a person has a license number similar to that of the wanted vehicle number, then this could disclose that person's route. In 2014, when searching for Yoo Byung-

143 the Supreme Court, October 25, 2012, 2012Da12641
144 Written by People's Solidarity for Participatory Democracy
145https://www.police.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000083492&fileSn=1&bbsId=B00000032
146 http://news.donga.com/3/all/20160616/78695611/1
147 Police Act, Article 2(4) (Scope of Job) and the Act on the Performance of Duties by Police Officers, Article 2(4) (Scope of Job)

eun, the chairperson of the shipping company that operated the Sewol Ferry, which sank and claimed the 304 lives (mostly children), the police randomly checked the personal information of private citizens who had searched for a specific location through a smartphone navigation application. A similar incident occurred in 2014 when the police tracked members of a rail workers union strike using the vehicle search system. This search not only included those participating in the strike, but also the participants' family members.

- Collection, dissemination, and distribution of personal information should only be permitted where there is a "special regulation in law" or such actions are "necessary" for the performance of the job.148 However, the police's current vehicle search system violates the principle of reservation and proportionality.

B. Recommendations

- The collection of personal information by the police should entail a public debate, as well as a legislative control plan by the National Assembly. Furthermore, a legal basis should be established for the vehicle search system. This includes civilian control of the system, preparation of an annual report on the system's operation status, a report by the National Assembly, and procedural control regulations.

C. Responsible ministries and agencies

- Ministry of Public Administration and Security / National Police Agency

3-3) CCTV Integrated Control Center[149]

A. Background

- CCTV integrated control centers, which have been installed and are operated by local governments, can connect the CCTVs of various public institutions so that all images can be checked in a single location.
- According to the Ministry of Public Administration and Security, as of the end of 2017, a total of 208 (92%) of the 226 local governments in Korea have installed and are operating integrated control centers. The Ministry plans to support the establishment of integrated control centers in all local governments in the future, and this project is currently underway in five cities, including Sokcho, Pyeongchang, Hwacheon, Yangyang, and Jindo.

<Installation Status of CCTV Integrated Control Center>

(Unit: the number of cities and towns)

Category	Recent statistics

148 Article 15 (1) No. 2, No. 3 of the Privacy Act
149 Written by People's Solidarity Participatory Democracy

	~2010	2011	2012	2013	2014	2015	2016	2017
Number of CCTV Integrated Control Centers	26	34	27	33	29	22	19	18
Total	26	60	87	120	149	171	190	208

※2010 figures include up to the number before 2010

- The CCTV integrated control centers connect CCTVs, which have been installed by local governments, to check and store footage. Police officers work at most of the integrated control centers to respond to a criminal activity.
- According to the data from 2017 from the National Police Agency, a video information sharing system was established between the police and the local government (CCTV integrated control center). Footage from the CCTV integrated control center can be viewed in the situation rooms of police stations.

Order	National Police Agency	Police Station	CCTV Integrated Control Center	Location	The number of systems accessible by PC
1	Seoul Metropolitan Police Agency	Seoul Yongsan Police Station	Yongsan Integrated Control Center	Police Station Situation Room	1
2	Seoul Metropolitan Police Agency	Seoul Seongbuk Police Station	Seongbuk Integrated Control Center	Police Station Situation Room	1
3	Seoul Metropolitan Police Agency	Seoul Seongdong Police Station	Seongdong Integrated Control Center	Police Station Situation Room	1
4	Seoul Metropolitan Police Agency	Seoul Gangbuk Police Station	Gangbuk Integrated Control Center	Police Station Situation Room	1
5	Seoul Metropolitan Police Agency	Seoul Geumcheon Police Station	Geumcheon Integrated Control Center	Police Station Situation Room	3
6	Seoul Metropolitan Police Agency	Seoul Jungnang Police Station	Jungnang Integrated Control Center	Police Station Situation Room	1
7	Seoul Metropolitan Police Agency	Seoul Gangdong Police Station	Gangdong Integrated Control Center	Police Station Situation Room	2
8	Seoul	Seoul Jongam	Seongbuk Integrated	Police Station	1

	Metropolitan Police Agency	Police Station	Control Center	Situation Room	
9	Seoul Metropolitan Police Agency	Seoul Yangcheon Police Station	Yangcheon Integrated Control Center	Police Station Situation Room	1
10	Seoul Metropolitan Police Agency	Seoul Songpa Police Station	Songpa Integrated Control Center	Police Station Situation Room	1
11	Seoul Metropolitan Police Agency	Seoul Bangbae Police Station	Seocho Integrated Control Center	Police Station Situation Room	1
12	Seoul Metropolitan Police Agency	Seoul Dobong Police Station	Dobong Integrated Control Center	Police Station Situation Room	1
13	Seoul Metropolitan Police Agency	Seoul Suseo Police Station	Gangnam Integrated Control Center	Police Station Situation Room	1
14	Daegu Metropolitan Police Agency	Daegu Dalseong Police Station	Dalseonggun Integrated Control Center	Police Station Situation Room	4
15	Daegu Metropolitan Police Agency	Daegu Suseong Police Station	Suseong-gu office Integrated Control Center	Police Station Situation Room	4
16	Incheon Metropolitan Police Agency	Incheon Jungbu Police Station	Jung-gu Integrated Control Center Dong-gu Integrated Control Center Ongjin-gun Integrated Control Center	Police Station Situation Room	1
17	Incheon Metropolitan Police Agency	Incheon Nambu Police Station	Nam-gu Integrated Control Center	Police Station Situation Room	1
18	Incheon Metropolitan Police Agency	Incheon Namdong Police Station	Namdong -gu Integrated Control Center	Police Station Situation Room	1
19	Incheon Metropolitan Police Agency	Incheon Bupyeong Police Station	Bupyeong -gu Integrated Control Center	Police Station Situation Room	1
20	Incheon Metropolitan Police Agency	Incheon Samsan Police Station		Police Station Situation Room	2

21	Incheon Metropolitan Police Agency	Incheon Gyeyang Police Station	Gyeyang -gu Integrated Control Center	Police Station Situation Room	1
22	Incheon Metropolitan Police Agency	Incheon Ganghwa Police Station	Ganghwa-gun Integrated Control Center	Police Station Situation Room	2
23	Incheon Metropolitan Police Agency	Incheon Yeonsu Police Station	Yeonsu-gu, Incheon Free Economic Zone	Police Station Situation Room	2
24	Gyeonggi Nambu Provincial Police Agency	Suwon Jungbu Police Station	Suwon-si Integrated Control Center	Police Station Situation Room	2
25	Gyeonggi Nambu Provincial Police Agency	Suwon Nmabu Police Station		Police Station Situation Room	2
26	Gyeonggi Nambu Provincial Police Agency	Suwon Seobu Police Station		Police Station Situation Room	2
27	Gyeonggi Nambu Provincial Police Agency	Anyang Dongan Police Station	Anyang-si Integrated Control Center	Police Station Situation Room	1
28	Gyeonggi Nambu Provincial Police Agency	Anyang Manan Police Station		Police Station Situation Room	2
29	Gyeonggi Nambu Provincial Police Agency	Gunpo Police Station	Gunpo-si Integrated Control Center	Police Station Situation Room	1
30	Gyeonggi Nambu Provincial Police Agency	Bucheonsosa Police Station	Bucheon-si Integrated Control Center	Police Station Situation Room	1
31	Gyeonggi Nambu Provincial Police Agency	Bucheonwonmi Police Station		Police Station Situation Room	1
32	Gyeonggi Nambu	Bucheonojeong Police		Police Station	1

	Provincial Police Agency	Station		Situation Room	
33	Gyeonggi Nambu Provincial Police Agency	Gwang Myeong Police Station	Gwang Myeong-si Integrated Control Center	Police Station Situation Room	1
34	Gyeonggi Nambu Provincial Police Agency	Ansan Danwon Police Station	Ansan-si Integrated Control Center	Police Station Situation Room	1
35	Gyeonggi Nambu Provincial Police Agency	Ansan Sangnok Police Station		Police Station Situation Room	1
36	Gyeonggi Nambu Provincial Police Agency	Siheung Police Station	Siheung-si Integrated Control Center	Police Station Situation Room	1
37	Gyeonggi Nambu Provincial Police Agency	Hwasung Dongbu Police Station	Osan-si Integrated Control Center	Police Station Situation Room	1
38	Gyeonggi Nambu Provincial Police Agency	Yongin Dongbu Police Station	Yongin-si Integrated Control Center	Police Station Situation Room	1
39	Gyeonggi Nambu Provincial Police Agency	Yongin Seobu Police Station		Police Station Situation Room	4
40	Gyeonggi Nambu Provincial Police Agency	Gwangju Police Station	Gwangju-si Integrated Control Center	Police Station Situation Room	1
41	Gyeonggi Nambu Provincial Police Agency	Gwacheon Police Station	Gwacheon-si Integrated Control Center	Police Station Situation Room	2
42	Gyeonggi Nambu Provincial Police Agency	Hanam Police Station	Hanam-si Integrated Control Center	Police Station Situation Room	1

43	Gyeonggi Nambu Provincial Police Agency	Icheon Police Station	Icheon-si Integrated Control Center	Police Station Situation Room	1
44	Gyeonggi Nambu Provincial Police Agency	Kimpo Police Station	Kimpo-si Integrated Control Center	Police Station Situation Room	1
45	Gyeonggi Nambu Provincial Police Agency	Yeoju Police Station	Yeoju-si Integrated Control Center	Police Station Situation Room	2
46	Gyeonggi Bukbu Provincial Police Agency	Dongducheon Police Station	Dongducheon-si Integrated Control Center	Police Station Situation Room	1
47	Gangwon Provincial Police Agency	Wonju Police Station	Wonju city information center	Police Station Situation Room	1
48	Gangwon Provincial Police Agency	Jeongseon Police Station	Jeongseon-gun Integrated Control Center	Police Station Situation Room	1
49	Gangwon Provincial Police Agency	Hongcheon Police Station	Hongcheon-gun Integrated Control Center	Police Station Situation Room	1
50	Jeonbuk Provincial Police Agency	Jeonju Wansan Police Station	Jeonju-si Integrated Control Center	Police Station Situation Room	2
51	Jeonbuk Provincial Police Agency	Jeonju Deokjin Police Station			
52	Jeonbuk Provincial Police Agency	Wanju Police Station	Wanju-gun Integrated Control Center	Police Station Situation Room	1
53	Gyeongbuk Provincial Police Agency	Yecheon Police Station	Yecheon Integrated Control Center	Police Station Situation Room	1
54	Jeju Provincial Police Agency		Jeju Integrated Control Center	112 General Situation Room	1
55	Jeju Provincial Police Agency	Jeju Dongbu Police Station		Police Station Situation Room	1

56	Jeju Provincial Police Agency	Jeju Seobu Police Station			1
57	Jeju Provincial Police Agency	Jeju Seogwipo Police Station			1

- Despite potentially infringing on the privacy of citizens' personal information, the integrated Control Center, which collects and stores all CCTV footage, has no basis for its operation within the Personal Information Protection Act or other legislation. Furthermore, CCTV images are often used for purposes other than their original intention and are supplied to police for criminal investigations. On May 5, 2018, the National Human Rights Commission of Korea recommended to the Minister of Public Administration and Security "to establish a legal basis for the operation of a CCTV integrated control center to comply with the constitutional standards, and to provide details on the use of personal video information through an enactment."150
- Under the current Personal Information Protection Act, there is no legal basis for the CCTV Integrated Control Center.
- Problems with the proposed legislation to protection private image information
  - The National Human Rights Commission noted that the legislation to protect private image information proposed by the Ministry of the Interior and Safety does not explicitly mention the Integrated Control Center, nor is it sufficient as a law to minimize human rights violations.

B. Recommendations

- Strict legal provisions are required for the purpose, requirements, and procedures about the operation of CCTV Integrated Control Centers, as well as set out provisions regarding the sharing of footage in real time with other agencies, and establish control procedures for such sharing.

C. Responsible ministries and agencies

- The Ministry of the Interior and Safety, National Police Agency

3-4) Domestic Intelligence Police[151]

A. Background

- Korean National Police Agency have been operating department that collects information that is not related to criminal investigation under the comprehensive licensing regulation of Article 3(5)

150 National Human Rights Commission Standing Committee Decision 2015.5.3. "Recommendation for improvement of installation and operation of closed-circuit TV integrated control center"
151 Written by Korean Progressive Network Jinbonet

of Police Act and Article 2(4) of Act on the Performance of Duties by Police Officers, which is "collection, preparation, and distribution of information on public security". Furthermore, the domestic intelligence of police department has been monitoring the people who criticize the government and making political reports for the ruling party's rule.

- According to media report152, the largest portion of the information police's work in 2018 was the creation of "policy data" sent to Cheong Wa Dae (22.5%). Foreign cooperation (20%) and assembly management (12.3%) followed, and criminal intelligence, which the original work, was only taking 1.3%.
- The aforementioned figures are evidence of illegal and widespread collection of information that does not have to be related to risk prevent or criminal investigation as 'information on public security'.
- The intelligence police have been collecting information from each citizen and using it. In the process, there was a reckless invasion of personal privacy and there is no way to recognize whether the data subject himself and/or herself has become a target of the monitoring.
- Evidence of civilian surveillance by the intelligence police continues to emerge. According to 'Research Team for Human Rights Violated by Police' on May 14, 2019, Yum Ho Suk153, a worker at Samsung Electronic Service, chose to die while on strike against company's oppression to labor union. After his death, intelligence police monitored the workers' families and acquaintances in collusion with the company.154 In addition, police officers were found following the bereaved families of the Sewol ferry disaster on a walking tour from Danwon High School in Ansan to Paengmok Port in Jindo.155
- It also conducted surveillance of state officials and lawmakers as well as civilians. Domestic intelligence police monitored and analyzed those who are burdened by the administration by analyzing the nature of each lawmakers and suggesting the direction in which government and the ruling party should respond.
- The domestic intelligence police were actively involved in the election. In 2011, the intelligence police conducted explicit political moves by checking the movements of the other candidates and examining relevant civic groups to win the ruling party's candidate in Seoul mayoral election, analyzing the election situation, and proposing the presidential office's plan to run state affairs before and after the election.156 Under the Park Geun-hye regime, the intelligence police tried to find strategies to change ruling party lawmakers all to police-friendly position

152 KBS(2019), Criminal Information is only 1.3%.... "Cheong Wa Dae opposes the recommendation to abolish the intelligence policy", http://news.kbs.co.kr/news/view.do?ncd=4149872&ref=A , [17, May, 2019]
153 The Kyunghyang Shinmun (2019), Police Acted as "Agent for Samsung" in the case of Yeom Ho-Seok, http://english.khan.co.kr/khan_art_view.html?artid=201905151627557&code=710100 [21, May 2019]
154 Hankyoreh (2019). In the late Yeon Ho Suk case, the intelligence police acted as Samsung's hands from start to finish. http://www.hani.co.kr/arti/society/society_general/893837.html [17, May, 2019]
155 Hankyoreh (2014). [Single] The plainclothes police are detected again while following the families of the Sewol victims. https://www.hani.co.kr/arti/society/society_general/646775.html [2019.5.17]
156 Hankyoreh (2019), [Single] Domestic Intelligence Police, Na Kyoung-won's self-appointed campaign during the Seoul mayoral race, http://www.hani.co.kr/arti/society/society_general/892328.html [17 May 2019]

through analyzing governing party lawmakers characters.157

- During the Lee Myung-bak administration, the intelligence police mentioned themselves as 'the advance guard' of the government, and asked government using them by wishing success of the government and in return for their political masters. Furthermore, they claimed a place of political office in document.158 In that document, it is mentioned that 'the police is pray for the success of the government of Lee Myung-bak, than any government ever'. Additionally, through that document you can see that 'the great majority of the senior police officials acted in the Lee Myung-bak's campaign and affected to police officers who work in field currently during the presidential election'.

B. Recommendation

- Abolishing 'domestic intelligence police' that have nothing to do with criminal investigation, conducting a thorough fact-finding investigation into civilian surveillance and election meddling that has been carried out by the domestic intelligence police and punishing those responsible.
- In the case of police intelligence activities for criminal investigations, control and supervision by independent bodies should be strengthened.

C. Responsible ministries and agencies

- National Police Agency

157 Hankyoreh (2019), The Domestic Intelligence Police, Make 'Party Management Card' and inspect personal connections, http://www.hani.co.kr/arti/society/society_general/881576.html [17 May 2019]]
158 The Kyounghyang Shinmun (2019), Police under the Lee administration, claiming to be "Frontier Guard' and pledging loyalty. http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201905130600015 [17 May 2019]

2. Communication Secrecy

1) Packet eavesdropping[159]

A. Background

- Packet eavesdropping involves intercepting and monitoring network traffic that is exchanged through a specific internet line (e.g. IP address, TCP address, etc.).
- Current packet eavesdropping technology remains incapable of distinguishing targeted information (such as information relevant to the crime) from other types of general information. This presents a challenge in fulfilling the requirements of the Protection of Communications Secrets Act. Despite the technical limitations of such technology, the courts have permitted investigative agencies to eavesdrop, and with court permission, investigative agencies may employ packet eavesdropping as a means of collecting intelligence.
- The full extent of packet eavesdropping remains unclear. It is estimated that in 2018, the NIS was responsible for 99.4%160 of eavesdropping, so it can be assumed that packet eavesdropping is also a surveillance technique used by the NIS.
- Constitutional Court 2018. 8. 30. 2016 HUNMA 263: As most people, including those not suspected of a crime, share a single internet line, use of packet eavesdropping extends beyond the scope permitted by the courts. Not only is the data of the suspect collected, but also the data of those not suspected of any crime.
- Therefore, we could not compare the amount of personal communication data acquired by the investigating agency with other communication restriction measures, such as surveillance through Internet wiretapping. In respect of internet wiretapping, there is a strong demand for legal devices to monitor or supervise whether information from third parties or information unrelated to a criminal investigation is collected or stored by the investigating agency and whether the investigation agency is using and processing the data within the scope and according to the purpose for which permission was originally granted.
- cases
    - On September 27, 2008, Kwak Dong-gi, a policy committee member of the Solidarity for Practice of the South-North Joint Declaration, was arrested and detained on suspicion of violating the National Security Law. During his trial, it was revealed that from June 12, 2008 to August 11, 2008, the NIS had conducted packet eavesdropping on all IP addresses and computers that Kwak had accessed in his home and office.
    - In February 2011, the NIS conducted packet eavesdropping on an individual named Kim, who had been acquitted of charges of violating the National Security Law. On March 29, 2011, Kim filed a petition with the Constitutional Court; however, on February 25, 2016, the Court terminated the petition on account of the victim's death. On March 29, 2016, civil society organizations filed a constitutional petition with other victims of packet eavesdropping. This eventually led to the Court declaring that the use

159 Written by People's Solidarity for Participatory Democracy
160 Ministry of Science and ICT 2019. 5. 10. Press Release <Announcement of status report on communication data and communication confirmation in the second half of 2018>

of packet eavesdropping does not conform to the Constitution.

- On October 1, 2014, Jeong Jin-woo, the deputy chairperson of the Labor Party, said that during an investigation, the police had tapped his KakaoTalk chat records, which involved conversations with 3,000 people. This led to concerns that authorities were engaged in packet eavesdropping on KakaoTalk, which led many users to migrate to foreign services.
- It was found that Min-Soo Kwon, a cyber security investigation chief with the National Police Agency, had used "Client Computing System"(B.F.S Matrix SW) to engage in surveillance activities similar to packet eavesdropping.
- In 2019, the Korea Communications Commission introduced 'HTTPS SNI field blocking' to block access to banned sites. However, the boundary between using SNI blocking and automated systems to conduct eavesdropping remains vague leading to concerns that a blocking system may be used at any time for packet eavesdropping.

- Article 5 (1) of the Protection of Communications Secrets Act, which sets out the requirements for obtaining permission for conducting eavesdropping should not be a basis for permitting packet wiretapping.
  - In the 20th National Assembly, a number of amendments on the Protection of Communications Secrets Act were passed to strictly comply with the requirements for permitting eavesdropping. However, as packet eavesdropping is a form of bulk surveillance, rather than a targeted surveillance method, the argument that such a technique can be employed with a warrant under the Protection of Communications Secrets Act grants the use of warrantless surveillance, which does not conform to the Constitution.
  - The Constitutional Court declared that packet eavesdropping constituted an excessive use of force and required an amendment by March 31, 2020.161 The Court added that due to the massive amount of information collected and the use of eavesdropping on targeted individuals, such a surveillance system must provide legal control and post-implementation notification from the enforcement stage.
- Information obtained by packet eavesdropping is rarely presented as evidence of a crime
  - In a case where the National Association for the Fatherland Unification was charged with violating the National Security Law, the prosecutors did not submit data obtained by the NIS through packet eavesdropping. Although the NIS had been surveilling the organization’s internet line for seven years, none of the collected data was submitted as evidence during the Constitutional Court trial.
  - Past cases of packet eavesdropping have raised strong doubts as to whether it is an indispensable method of collecting "evidence" as this evidence has never been used in actual criminal justice procedures. Furthermore, the NIS has not commented on its reasons for employing such techniques to gather extensive information that is never used as evidence.

161 Constitutional Court 2016 HUNMA 263

B. Recommendations

- Current packet eavesdropping techniques and technology do not allow for distinguishing targeted data from general data. Therefore, it is necessary to establish strict control procedures for packet eavesdropping.

C. Responsible ministries and agencies

- Ministry of Justice / Ministry of Science and ICT

2) Communication Confirmation Data[162]

A. Background

- Article 13 of the Protection of Communications Secrets Act allows the law enforcement bodies to request a telecommunications business entity for their access to or the submission of the data which can verify the fact of one's communication (Communication Confirmation Data) if necessary for a criminal investigation and execution.
- It is clearly provided that an investigation agency shall obtain permission from courts to request the Communication Confirmation Data, but if an urgent ground exist that makes it impossible to obtain a permission from the competent district court or branch court, it can obtain such permission after requesting the Communication Confirmation Data.163 Since the investigation agency can access to such data simply by a court permission, not by a warrant, reckless requests for Communication Confirmation Data are being made under a loose supervision.
- In 2014, the National Human Rights Commission of Korea ("NHRC"), through the "Recommendation for Improving the Communications Data Provision under the Telecommunications Business Act and the Communication Confirmation Data Provision under the Protection of Communication Secrets Act, pointed out that the permission requirements for requesting the Communication Confirmation Data are too vague to prevent investigative agencies from its abuse and they are not sufficient to protect the privacy ."
- In the abovementioned recommendation, the NHRC recommended deleting 'real-time location tracking' from the Communication Confirmation Data and limiting conditions of the provision of communication confirmation data into the fact that "there is a reasonable ground for a suspicion that a suspect has committed a crime in relation to a case concerned". Also, in the case of 'real-

162 Written by Korean Progressive Network Jinbonet

163 Protection of Communications Secrets Act, Article 13 (2): Any prosecutor or judicial police officer shall, when he/she asks for the provision of the communication confirmation data under paragraph (1), obtain permission therefor from the competent district court (including any ordinary military court; hereinafter the same shall apply) or branch court with a document in which the reason for such asking, the relation with the relevant subscriber, and the scope of necessary data are entered: Provided, That if the urgent grounds exist that make it impossible to obtain permission from the competent district court or branch court, he/she shall obtain permission immediately after asking for the provision of the communication confirmation data and then send it to a telecommunications business entity.

time location tracking' for a criminal investigation, in addition to the enhanced requirements, it was recommended that supplemental requirements be met.

- Number of requests for communication confirmation data by communication methods.[164]

(Unit: Number of documents)

Year	Telephone	Mobile Phone	Internet and PC communication
2014	48,890	177,361	32,933
2015	57,838	207,004	36,100
2016	58,755	213,813	30,753
2017	59,590	204,524	37,207

- The Communication Confirmation Data are metadata, which do not include contents, but they are sensitive data that can infer information about data subjects by combining and analyzing different types of information.165
- The Communication Confirmation Data requested by investigation agencies include phone numbers, the time and duration of communication, internet log records, IP addresses, and location of base stations from which a communication is dispatched.166
- An investigation agency makes extensive use of 'base-station investigation', which requesting communication records for all people who connected with base station in specific time and place without pointing out a specific subject, and 'real-time location tracking', which is tracking

164 Ministry of Science and ICT, Current situation about the provision of communication data and communication confirmation data (2014~2017).
165 the Constitutional Court, June 28, 2018, 2012Hun-ma538
166 The Article 2, 11 refers what communication confirmation data includes.
11. The term "communication confirmation data" means the data on the records of telecommunications falling under any one of the following:
(a) The date of telecommunications by subscribers;
(b) The time that the telecommunications commence and end;
(c) The communications number of outgoing and incoming call, etc. and the subscriber number of the other party;
(d) The frequency of use;
(e) The computer communications or Internet log records relating to facts that the users of computer communications or the Internet have used the telecommunications services;
(f) The data on tracing a location of information communications apparatus connecting to the information communications networks;
(g) The data on tracing a location of connectors capable of confirming the location of information communications apparatus to be used by the users of computer communications or Internet for connecting with the information communications networks;

the target's future location in real time.

- In 2015, UNHRC remained concerns about asking the provision of subscribers' information from telecommunication businesses without warrants and insufficient regulation of 'base station investigation' to target participants in the specific rally.167
- The 'base station investigation' of the investigation agency directly violates the inviolability of communications secrets and privacy rights. Furthermore, it is violating communications secrecy and the secrecy of location data even if he/she is not suspected.
- Because there is no provision as to for which crime the Communication Confirmation Data can be requested, any crimes can be subject to such request. Without a warrant from the court, sensitive data such as personal communication details and location data can be provided to an investigation agency.
- In 2012, while investigating suspicion of bribery during the election campaign, an investigation agency was provided with the Communication Confirmation Data of 659 people by using 'base station investigation'. For this, in the same year, people filed a constitutional complaint at the Constitutional Court. In 2018, the Constitutional Court ruled unconstitutionality about 'base station investigation' on the grounds that the clause violates the principle of the proportion and infringes on the right to informational self-determination and freedom on communication.168
- 'Real-time location tracking' of mobile phone is automatically checking the location of a cellphone by every 10~30 minutes not only during the call but also in standby mode and location data of specific base station is sent by message to the investigator's mobile phone.
- The current Protection of Communications Secrets Act does not clarify who is subject to the provision of Communication Confirmation Data, and not only the suspect him/herself but also his/her family and unrelated acquaintances may be the subject for the Communication Confirmation Data.
- Activists have been indicted on charges of violating the "Assembly and Demonstration Act" because they held a "hope bus rally" to cheer on laid-off workers at the shipyard in Busan from June to Oct in 2011. After that, an investigation agency obtained the Communication Confirmation Data from Dec 2011 to April 2012. For this, a group of activists filed a constitutional complaint at the Constitutional Court. The Constitutional Court ruled unconstitutionality on the grounds that the clause violates the principle of proportion so infringes on the right to informational self-determination of and freedom of communication.169
- Investigation agency received the Communication Confirmation Data of 15 railway workers' union members, including its chairperson who had been striking against privatization of the Korea Railroad, and 21 family members of the railway workers' union members from Dec. 9 to Dec. 30 in 2013. It is revealed that the investigation agency had tracked location data of mobile phone and internet site.170 Those who were involved in the case filed a constitutional

167 CCPR/C/KOR/CO/4. para42~43.
168 the Constitutional Court, June 28, 2018, 2012Hun-ma538
169 the Constitutional Court, June 28, 2018, 2012Hun-ma191 and 550, and 2014Hun-ma357.
170 It is revealed that police officers, at that time, were tracking real-time location of not only mobile phone but also place where connecting web site. In addition, agencies received personal information of workers and

complaint at the Constitutional Court in 2014. The Constitutional Court ruled unconstitutionality on the grounds that the clause violated the principle of proportion and infringed the right to informational self-determination and freedom of communication.171

- The Constitutional Court mentioned that although the Communication Confirmation Data are metadata with unidentifiable contents, they are sensitive data because they can infer about data subjects by combining and analyzing different types of information. In addition, it was held that the location data are sensitive data and should be protected thoroughly. The Constitutional Court recommended to make tougher requirements for the request of the provision of Communication Confirmation Data.
- The government published an amendment in order to eliminate unconstitutional elements, such as 'extending period of restricting communication', 'location tracking data' and 'base station investigation', but the amendment does not have enough measures to minimize the human right violations. The amendment still puts the convenience of investigation and efficiency of law enforcement ahead of all, and leaves the possibility of human right infringements in the information society.

B. Recommendations

- An amendment for Protection Communications Secrets Act shall be made to minimize infringement of human rights in the information society by the investigation agency and abuse of authorities by powered authorities.
- It should be under control of the court by introducing the warrant requirement principle into the provision of Communication Confirmation Data. In addition, strengthened requirements should be made for confiscation, search, and verification of telecommunications already transmitted, establishing appropriate rational and supplementary grounds and specifying the rights of participation for the parties' involved in the relevant procedure.
- For the 'base station investigation', a specific provisions and strengthened requirements should be made.
- The location tracking data, especially 'real-time location tracking', has the effect of real-time wiretapping. Therefore, the type of crime for this should be limited to a crime for which an action for restricting the concerned communication has been made, and the strengthened requirements should be made.

C. Responsible ministries and agencies

- Ministry of Justice

their family members without warrant, which was personal information held by public institutions including Health Insurance Corporation.

171 The Constitutional Court ruled June 28, 2018. 2012Heonma191and 550, and 2014Heonma357.

3) Providing communication data[172]

A. Background

- Article 83(3) of the Telecommunication Business Act stipulates that the investigative agencies can obtain from telecommunication carriers information on their subscribers, including name, ID, resident registration number, address, telephone number (Communication Data) without court permission when it is necessary to identity the subject of investigation. However, this requirement remains too broad and unclear.

- The Constitutional Court has decided173 that a request for the Communication Data by an investigative agency does not qualify as a compulsory investigation. However, the Supreme Court, concerning the Naver case where Naver, an internet portal, passed its subscriber information to an investigative agency in March 2010,174 held that a telecommunications provider must provide its customer's data at the request of investigative agency if the agency satisfies procedural requirements. The Article 83(3) is, in practice, operated in such a way that a telecommunication service provider must comply with agency's request of such provision if the agency considers it necessary, for which no judicial control applies.

- Furthermore, the carrier (or the agency) does not have to notify its customers of such provision before or after the provision of the Communication Data. Therefore, the subject of investigation cannot access to basic information with which s/he can ascertain whether the collection of his/her Communication Data is a legitimate law enforcement process with the necessity and the appropriateness.

- In Korea, the situation is worsened by its national ID system called the 'resident registration number' in which a large amount of crucial personal information is combined. Thus, the resident registration number acts as a primary source of personal information. The investigative agency can obtain the resident registration number of a particular person at its own discretion, which implies that the infringement to the fundamental civil rights is worsened in Korea than other countries.

- From 2013 to 2017, average 1,034,036 cases (in relation to 9,539,337 accounts) of Communication Data were provided to the investigative agencies in each year. Since 2016, both the provision of Communication Data from the total telecommunication and from Internet has been gradually decreasing.

    - However, it should be noted that while the provision of Communication Data over the Internet is on the decline in terms of the number of documents, the number of accounts in 2017 has more than doubled from the previous year.

Communication data	In 2013		In 2014		In 2015		In 2016		In 2017	
	Numb	Num	Numb	Numb	Numb	Numb	Numb	Num	Numb	Num

172 Written by People's Solidarity for Participatory Democracy
173 Constitutional Court 2010 HONMA 439
174 Supreme Court 2012 DA 105482

provision	er of documents	ber of accounts	er of documents	er of accounts	er of documents	er of accounts	er of documents	ber of accounts	er of documents	ber of accounts
All communications	944,927	9,574,659	1,001,013	12,967,456	1,124,874	10,577,079	1,109,614	8,272,504	989,751	6,304,985
The Internet [175]	115,194	392,511	114,260	489,916	100,643	423,533	84,302	312,056	65,151	635,795
Two major companies[176]	1	17	0	0	0	0	0	0	0	0

- Annually, investigators receive, without a warrant, information on 9.5 million accounts, (18.4% of the total population).

- The National Human Rights Commission submitted the following opinions to the Constitutional Court (Constitutional Court 2016 Hunma388) on the communication data provision system: "The purpose of collecting personal information and the scope of the subject is too wide. No preliminary or post-legal control is provided, and a notification procedure does not exist, which may lead to the violation of the right to informational self-determination."

- Cases

  - In March 2010, on an online Naver cafe bulletin board, a netizen posted a video showing Kim Yu-na, a world star skater then, who appeared to avoid contact with Yoo In-chon, the Chief of the Ministry of Culture, Sports and Tourism then when he tried to hug her. The police investigated the netizen for alleged defamation of Yoo. During the investigation, the netizen learned that Naver had provided his personal information to the investigative agency without notifying him. This prompted him to file a lawsuit

175 'The internet' means "Internet, etc.", as defined by the Ministry of Science and ICT and is the sum of the communication records reported by the remaining telecommunication operators, excluding wired and mobile telephones.

176 'Two major companies' refers to Naver and Kakao, two online service providers in Korea that provided a transparency report. After a subordinate ruling by Seoul High Court on Oct. 18, 2012 (Decision of 2011 NA 19012), the companies were ordered to compensate customers for providing customer information to investigative agencies. From 2013, major portal companies ceased providing such information. Although the Supreme Court later overturned the ruling on March 10, 2016 (Decision 2012DA105482), Naver and Kakao have not responded to requests from investigative agencies for communication data. As these service providers have ceased the provision of communication data, it can be assumed that such data is provided primarily by Internet Service Providers.

against Naver, and although the first trial was rejected, an appeals court177 acknowledged that Naver was liable for the damages of 500,000 Korean won for violating the plaintiff's right to informational self-determination and anonymity, and for failing to protect the user's personal information. Since that ruling in October 2012, major internet companies (e.g. Naver, DAUM, SK Telecom and Kakao) have not provided any telecommunications data to investigators without a court order.

- In April 2013, a lawsuit against three telecommunication companies were filed by their users for the provision of their Communication Data to an investigative agency and for not responding to their requests of disclosing information in relation to the provision. The users claimed for the disclosure of relevant information and damages. In the first trial, the court ordered the telecommunications companies to disclose the information while rejecting the claim for damages, which too later admitted by an appeal court.178 The appellate court declared that it is not permissible to limit the right to informational self-determination according to the Constitution, nor is it permissible to claim vague legal circumstances that argue that the failure to provide such information would interfere with the investigation.

- Further, the refusal of telecommunications companies to comply with the plaintiffs' disclosure request for an extended period of time is an illegal act that infringes on the right to informational self-determination. While the telecommunications companies appealed the ruling, the Supreme Court dismissed their appeal on July 20, 2018.

    - In March 2016, it was found that investigators collected the Communication Data for a number of people, including lawmakers and union members, who opposed the enactment of the Anti-Terrorism Act. Civil society groups have used campaigns to urge citizens to check whether their communication data is being collected. This eventually led to more than 500 citizens, who had confirmed their data was collected, filing a constitutional petition under the Article 83(3). As of today, the petition remains in progress.

B. Recommendations

- To amend the Telecommunications Business Act so that investigative agencies cannot collect unlimited personal information without a court order
- Completely abolish the communication data provision system that enables investigative agencies to collect information of telecommunication users without warrants
- To implement measures to improve rights to informational self-determination by rectifying the reality of prioritizing the convenience of investigative agencies activities

C. Responsible ministries and agencies

177 Seoul High Court 2011 Na 19012
178 Seoul High Court 2014 NA 2020811

- Ministry of Justice, Korea Communications Commission, Ministry of Science and ICT

4) Digital information search and seizure[179]

A. Background

- Ensuring the confidentiality of communication contents is fundamental and central to the privacy of an individual. However, under the current criminal procedural law, e-mails that have been sent and received are classified as “goods” and are subject to general confiscation procedures. If a computer server or laptop is seized for a certain length of time, then any contents communicated may be unprotected and exposed. Such actions by investigative agencies have brought a criticism, especially when emails from seized devices have been used as evidence of guilt.
- The case of PD Notebook, a television program, where, the email records of its staffs were searched and seizure, shows such problems:
    - On April 29, 2008, when massive candlelight protests were commenced against the Lee Myung-bak administration’s increase in US beef imports, the PD Notebook broadcasted, "Emergency reporting: US beef. Is it safe from mad cow disease?". The Lee Myung-bak administration claimed that the PD Notebook was the controller behind the large-scale protests and accused its producers of defamation of the government (Ministry of Food, Agriculture, Forestry and Fisheries). During the case, the prosecution not only searched for emails without prior notice, but also disclosed the results of the investigation, as well as personal emails, and claimed this as evidence of guilt. It had been reported that the prosecution had looked at private email conversations that were beyond the scope of the criminal charges.
- In August 2010, the National Human Rights Commission of Korea (NHRCK) advised the National Assembly Chairman on amending the criminal procedure law: "It is advisable to legislate the grounds and procedures for the seizure of e-mails stored in telecommunication carriers, and that the scope must be specified in relation to the criminal charges when searching for confiscation."180
- There are many indications that it was possible to collect massive amounts of digital information, leading to multiple chances for infringing on people’s privacy through the gathering of irrelevant information. Cases involving the Korean Teachers and Education Workers' Union (KTU) and the Sewol Ferry Disaster, where the investigative agencies opened new investigations based on information gathered from search and seizures, were controversial.
    - In June 2009, the KTU issued a state declaration demanding the suspension of media legislation and denounced the Grand Canal Project. The prosecution issued a warrant for the seizure of equipment in the KTU office and while executing the warrant, seized three desktop computers and ten server computers at the KTU headquarters in Seoul. At this time, based on the information obtained from the seized computers, the prosecution expanded the scope of its investigation to teachers who had sponsored or

179 Written by People’s Solidarity for Participatory Democracy
180 National Human Rights Commission, Aug. 18, 2010.

paid KRW5,000 ~ 20,000 per month in membership dues to the Democratic Labor Party. Subsequently, the teachers of the KTU were charged with a violation of the Political Parties Act and Political Funds Act.

- The KTU countered that the prosecution's seizure procedure went beyond that which was stipulated in the warrant. The Supreme Court clarified that the seizure of electronic information should be executed only according to that which is specifically printed in the warrant as it relates to the allegations and to the site of seizure. Further, the removal of data storage devices from the site is permitted only in exceptional cases as specified in the warrant.
- Since July 2011, the Criminal Procedure Law has been amended to include a new provision regarding information storage media, specifically setting out that the seizure of data storage devices should be executed by copying it in principle.181
- In July 2014, the police investigated 76 members of the KTU on allegations of leading the making of a declaration related to the Sewol Ferry Disaster. The police executed an emergency search of the KTU's servers in Seocho-dong, Seoul. While the warrant was limited to 'homepage server data' and 'records of the KTU e-mail accounts stored on the server', during the police's investigation, it is known that e-mails containing private conversations and the seized records of Naver Band conversations were included in the search. The e-mail and the Band records search and seizure conducted by investigators included conversation records and content that were beyond the scope of the criminal allegations. There was a criticism that the police could examine the conversations of those not under investigation, actions that seriously infringed on privacy rights.

- On July 16, 2015, the Supreme Court182 confirmed the principle of electronic information seizure by declaring that during searches, if crimes are found to have been committed that weren't previously uncovered, then investigators must obtain a warrant pertaining to those crimes.

---

181 Article 106 (Seizure) (1) If necessary, a court may seize any articles thought to be used as evidence or liable to confiscation, only when such articles are deemed to be connected with the accused case: Provided, That the same shall not apply where otherwise provided in Acts. <Amended by Act No. 10864, Jul. 18, 2011> (2) A court may designate articles to be seized and order the owner, possessor, or custodian thereof to produce such articles. (3) Where the object to be seized is a computer disc or other data storage medium similar thereto (hereafter referred to as "data storage medium or such" in this paragraph), the court shall require it should be submitted after the data therein are printed out or it is copied within the specified scope of the data stored: Provided, That the data storage medium or such may be seized, when it is deemed substantially impossible to print out or copy the specified scope of the data or deemed substantially impracticable to accomplish the purpose of seizure. <Newly Inserted by Act No. 10864, Jul. 18, 2011>

182 Supreme Court, July 16, 2015. 2011 MO 1839 decision. "In principle, the search for electronic information by an investigating agency should be conducted by copying the files to a storage medium carried by the investigating agency or by collecting the printout of only those parts related to the criminal allegation for which the warrant was issued. It is only permissible in exceptional cases to export the storage medium itself or to retrieve all of the electronic files contained in the storage medium by removing it from the site. If it may require an extended period to obtain relevant information or if it is not possible to set the scope and print or copy, or when it is recognized as being extremely difficult to achieve the purpose of seizure, only then in such cases is an exception allowed."

- Other cases
    - In 2008, during the prosecutors' investigation of Ju Kyung-bok, a candidate for the Seoul Superintendent of Education and a professor of Konkuk University, for potential election law violations, it searched his e-mail he communicated for seven years and seized contents without providing prior notice to the suspect. Only during the trial did Ju learn about this.
    - In 2009, Park Rae-Gun, co-executive chairman of the Justice for Yongsan Evictees, had email records seized related to his conversations about his defense with his lawyer.
    - In 2009, the police seized nine-months' worth of company e-mail records from 20 YTN union members who were under investigation for charges of business disruption. It had included meeting documents of media trade unions and accounting records unrelated to the allegations. As the members never received notice, they were unaware of the seizure until more than three months after it had taken place.
    - Seizure of Naver Band or KakaoTalk chat room records may result through surveillance techniques, including real-time eavesdropping. Nevertheless, this is done in accordance with the provision of confiscation under the Criminal Procedure Code. These seizures are much more intrusive than general types of seizures.

B. Recommendation

- The search and seizure of electronic information by a general warrant under the Criminal Procedure Act is contrary to the principle of proportionality, and the extent of the invasion of privacy and communication is severe. These points should be taken into consideration and improvements should be made on the relevant regulations.

C. Responsible ministries and agencies

- Ministry of Justice

3. Resident Registration System

1) Resident Registration Number System[183]

A. Background

- All Korean citizens are given a unique national identification number, called the resident registration number ("RRN") from birth. The RRN is made up 13 digits, composed of date at birth for the first digits and rear seven digits including sex, birthplace, order of birth registration in that day, and error verification number. In principle, a RRN cannot be changed for life once it is granted.
- The RRN has been collected for personal identification in various public and private areas. Therefore, the RRN can be a key to connect information from different databases. Under these circumstances, massive personal information leaks, including the RRN, have caused significant damage. For example, RRNs were leaked from the following companies.
    - 18 million cases leaked in 2008 from Auction
    - 35 million cases leaked in 2011from SK Coms Nate, Cyworld
    - 13 million cases leaked in 2011 from Nexon 'Maple Story'
    - 114 million cases leaked in 2014 from Lotte Card, NH Card, and KB Card
    - 10.3 million cases leaked in 2016 from Interpark,
- 1st UPR (2008) made recommendations to limit the uses of RRN only for the necessary purpose of public interests.184
- In order to limit excessive collecting of RRN, it has been prohibited from collecting RRN online since August 2012 due to the revision of 'Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.' and from August 7, 2014, it is prohibited from collecting RRN unless the 'Personal Information Protection Act' allows them to do.
- On August 8, 2014, the National Human Rights Commission of Korea (NHRC) recommended that the speaker of the National Assembly and Prime Minister make a fundamental reform of the RRN system.185 NHRC, at that time, also recommended limiting the uses of RRN to administrative affairs related to RRN only. In other areas, it was recommended to use a unique purpose-specific number in the area, change the RRN and change the RRN system to a random number that does not include personal information.
- The Constitutional Court ruled that not allowing the change of RRN itself violates the right to informational self-determination, and ruled the unconstitutionality of the current Resident Registration Act on December 23, 2015. At the same time, the Constitutional Court recommended that the Resident Registration Act be revised by December 31, 2017.186
- There are three problems of the resident registration number system. First of all, the RRN is

183 Written by Korean Progressive Network Jinbonet
184 A/HRC/8/40, para 64.13
185 National Human Rights Commission of Korea, Recommendation for improvement of RRN system, May 8, 2014.
186 the Constitutional Court, December 31, 2015, 2014Hun-ma449 and 2013Hun-ma68

excessively collected from overall private and public areas, so it can be the foundation for the integration of different personal information and tracking or profiling of individuals. Secondly, the RRN cannot be changed in principle, and as a result, it can cause potential damage from leaking RRNs. Finally, because the RRN including birth date, sex, the place of birth, etc., personal information can be exposed even if data subjects do not want that and used as a basis for discrimination.

- In order to restrict the collection of personal information, RRNs were not allowed to be collected without a basis in the Act from August 2014, but still, many laws permit the collection of RRNs. According to the data released by Ministry of Security and Public Administration (currently, it is Ministry of the Interior and Safety) in January 2014, 866 statutes permit the collection of RRNs, and also collects RRNs in the financial and telecommunication sectors, which are private sectors. Additionally, in some cases, RRNs are collected based on forms, not laws or enforcement ordinances.
- In December 2015, following the Constitutional Court's decision of constitutional inconformity, the National Assembly passed a revision bill to the Resident Registration Act on May 19, 2016, which allowed people to change their resident registration numbers.187 However, such changes are allowed to only those who have been suffered with or are likely to suffer with damages such as life, body, property, or sexual violence due to the leakage. In reality, it is difficult to prove the direct damage caused by the leak of RRNs. In addition, since only the rear 6 digits of the 13 digits of RRN is allowed to be changed, and the new RRN still contains information on birth and sex, from which the entire RRN can be retrieved. In response, the head of the NHRC issued a statement expressing regret over the limited change, demanding the introduction of an objective number and random number.188
- Personal information is unintentionally exposed on RRNs, because it includes information on birth date, sex, and place of birth, so it could encourage discrimination by age, sex, and region. In addition, the RRNs can be chased from personal information.
    - A research from the Seoul National University of Science & Technology in 2014 shows that, by using personal information of Facebook, RRN of 45% of 115,615 cases were obtained.189
    - Research from Harvard University in 2015: The RRNs of Korean, which sold to IMS Health in the U.S. succeeded in identifying 23,163 cases by using a model of the RRN system. "it was easy thanks to the data of birth, sex, region, and a verification

187 Joint Statement of Civil Society Organizations (2016) Joint Statement of Social Organizations on the 19th National Assembly Passed Resident Registration Act - Improve RRN that ended incomplete, so change them in the 20th National Assembly! http://act.jinbo.net/wp/9538/ [14 May 2019].
188 National Human Right Commission of Korea (2016). Chairman's statement on the approval of a bill to revise part of <Resident Registration Act>
https://www.humanrights.go.kr/site/program/board/basicboard/view?&boardtypeid=24&currentpage=55&menuid=001004002001&pagesize=10&boardid=611785 [14 May 2019].
189 Channel A. (2014). [Single] If You Type the Address in the Facebook, You Will See Your Resident Registration Number!
http://www.ichannela.com/news/main/news_detailPage.do?publishId=61503088-1 [14 May 2019].

number."190

- ❍ According to the 2009 recognition survey, 77.2% of the people said that they were concerned because they were exposed to information about their sex and data of birth even though they did not want to be known through their resident numbers.191
- ❍ The sex of the RRN is only divided between male and female, the number for males is 1 (the person born after 2000 is 3) and the number for females is 2 (the person born after 2000 in 4) which is criticized as reflecting the perception of male dominance and is a factor that discriminates against sexual minorities.

- Despite recommendation made by the NHRC in 2014, the Ministry of the Interior and Safety, which is in charge of the matter, has not yet been willing to change the RRN system to a random number system.

B. Recommendations

- The collection and uses of resident registration numbers should be based on the status, not the form.
- The uses of resident registration number should be strictly limited for administrative and judicial purposes, and in other areas of the public sector, a separate identification number (e.g., a tax number) unique to that purpose is used.
- To prevent identification number in different fields from being linked to RRNs without the basis of the law.
- Change the RRN to a random number system that does not include personal information.
- The RRN can be changed as long as the relevant requirements are met.

C. Responsible ministries and agencies

- Department of Resident in the Ministry of Interior and Safety
- Prime Minister

2) Compulsory Fingerprinting System[192]

A. Background

- Fingerprints are unique biometric information to everyone and need to be protected as sensitive information, which is requiring special protection.
- The fingerprinting system was introduced in Korea in 1968 with the issuance of a resident

190 Hankyoreh. (2019). [Single] The Risk of Big Data in the Welfare Department…It Can be Solved Even If Personal Information Is Encrypted. http://www.hani.co.kr/arti/society/society_general/762609.html [14 May 2019].
191 Kim, Min Ho et al. 2009. A Study on the Improvement of the resident registration number system. National Competitiveness Council.
192 Written by Korean Progressive Network Jinbonet

registration card, and all Koreans over the age of 17 have the fingerprinting of their fingers. Currently, fingerprints of all citizens are electronically managed and used by the National Police Agency for investigation purposes through the Automated Fingerprint Identification System (AFIS). The Ministry of Interior and Safety has thumbprint information and uses it for identification purpose.

- Forcing the fingerprinting of all Koreans aged 17 or older to be used for criminal investigation purposes is treating the entire nation as a potential criminal.
- In 1999, activists from social organizations filed a constitutional complaint at the Constitutional Court against the police's collection of information on the thumbprints of citizens aged 17 and over, and the establishment and operation of the database system. In 2004, three teenagers who reached the age of 17 filed a complaint with the intention that the fingerprinting system of the country is unconstitutional. However, the Constitutional Court rejected this in 2005 on the grounds that Police Act and Act on the Performance of Duties by Police Officers include "collection, preparation, and distribution of information on public security (Article2, 4)" as one of the duties.193 In 2011, the objectors again filed a complaint with the Constitutional Court, but for the same reason it was decided as constitutional.

B. Recommendation

- Encouraging the abolition of the compulsory fingerprinting system.

C. Responsible ministries and agencies

- Department of Resident in the Ministry of Interior and Safety

3) Identity Verification Agency System[194]

A. Background

- In response to the repeated incidents of massive-scale data breaches, the government has banned the collection of resident registration numbers (RRNs), which are the main target of the data breaches, through the information and communications network since 2012. However, the identity verification agencies under the Information and Communications Network Act195 still has the authority to collect RRNs.
- Many laws requiring identity verification stipulate to use the identification methods provided by the identity verification agencies. Therefore, Internet companies with identification obligations under such laws including the Juvenile Protection Act, the Public Official Election Act, and the Game Industry Promotion Act had to use the identity verification under the Information and

193 the Constitutional Court, May 26. 2005. 99Hun-ma513, etc.
194 Written by Open Net Korea
195 Article 23-2 (Restrictions on the Use of Resident Registration Numbers) (1) An information and communication service provider shall not collect or use the resident registration number of the user unless it falls under any of the following subparagraphs:
1. If you are designated as your identity verification body pursuant to Article 23-3

Communications Network Act. Moreover, as the identification methods stipulated by enforcement decrees are very limited, and Internet companies had to rely on identity verification services provided by telecoms, which are the only universal method of identification.

- ❍ The identification service market is monopolized by the telecoms providing the SMS identification service. According to data MP Choi Myeonggil obtained from the Korea Communications Commission, three major telecoms' revenue from the identification service was 25.8 billion won for just one year in 2015.

- The purpose of adopting the identity verification agency system was to encourage the agencies to develop identification methods that could replace the RRN system. However, major three telecoms that collect RRNs of mobile phone subscribers are all designated as identify verification agencies. Consequently, telecoms' identification service is practically the same as identification based on mobile RRN system because they can exactly match a mobile phone number to the mobile phone user's RRN.
- In March 2014, one of the major three telecom KT (Korea Telecom) was hacked and RRNs and other personal information of 12 million users were stolen. Such a massive leak occurred because KT is allowed to collect RRNs as an identity verification agency.
- Moreover, telecoms are required to keep a record of their users' identification transactions online. It means that they have logs of websites such as sites with age restriction that users visited, which are private information. If the telecoms are allowed to keep accumulating those private data, they will be able to profile users' preferences, and one day might become big brothers.
- In June 2014, Open Net Korea filed a constitutional complaint at the Constitutional Court against the identity verification agency system because the system infringes on the citizen's right to informational self-determination.

B. Recommendation

- Abolish the identity verification agency system under the Information and Communications Network Act that compels certain companies to collect resident registration numbers and sensitive information about subscribers

C. Responsible ministries and agencies

- Korea Communications Commission

4) Connecting Information (CI)[196]

A. Background

- Connecting Information (hereafter "CI") means information encrypted with 88 bytes as a co-

196 Written by Korean Progressive Network Jinbonet

identifier of the website for service linkage. Online identification service institutions generate CI based on a resident registration number (hereafter “RRN”) and it is used to identify customers when providing affiliated services between websites.

- It means that CI is pseudonymized RRN information. Because CI can be matched one by one, so it can make recognize person anywhere in online like ‘online resident registration number’.
- Problems regarding the collection and utilization of RRN have occurred continuously as all administrative services and private companies have been identified by their RRN. As a result of continuous problem raising, CI was introduced as a means of verifying identity online instead of RRN, as the Act was amended to allow the collection and utilization of RRN only if they were limited.
- However, major Korean Internet companies have been not only requesting users to identify more than they need, but also using CI for comprehensive consent through the terms and conditions of use, taking advantage of the loopholes in the law because CI is not protected as much as RRN. Also, investigative agencies have used CI to track online activities for specific user.
- Eventually, through CI linked to the RRN, individuals’ on- and off-line activities will not only be put in a state where they can be tracked intact but will also have an adverse impact on the freedom of online expression a based on anonymity.
- System of identification by using CI is directly linking to the Internet real-name system. In other words, even though there is a way to identify each user without having to authenticate themselves in an online environment based on anonymity, and to block or punish each user in case of a problem, such as a crime, by verifying the user’s real name, thereby creating a chilling effects that restricts the user’s right to speak.
- The Constitutional Court197 ruled that allowing users of bulletin board only after a personal identification procedure violates the freedom of expression of Internet bulletin board users, the right to personal information self-determination, and the freedom of the press of information and communication service providers running Internet bulletin boards.
- Although the actual CI is encrypted and cannot be identified by the CI alone, the combination of phone numbers, names and mobile phone numbers makes it possible to identify individuals, such as RRN.
- On February 14, 2019, the Ministry of science and ICT issued a temporary permit to <administrative and public institution’s mobile electronic notice service based on messengers and text messages> which was applied by Kakao Pay and KT for its first ICT regulated sandbox project based on the “Special Act on Promotion of Information Communication and Promotion of Convergence”. Through this measure, it is allowed to convert RRN into CI for mobile electronic notification by administrative and public institutions.
- In order for public institutions to handle RRN, “it should be a business of state with grounds to specifically demand or permit to processing of RRN under the law”198. However, the administration that carried out the notification by consent, such as text message, or e-mails, argues that the CI-based notification is needed to track and alert people everywhere in the

197 the Constitutional Court, August 23, 2012, 2010Hun-ma47 and 252
198 Personal Information Protection Act, Article 24.

country because the phone numbers and e-mail addresses of the people change frequently. However, ‘Alert-Talk Service’ which government wants to use, is malformed structure of service that could be realized only in S.Korea where a national identification number is collected and utilized universally in private and public sectors. Continuing to keep track of people’s online activity through CI is an abuse of administrative power.

- It is a clear violation of the right to informational self-determination that the government is actively engaged in utilizing the services of certain companies to utilize RRN, which are sensitive personal information.

B. Recommendations

- Identification service agency designating regulation of the Information and Communications Network Act should be abolished, and also CI as an online RRN should be abolished too.
- Unnecessary identification in online is violating the right to informational self-determination. Therefore, it is necessary to lead the personal information supervisory body so that unnecessary identification is not obtained.

C. Responsible ministries and agencies

- Ministry of Science and ICT
- Korea Communications Commission
- Personal Information Protection Committee

4. Anonymity of Communication[199]

1) Mobile Phone Real-name System

A. Background

- Article 32-4 of the Telecommunications Business Act200 introduced in October 2014 provide for the “mobile phone real-name system” that requires a telecommunications business operator to verify whether the other party is the principal when entering into a contract for the provision of telecommunications services. In other words, a telecom must verify the identity of a potential subscriber when signing the mobile phone contract, and the telecom may refuse to sign the contract if the person is found to be a different person or he/she refuses such identification.
- Mobile phone real-name system infringes on users’ freedom of anonymous communication, right to privacy, and right to informational self-determination. Open Net filed a constitutional complaint in November 2017 and the case is currently pending at the Constitutional Court.
    - ❍ Infringement of the Freedom of Anonymous Communication: The Constitutional Court had confirmed that the freedom of expression also protects anonymous expression. In the same vein, the freedom of communication protects not only the content of communication but also all details of communication such as the parties to the communication (sender and recipient), destination and origin, the number of transmissions, etc., and this includes the freedom of anonymous communication, which is freedom to communicate anonymously with the counterparty and third parties. The mobile phone real-name system obviously infringes on the freedom of anonymous communication since it makes anonymous communication totally impossible.
    - ❍ Infringement of Privacy: Today, because all communications and expressions online are recorded, it is very easy for the state to monitor and track. At the same time, the mobile phone real-name system mandatorily connects all communication devices to the actual identity of users and greatly increases the risk to privacy not only by the state but also by companies and individuals.

199 Written by Open Net Korea

200 Article 32-4 (Avoidance of fraudulent use of mobile communication devices) ① omitted
② In entering into a contract for the provision of telecommunications services (including contracts concluded through agents and consignees that enter into contracts for the provision of telecommunications services on behalf of, or outsourced by, telecommunications business operators), a telecommunications business operator prescribed by Presidential Decree, taking into account the type of telecommunications services, scale of business, protection of users, etc. shall, with the consent of the counterparty to the contract, verify whether the counterparty is the principal by utilizing illegal subscription prevention system, etc. referred to in Article 32-5 (1), and may reject a contract if the relevant person is not the principal or refuses to verify whether he/she is the principal. Where the user who is the principal is changed for a ground for the transfer of telecommunications services provided or the succession to the user's position, etc., the same shall also apply to a person who intends to obtain the telecommunications services according to such change.
③ In verifying the principal prescribed in paragraph (2), a telecommunications business operator may request the counterparty to the contract to present a certificate or document, such as a resident registration certificate or driver's license, through which the relevant person can be verified as the principal.
④ Matters necessary for the methods of verification of the principal prescribed in paragraph (2) and the type, etc. of certificates and documents through which the relevant person can be verified as the principal prescribed in paragraph (3) shall be prescribed by Presidential Decree.

- ❍ Infringement of the Right to Informational Self-determination: The mobile phone real-name system compels telecoms to check, collect, and store identifying information of a user such as the name, the resident registration number, and the address. This infringes on the user's right to informational self-determination since the identification information is personal information as it allows to identify an individual.

- Mobile phone real-name system increases the risk of a data breach including hacking due to excessive accumulation of personal information, and in fact, a massive-scale data breach occurs almost every year. In particular, although telecoms have been the source of such data breach several times, the mobile phone real-name system gives telecoms broader collection authority, rather than limiting the authority.

B. Recommendation

- Abolish the mobile phone real-name system that infringes on the freedom of anonymous communication, the right to privacy, and the right to informational self-determination.

C. Responsible ministries and agencies

- Ministry of Science and ICT

2) Internet Real-name System: the Public Official Election Act, the Juvenile Protection Act, the Game Industry Promotion Act

2-1) Real-name System under the Public Official Election Act

A. Background

- Article 82-6 of the Public Official Election Act201 states that any Internet press agency allowing posting of information including texts, voice, pictures or video clips expressing support for or opposition to candidates or political parties on its website during the election campaign period must check the real name of the poster. It lists the identity verification system under the Information and Communications Act as an identification method.

- Internet portals such as Naver are also considered as Internet press agencies. And the provision imposes the identification obligation on any internet press agency that "allows" anyone to post

201 Article 82-6 (Identification of Real Names on Bulletin Boards or Chatting Pages, etc. of Internet Press Agencies) ① If any Internet press agency allows anyone to post information (hereafter in this Article referred to as "information, etc.") including texts, voice, pictures or video clips expressing his/her support for or opposition to candidates or political parties on the bulletin board and chatting page, etc., of its Internet web-site during the election campaign period, it shall take technical measures to have his/her real name identified in the methods of identifying real names that are provided by the Minister of the Interior and Safety or credit information business operator (hereinafter in this Article "credit information business operator") under subparagraph 4 of Article 2 of the Credit Information Use and Protection Act: Provided, That where the Internet press agency has taken measures to identify the person himself/herself pursuant to Article 44-5 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., it shall be deemed that the technical measures to have the real name identified have been taken.

information expressing his/her support for or opposition to candidates or political parties. Virtually, the law applies on all news websites providing any feature that allows anyone to post any information because there's a "possibility" that anyone might post his/her support or opposition.

- This system infringes on the freedom of anonymous expression as well as the freedom of anonymous communication.

B. Recommendation

- Abolish the real-name system under the Public Official Election Act that infringes on the freedom of anonymous communication.

C. Responsible ministries and agencies

- National Election Commission

2-2) Real-name System under the Juvenile Protection Act

A. Background

- Article 16 of the Juvenile Protection Act202, which came into force on September 16, 2012, imposes an obligation of "identity verification" in addition to "age verification" on those who want to provide harmful media products.
- Identity verification of all people including juveniles and adults on top of age verification of those who want to access harmful media infringes on the freedom of anonymous communication, right to informational self-determination, freedom of anonymous expression, and the right to know.
    - ❍ In particular, in order to verify the identity of a person, those verification agencies should always keep users' personal information. If such personal information and identification transaction records generated from identification requests are accumulated in identity verification agencies, the risk of data breach inevitably increases.
- In May 2013, Open Net Korea filed a constitutional complaint at the Constitutional Court against the provision.

B. Recommendation

- Abolish the real-name system under the Juvenile Protection Act that infringes on the freedom of

202 Article 16 (Prohibition of Sale, etc.) ① A person who intends to sell, lend, or distribute a media product specified by Presidential Decree as harmful to juveniles to a person or provide such product to a person for viewing, watching, or using shall verify the age and identity of the other party and shall not sell, lend, or distribute such product to a juvenile or provide such product to a juvenile for viewing, watching, or use.

anonymous communication and the right to informational self-determination.

C. Responsible ministries and agencies

- Ministry of Gender Equality and Family

2-3) Real-name System under the Game Industry Promotion Act

A. Background

- Article 12-3 of the Game Industry Promotion Act203, which came into force on September 16, 2012, requires online game companies to verify the identity of users and obtain consent from the parents if the user is a minor (under 18 years old) in order to prevent excessive immersion in or addiction to games.
- Identity verification of all people including juveniles and adults when signing up for online games infringes on the freedom of anonymous communication, right to informational self-determination, and the freedom of anonymous expression.
    - ❍ In particular, in order to verify the identity of a person, the verification agency must keep users' personal information at all times. If such personal information and identification transaction records generated from verification requests are accumulated in identity verification agencies, the risk of data breach inevitably increases.
- In July 2013, Open Net Korea filed a constitutional complaint at the Constitutional Court against the provision.

B. Recommendation

- Abolish the real-name system under the Game Industry Promotion Act that infringes on the freedom of anonymous communication and the right to informational self-determination.

---

203 Article 12-3 (Prevention Measures against Excessive Immersion in and Addiction to Games, etc.) ① In order to prevent excessive immersion in or addiction to games by users of game products, game products related business entities [limited to service providers making game products available to the public through the information and communications network defined in Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. (hereinafter referred to as "information and communications network"): hereafter the same shall apply in this Article] shall take measures to prevent an excessive use of game products including the following (hereinafter referred to as "preventative measures"):
1. Verification of real names and ages of users of game products when they join as members and self-authentication;
2. Securing the consent of legal representatives, such as persons having parental authority, when juveniles join as members;
3.-7. omitted.

C. Responsible ministries and agencies

- Ministry of Culture, Sports and Tourism

5. Personal Data Protection

1) Big Data Legislation for Personal Data Protection[204]

A. Background

- In the name of vitalizing the big data industry, the government is infringing on the right to informational self-determination by allowing companies to use personal data for commercial purposes without the consent of a data subject.
- On June 2016, ministries of Park Geun-hye government (The Office for Government Policy Coordination, the Ministry of Administration and Home Affairs, the Korea Communications Commission, the Financial Services Commission, the Ministry of Science, ICT and Future Planning, the Ministry of Health and Welfare) jointly published the <personal information de-identification guideline>. According to the guideline, if personal data is de-identified by using measures in accordance with the guideline, it is "assumed that it is not personal information" so that it can be used for purposes other than the original purpose of its collection without the consent of the data subject. In addition, the Korea Internet & Security Agency (KISA) and other public institutions are designated as specialized agencies to support the combination of de-identified personal data from different companies and provide combined (de-identified) personal data to the original data controllers.
- According to the 2017 parliamentary inspection of the administration, about 340 million cases of data from private companies were combined on 26 occasions between August 2016 and September 2017 following the guideline. The data subject has not been informed whether his or her personal data has been used for the combination, nor has he or she been answered for requesting access rights from the company.
- On November 9, 2017, the civil society organizations filed a complaint against four de-identification specialized agencies and 20 companies on charges of violating the Personal Information Protection Act, but the prosecution has not indicted them without charge on March 25, 2019.
- In the Moon Jae-in government, the government proposed the amendment of Personal Data Protection Act to the national assembly through a ruling party lawmaker, In Jae-geun, on November 15, 2018. The amendment allows the use of pseudonymized personal data or providing them to third parties for statistical and scientific research purposes beyond the original purpose of collection without the consent of data subject (Article 28-2). But here, scientific research involves the internal R&D of the companies, including the development of new technologies, products, and services. In addition, similar to the <Personal Data De-Identification Guideline>, the amendment allows the pseudonymized personal data from different companies to be combined through designated specialized agencies and combined pseudonymized or anonymized personal data to be provided to the original data controllers or third parties (Article 28-3). As regards pseudonymized personal data, the rights of the data subject such as access right, storage limitation, and leakage notice are limited.
- Korean civil society criticizes the government's amendment of the Personal Information Protection Act that it infringes on the right to personal data of a consumer (user) by allowing

204 Written by Korean Progressive Network Jinbonet

companies to sell, share and combine (pseudonymized) personal data without the consent of data subject.

- The government's proposed amendment to the Credit Information Use and Protection Act (as proposed by a ruling party lawmaker, Kim Byung-wook on November 15, 2018) allows not only the use of personal credit information without the consent of data subject for commercial research purposes by businesses when that personal information is pseudonymized, but also the collection and use of SNS information for credit evaluation purposes without the consent of data subject. SNS information should not be freely used by anyone regardless of the intention of the data subject simply because it is publicly available personal information. The use of SNS information in credit rating may cause a chilling effect on the user's freedom of expression through SNS.

B. Recommendations

- The utilization of pseudonymized personal data without consent should be limited to scientific research that may strengthen the scientific domain of society, and not be sold, shared or combined among companies merely for their internal research. Even if personal data is provided for scientific research purposes, sufficient safeguard should be prepared, such as anonymization if applicable, and the right of the data subject should be guaranteed unless it hinders the achievement of the purpose.
- The amendments from the government of the Personal Information Protection Act and the Credit Information Use and Protection Act, which are focused only on the economic use of big data, should be scrapped, and a personal information protection system should be prepared at least compatible with the EU GDPR.

C. Responsible ministries and agencies

- the Ministry of the Interior and Safety (former the Ministry of Administration and Home Affairs)
- the Korea Communications Commission
- the Financial Services Commission
- the Personal Information Protection Commission

2) Data Protection Authority[205]

A. Background

- The U.N. <Guidelines for the Regulation of Computerized Personal Data Files> (1990) requires all countries to set up an independent authority to be responsible for supervising the observance of the principles set forth in the guideline. In addition, <Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding

205 Written by Korean Progressive Network Jinbonet

supervisory authorities and transborder data flows>(2001) adopted by the Council of Europe specifies the specific authority of the data protection supervisory authorities, such as powers of investigation and intervention, the power to engage in legal proceedings, etc.

- In S.Korea, the legislation for personal information protection is divided into the Personal Information Protection Act, the Network Act, and the Credit Information Use and Protection Act etc, while the data protection supervisory authority is also divided into the Ministry of the Interior and Safety, the Korea Communications Commission, the Financial Services Commission, and the Personal Information Protection Commission. The Ministry of the Interior and Safety has no independence as a government ministry, and the Korea Communications Commission and the Financial Services Commission are implementing policies to ease personal information protection under the pretext of fostering the big data industry. The Personal Information Protection Commission does not have the independence of personnel and budget, nor does it have the executive power as a supervisory body, such as the power to investigate and take corrective action. In addition, the dispersed supervisory system hinders the implementation of a unified privacy policy and efficient supervision.
- The government proposed amendment of the Personal Information Protection Act on November 15, 2018, unifies the supervisory authority of the Ministry of the Interior and Safety and the Korea Communications Commission into the Personal Information Protection Commission, which is the welcome move. However, the supervisory authority of the Financial Services Commission is still remains, and the independence of the Personal Information Protection Commission is limited, given that the amendment excludes the prime minister's right to direct and supervise only for some of the authority of the Personal Information Protection Committee (investigation and disposition of rights violations, dispute settlement) and that the prime minister can still exercise the right to direct and supervise important functions of the commission, such as improvement of laws related to personal information protection, establishment and implementation of a policy and plan on data protection, etc.

B. Recommendations

- The data protection authority should be streamlined into the Personal Information Protection Committee and assured of full independence.

C. Responsible ministries and agencies

- the Ministry of the Interior and Safety (former the Ministry of Administration and Home Affairs)
- the Korea Communications Commission
- the Financial Services Commission
- the Personal Information Protection Commission

3) Customers' Personal Information - Homeplus Case[206]

A. Background

- Homeplus collected about 7.12 million consumers' personal information for the purpose of selling it to the insurance companies and did not notify consumers of the provision. And Homeplus wrote the personal information consent category in 1mm size to prevent consumers from actually reading it. Also, consumers cannot but agree on unnecessary personal information such as date of birth and number of children.
- Meanwhile, Homeplus handed over personal information to the insurance companies without consent from consumers. The insurance companies filtered the information and selected only those who are likely to sign insurance contracts. After obtaining the consent of the provision from those selected consumers, Homeplus handed it over again to the insurance companies.
- In a damages suit filed by the Korean National Council of Consumer Organizations with 683 consumers to the defendant Homeplus, Lina Life Insurance and Shinhan Life Insurance, the appeals court sentenced that Homeplus violated Personal Information Protection Act, Display Advertisement Act, etc., by engaging in deceiving advertising activities such as offering prizes as part of the customer appreciation event, writing the purpose of collecting and using personal information in small letters measuring about 1mm in size, and collecting unnecessary personal information out of purpose. Since it is recognized that the victims suffered mental distress due to such illegal activities by Homeplus, the court ordered Homeplus to pay 200,000 won by a person in compensation. Also, the act of Homeplus providing personal information to the insurance companies violated the Personal Information Protection Act. Members of the Homeplus family card have felt the anxiety that their personal information could be learned by a third party or the displeasure that they were treated as targets of for-profit activities by using it for business, so the court ordered Homeplus and the insurance companies jointly pay 50,000 won by a person in compensation for mental damage.
- In the meantime, the court believed that consumers were responsible for the burden of proof that their personal information had been provided to the insurance companies. The request of 222 plaintiffs which is not clear that personal information was provided in the criminal procedure, was rejected as the victim of the illegal act unless the consumers can prove it. Appeals procedures are currently underway for 222 plaintiffs.
- In the absence of a class action suit system, consumers may file a claim for damages under the Civil Procedure Act. However, only consumers who have participated in a joint lawsuit can be saved, even though there has been a large number of infringements. In addition, consumers are responsible for proof in the circumstances in which the company has all the evidence, and consumers must endure the long time and high cost of the lawsuit. Even if consumers tolerated, the amount of relief is significantly lower than the amount of damage. Therefore, there are clear limitations to the application of consumer damage.

B. Recommendations

- Although Homeplus sold about 6 million personal information and earned a whopping 1.19

206 Written by Korea National Council of Consumer Organizations

billion won in profits, the damage relief amount is less than 1 percent, which is the limit of consumer damage relief due to the absence of the 'consumer class action suit system'. Therefore, it is necessary to introduce a class action suit system quickly.

- The most efficient way to relieve minor and large numbers of damage is to introduce a 'consumer class action suit system'. The government needs to introduce a 'consumer class action suit system' with measures that can enhance the effectiveness of the law, such as a system to ease the burden of proof, a system to initiate evidence and punitive damages, according to the characteristics of consumer damage.
- The court acknowledges that the personal information of the members of the Homeplus family card has been provided to the insurance companies and that the defendant is in a position easy to prove due to the imbalance of evidence, but only adheres to the principle of law interpretation and imposes the burden of proof on consumers. As it is virtually impossible for consumers to prove the illegal activities of a company, it is necessary to shift the burden of proof.

C. Responsible ministries and agencies

- Ministry of the Interior and Safety
- Personal Information Protection Commission

4) Medical Information and Right to Privacy[207]

4-1) Out-of-Purpose Use and Provision of Medical Information

A. Background

- In principle, patients' information collected by medical institutions can only be used for the medical needs of the patients.
- However, as digitalization of medical data has taken place, various entities - electronic prescription system providers, electronic medical records system providers, medical information storage companies, medical device companies, pharmacies etc. - came to handle medical information.
  Each of these companies is now processing medical information gathered from medical institutions without legal basis and without explicit consent of patients who are the data subject.
- Current State
  - In 2010, SK Telecom, a telecommunication company, used patient information provided by medical institutions in the form of electronic prescription. Without patients' consent, the company store the information in the company's server, processed the data and made profit out of it. A criminal trial is still under way.
  - Also, in 2010, it was revealed that Korea Pharmaceutical Information Center obtained

207 Written by Center for Health and Social Change

unjust advantage by processing patients' medical information collected from pharmacies and selling it to IMS Health without patients' consent. A criminal trial is still under way.

- Some medical institutions and IT corporations are jointly planning to store patients' medical information in the cloud server of the IT corporation and process that data in various way without patients' consent.
- News reports about Asan Medical Center(a major hospital that belongs to Hyundai group), Hyundai Heavy Industries(a conglomerate) and Kakao Corporation (a major IT corporation) establishing a joint venture corporation: "Kakao Advances to Medical Big Data Industry(카카오, AI 의료 빅데이터 사업 진출)"
- News reports about Seoul National University Bundang Hospital(one of the highest ranking hospitals), Daewoong Pharmaceutical Corporation(one of the largest pharmaceutical company in Korea) and NAVER(another major IT corporation) establishing a joint venture corporation: "IT Corporations Reaches Out Their Hands to Healthcare Industry (헬스케어 산업에 손 뻗는 IT기업들)"
- Government pushes forward to develop systems that can easily provide personal medical information to private insurance companies through mobile application: Government removes the barrier protecting personal health information from insurance companies(정부, 보험사에 개인 진료·건강정보 '빗장 풀기' 논란).
- Health Insurance Review and Assessment Service (HIRA) provides Sample Research DB to private insurance companies in 52 occasions (the total number of patients sums up to 64.2 million) on the basis that the provided data was de-identified.

B. Recommendation

- Reduce the gray area by strictly banning out-of-purpose use and provision of medical information without the consent of data subject; and by allowing it exceptionally only on the basis of conditions defined by law.

4-2) Storage and Retention of Health Information

A. Background

- It should be the principle that health-related personal information should be discarded once the goal of the data collection is reached.
- However, National Health Insurance Corporation, Health Insurance Review and Assessment Service and many medical institutions are retaining the data semi-permanently without explicit legal basis, claiming that the data is needed for academic research.
- (Institute for Digital Rights, A Study on Developing System that Enhance Connecting and Combining Datasets, 2017. (Original title: 데이터 연계· 결합 지원제도 도입방안 연구, 2017.)

Personal Information Protection Commission)

B. Recommendation

- The legal and administrative guideline defining the period that medical institutions and public institutions that handle health information can retain and use health information should be more specifically defined.

4-3) Medical institutions' lack of fulfillment of duty of safeguards regarding protecting personal information

A. Background

- As health information is especially sensitive among various personal information, its protection level should be stronger than those guided by Personal Information Protection Act.
- Nevertheless, the security level of protecting medical information is relatively low in South Korean medical institutions. As a result, leak of medical information and infringement of Personal Information Protection Act take place frequently.
- According to the 2015-2016 Ministry of Public Administration and Security's statistic report on administrative punishment, there were 73 cases of infringement of Personal Information Protection Act. Among those cases, there were 22 cases of infringement made by 6 institutes in medical field. (4 cases of infringement made by one institution in 2015 and 18 cases of infringement made by 5 institutions in 2016)

B. Recommendation

- Supervision and inspection of medical institutions on handling personal information should be strengthened.

4-4) Providing individual health information as open data

A. Background

- As health information is very sensitive, it should not be provided openly even if the data is de-identified.
- Before 2017, National Health Insurance Corporation allowed anyone to download de-identified dataset. Even now, researchers can download Sample Research DB and Customized Research DB after following several steps of process. See National Health Insurance Corporation homepage https://nhiss.nhis.or.kr/bd/ab/bdaba000eng.do;jsessionid=khxrsioO4MpXAmdiwCaTsdSnb25XGhnGp95JFbHr1BYVCTI9UHBjeXLjrNkSje6p.primrose22_servlet_engine1

B. Recommendation

- Providing health data (including de-identified data) as open data should be legally banned.

4-5) Use of Health Data in Academic Studies

A. Background

- Health information could be used for academic studies without individual consent but the purpose of the study should be proportionate to the original purpose of data collection. Also, data should be used under maximum security condition.
- In Korea, even if personal data is not systematically and legally protected sufficiently, personal medical information that is retained by individual medical institutions and public institutions (such as National Health Insurance Corporation) is provided to researchers on the basis that the data is de-identified and the researchers have followed the application process.
- When medical information is provided for research, the fact that their information is used should be notified to the data subjects and the chance to choose between opt-in and opt-out should be given to them. However, this process is not observed properly. See National Health Insurance Corporation homepage: https://nhiss.nhis.or.kr/bd/ab/bdaba000eng.do;jsessionid=WZzEkwUgzPcCQ9o2asY0Z1KmssRBDSa0pBV7LGVbTNWhzjrdUYlzADD1u7DXrtdr.primrose22_servlet_engine1

B. Recommendation

- The scope, process, and security procedure of academic research that can be carried out without the consent of data subjects should be legalized.

5) Provision to Investigative Agency of Personal data from Public Institution[208]

A. Background

- According to the current Personal Information Protection Act (PIPA), personal information can be used for other purposes or provided to 3rd party “where it is necessary for the investigation of a crime, indictment, and prosecution” (the Article 18 (2), 7). Although this does not apply “when it is likely to infringe on unfairly the interest of a data subject or third party”, there are not specific requirements on that.
- According to the current PIPA, main regulations of PIPA does not apply to “personal information collected or requested to be provided for the analysis of information related to national security” (the Article 58 (1), 2).
- So, there has been a lot of controversy over extensive provision of personal information, which is especially belonged to public institutions, to intelligence and investigative agencies. In particular, it is increasing that investigative agencies are given a huge amount of personal information from

208 Written by Korean Progressive Network Jinbonet

public institutions and investigate who are not suspects by using 'dragnet' investigation method. Even sensitive information such as health-related information has been provided to them without a warrant.

- In 2013, police agency was given medical care details of the railroad trade union members, who were on the wanted list for illegal strike, from National Health Insurance Service without a warrant. At that time, the information, which was given to police agency without a warrant, was not only from NHIS but also several other public institutions including National Pension Service and National Education office. The railroad trade union members had been indicted with the suspicion of illegal strike on March 11 2014, but afterwards they were found not guilty. They filed a constitutional petition against the provision of medical care details, which was ruled unconstitutional in 2018.209
- In 2014, the police was provided with information of 3,000 basic living security recipients from local governments in order to arrest a person who scribbled on the wall to criticize the government with the phrases such as "Park Geun-hye administration dismissed" and "illegal election intervention by NIS".210
- In 2016, the police were provided with personal information of 600 people, who are assistant to impaired, from local governments without a warrant in order to investigate benefits fraud by tracking their location of cell phone call. The dragnet investigative techniques targeting assistants to impaired have been used by many other local police too. Assistants to impaired filed a petition with the constitutional court, but it was rejected in 2018.211
- According to the National Assembly's audit of the government in 2014, the police and the prosecution had viewed 967,000 insurance medical information per year and 2,649 per day.212
- Cheong Wa Dae and the NIS inspected the private lives of the prosecutor general who indicted, in spite of the government's opposition, the director of NIS for violating the Public Official Election Act in 2013. For the inspection, e-government system, such as family relations information system of district office, police computer networks, NHIS (National Health Information Service) system and NEIS (National Education Information System), have been illegally inquired, so those involved are on trial.
- However, despite the ongoing controversy and the Constitutional Court's ruling on the constitutionality of the case, no improvement has been made to control and supervise the collection of personal information by the intelligence and investigative agencies.
- The Constitutional Court saw the provision of personal information held by public institutions to investigative agencies as arbitrary investigation that do not require a warrant. It only ruled that, as for the petition of the railroad workers, the provision of two to three years information of sensitive medical care benefits, including the name of the disease, was unconstitutional on the grounds that it was not inevitable. On the other hand, as for the petition of assistants of

209 the Constitutional Court, August 30, 2018, 2014Hun-ma368
210 HUFFPOST KOREA. (2014). The Government Critic Graffiti, Finding Among One of the Basic Feeders? https://www.huffingtonpost.kr/2014/10/15/story_n_5987854.html [15 May 2019].
211 The constitutional court ruled Aug 30, 2018. 2016Heonma483
212 Yonhap News. (2014). <Giving Personal Information to Agency and Peeping them… Health Insurance Management Corporation's Personal Information Management is 'Mess'> https://www.yna.co.kr/view/AKR20141016161100017 [15 May 2019].

impaired, the Constitutional Court rejected it on the grounds that it was not an excessive provision of large-scale personal information by local government because the public interest of punishment of benefits fraud is much bigger.

- As for the collection of personal information by investigative agency, since the establishment of the Council of Europe's police recommendations, until Europe enacted what it calls a "police directive"213 in 2016, international norms have been strengthened for requiring investigative agencies as well, to abide by the privacy principle.
- Ever since Edward Snowden's revelation, the call for proper control and supervision of the data collection by intelligence and investigative agencies continued internationally, including the U.N. General Assembly's resolution on digital privacy.214

B. Recommendations

- The system shall be improved to control the personal information collection by the police and other investigative agencies to comply with the privacy principles and to be supervised by an independent third party. In order to collect a large scale of personal data including non-suspects, it must be regulated by laws including specified procedure. Especially, in case of sensitive data such as health-related information, when they collect sensitive data, they should ensure following orders from courts including getting a warrant.
- The system should be improved so that it can be supervised by an independent third party in order to control the collection of personal information by the intelligence agency in an essential and proportionate case. In order for the intelligence agency to collect personal information, it is subject to control under the law, including specific requirements and procedures.

C. Responsible ministries and agencies

- Ministry of the Interior and Safety
- Personal Information Protection Commission
- National Police Agency
- National Intelligence Service

6) Social Security Information System[215]

A. Backgrounds

- In 2010 the Ministry of Health and Welfare introduced the 'Social Security Information System'(SSIS) for the management of several types of welfare benefit schemes through one

213 DIRECTIVE (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
214 A/RES/68/167
215 Written by MINBYUN-Lawyer for a Democratic Society

electronic portal system (in 2013 the system was expanded to cover around 360 welfare schemes by 22 ministries and agencies)

- Every person and household receiving social welfare benefit or service is registered and their history recorded in the SSIS. As of Dec 2015 17,140,887 recipients were registered (including overlaps).
- One important function of the SSIS is to gather and manage documentation for the investigation of income and assets of applicants and beneficiaries.
- For the investigation of assets and income the applicant is required to provide the relevant agency with a comprehensive consent by which 77 types of information from 24 public institutions (as of Dec 2017) including tax information, information on departure from and arrival into the country etc. and financial information from approx. 140 financial institutions are collected. Much of that information is updated automatically. Regular investigations into changes of assets and income are implemented twice a year.
- In 2014 after the suicide of a mother and her two adult daughters on account of economic difficulties received much public attention, the government announced that it would proactively "dig up" those in need and enacted the 'Act on use, provision of social security benefits and excavation of eligible persons' ("Excavation Act"). According to the act, information such as cessation of utilities on account of late payment of fees or late payment of health insurance fees can be collected without prior consent. The purpose of the act was to alleviate "blind spots" in the social security system through the use of big data. Some of the information collected this way can be disclosed to local governments without consent and by consent to charity organizations.
- In 2017 the Excavation Act was revised to allow collection of information regarding late payment of loans and or credit card bills.
- However, the fundamental cause of so-called blind spots (persons in need but not covered by social security) lies in the residualism dominating Korea's social security system, especially public aid. For example, if the income or assets of a relative with duty to support (parents or adult children) registered in the SSIS exceeds a certain level, public aid is suspended regardless of whether that relative actually fulfills the duty. Due to such harsh requirements, the number of persons in need but not covered by social security is estimated at 930,000 (as of 2015). On the other hand, many recipients lost their status due to the inflexibility of the SSIS leading to several suicides.
- According to government figures, of the 243,647 persons "excavated" through the use of "big data" in 2018 from Jan to Nov, only 81,354(33.4%) received any kind of support, and only 28,932 (12%) received public support or services. The rest were referred to privately owned charities.
- In April 2019, the Ministry of Justice announced that it would spend KRW 356,000,000,000 to set up a "next generation social security information system" (NGSSIS). One of the intended features of the NGSSIS is a "welfare membership" scheme, by which the system will at regular intervals make assessments regarding for which social security benefits or services a person registered with the system may be potentially eligible and provide that person with a "personalized list" of such benefits or services. The assessment will be made based on information on household, income and assets collected with prior consent.

- In short, the NGSSIS will regularly collect and update information on household, assets, income etc. of anyone registered as a "member", even if the person is not yet a recipient of any kind of social security service or benefit. In light of the fact that the scheme targets the whole population, and the vast range of information collected from hundreds of public and financial institutions, the potential threat to personal information and the right to privacy is substantial, even if prior consent is a prerequisite.
- The basic idea of collecting vast amounts of personal information under the pretext of potential provision of social security services or benefits and the idea that social service delivery systems can be substituted with a centralized computerized system, while ignoring that the problem lies in a system of segmented benefits and services that do not complement each other and an exclusiveness by which the burden of proof always lies with the applicant, making it most difficult for the most vulnerable to access adequate support, is indicative of a drive to control through concentration and centralization of information.

B. Recommendations

- Stop collecting information without the consent of vulnerable populations under the pretext of "excavating" persons in need of social services or benefits. Resolve "blind spots" in the social security system by raising the budget to expand coverage.
- Scrap the 'Welfare Membership' scheme which will lead to excessive amassment and centralization of information into the NGSSIS. Reform the social services delivery system to ensure accessibility to adequate social security services and benefits.

C. Responsible ministries and agencies

- Ministry of Health and Welfare

7) DNA Database[216]

A. Background

- Relocated residents from dwellings to be demolished, labor union members and activists from street vendors who occupied and protested became subject to DNA collection and their DNA identification information, known as 'profile' are kept in the national DNA identification database.
- The constitutional complaint filed in 2011 by the Yongsan demolition and Ssangyong workers was dismissed in 2014. In the case of DNA collection, the identity information includes genetic information that is shared with the family, unlike other biometric information such as other personal information or fingerprints, and such infringement resulting from the collection of the national database extends to family members such as children.
- In 2016, KEC trade union members filed a constitutional complaint. After a conviction for "a

216 Written by MINBYUN-Lawyers for a Democratic Society

crime of breaking into the building of others by the power of the multitude" during a factory occupation strike in 2010, a warrant was issued, and DNA samples were taken from 2015 to 2016. In 2017, activists of Korea Democratic Street Vendors Confederation filed a constitutional complaint. In 2013, a plaintiff was convicted of "infiltration into the store by the power of the multitude" in the process of demonstration by occupying outlets, and a warrant was issued to take DNA samples in 2017. On August 30, 2018, the two incidents were merged and decided to be the constitutional inconsistency.217 The reason for the DNA procedure provision by a warrant lacks the opinions of the subject, the right of appeal and remedies.

- However, even though the controversies, including the constitutional-inconsistency decision of the Constitutional, continue, the Korean government has not submitted a bill for revision the system. And the government refused the request of victims to delete their DNA information.
- ACT ON USE AND PROTECTION OF DNA IDENTIFICATION INFORMATION, legislated in 2010, allows the collection of DNA samples of people, who are sentenced criminal punishments or detained suspects, including juvenile delinquents without considering the chances of re-committing crimes individually. It also allows the uses of their DNA identification information, known as 'profile', for investigations after keeping DNA identification information into the database.
    - This Act does not specify the risk of re-committing crimes as a requirement for the collection of DNA samples. The act also does not specify the requirements of the issuance of warrant, so that the monolithic collection of DNA samples is allowed considering only whether the people committed certain crimes listed in the act.
    - For these reasons, only 23% of people in DNA identification database are the people who have actually sentenced criminal punishments218
    - Moreover, relocated residents from dwellings to be demolished, labor union members and activists from street vendors who occupied and protested became subject to DNA collection since the act allowed the collection of people who have done "the threat of collective force."
- The act allows the erasure of DNA identification Information only when people have special reasons such as a sentence of "not guilty". If there are no special reasons, the erasure of information only can be done when the person is dead or if there is a request of the person or a decision of the person in charge of the information.
    - It is very problematic that the retention period of DNA identification information is excessively long even in the case that the targeted person for the collection does not re-commit the crimes for considerable time
    - Especially, it is very cruel for the juvenile delinquents.
    - The Constitutional Court also pointed out that the act should be improved to allow the

217 the Constitutional Court, August 30 2018, 2016Hun-ma344·2017Hun-ma630. The act is valid until December 31, 2019 or the time when the legislator revise the act.

218 According to The 2017 annual report of DNA Identification Database, 37,636 people who are imprisoned, and 99,883 people who are not imprisoned by getting the sentence of the fine, suspension of execution, suspension of probation and so on among total 137,519 people in the database.

person who does not re-commit for certain period of time can erase his or her DNA identification information in its dissent opinion and supplementary opinion in the decision219 on the article for the erasure.

Article 13 (Erasure of DNA Identification Information)(1) If a judgment for acquittal, exoneration, or dismissal of public prosecution or a decision of dismissal of public prosecution is finally and conclusively affirmed for a prisoner in a retrial, the person in charge of DNA identification information shall, ex officio or at the prisoner's request, erase DNA identification information collected pursuant to Article 5 and stored in the database.

(2) If any of the following events occurs to a detained suspect, the person in charge of DNA identification information shall, ex officio or at the suspect's request, erase DNA identification information collected pursuant to Article 6 and stored in the database:

1. If the public prosecutor makes a disposition of "cleared of suspicion" "not guilty" or "not prosecutable" or if the name of a crime of the detained suspect allegedly perpetrated is changed from the name of a crime under any subparagraph of Article 5 (1) to the name of a crime not specified in any subparagraph of the aforesaid paragraph in the course of investigation or trial: Provided, That cases where the public prosecutor makes an independent demand for a disposition of medical treatment and custody pursuant to subparagraph 1 of Article 7 of the Medical Treatment and Custody Act, along with a disposition of "not guilty", shall be excluded herefrom;

2. If a judgment of acquittal, exoneration, or dismissal of public prosecution by a court or a decision of dismissal of public prosecution is finally and conclusively affirmed: Provided, That cases where a sentence of medical treatment and custody is imposed along with a judgment of acquittal shall be excluded herefrom;

3. If a judgment by a court of dismissal of an independent demand for a disposition of medical treatment and custody under subparagraph 1 of Article 7 of the Medical Treatment and Custody Act is finally and conclusively affirmed.

(3) If a prisoner or a detained suspect is dead, the person in charge of DNA identification information shall, ex officio or at the request of any of the deceased's relatives, erase DNA identification information collected pursuant to Article 5 or 6 and stored in the database.

B. Recommendations

- Complement the judicial review process to consider the risk of re-committing crimes of the targeted individual for the collection of DNA identification information and provide the procedures for the remedy or allow the targeted individual to express his or her opinion.
- The right of the erasure of DNA identification information should be granted for the targeted individual when the purpose of the database is fulfilled by the situations, such as the targeted individual does not re-commit the crimes for the considerable period of time.

219 the Constitutional Court,2011Hun-ma28; 2016Hun-ma344, 2017Hunma630(merged)

C. Responsible ministries and agencies

- Ministry of Justice (Responsible for the act)
- Supreme Prosecutor's Office (In charge of the database for the people who are sentenced criminal punishments)
- National Police Agency (In charge of the database for the detained suspects, and crime scenes)

6. Labor monitoring[220]

A. Background

- Recently, it has become a major social problem for users to monitor workers using electronic devices like closed-circuit television(CCTV) and mobile phone applications.
- KT(one of the major company in Republic of Korea) ordered its workers to install specific applications, and if installed, company managers can access workers' current location, calendar schedule, account and photo information and contact information on workers' personal phones. The company practically forced the installation of the application by imposing a one-month suspension penalty on the workers, when the workers refused to install it. The use of CCTV video data for disciplinary actions against workers is raising problems in various industries, including not only private companies but also public offices like teachers and police officers, and some private companies installed 200 CCTVs at factories where 280 employees work including staff lounge areas, after the establishment of labor unions.
- Personal Information Protection Act221 stipulates that no one shall install and operate any visual data processing device at open places except, 1) where states allow install in a concrete manner, 2) where it is necessary for the prevention and investigation of crimes, 3) where it is necessary for the safety of facilities and prevention of fire, 4) where it is necessary for regulatory control of traffic, 5) where it is necessary for the collection, analysis and provision of traffic information. Therefore, installing CCTVs for the purpose of monitoring workers is the action that company uses information collected for purposes other than those prescribed by law, which is illegal. Meanwhile, Article 20 (1) 14 of the Act on the Promotion of Workers' Participation and Cooperation stipulates 'Installation of surveillance equipment for workers within a workplace' is Matters requiring consultation between the labor and management council. There's leaving room for monitoring workers when consulted with workers, but forcing them to install applications that can acquire internal information of personal mobile phones arbitrarily has no legal basis.
- The National Human Rights Commission recommended that labor monitoring using CCTV be stopped and that the Ministry of Employment and Labor should come up with measures to enhance the protection of employees' personal information from electronic monitoring of workplaces, but monitoring using various electronic devices is still rampant at the site and there is no countermeasures against labor monitoring using new media.

B. Recommendations

- Explain the efforts made by government agencies to prevent labor monitoring by electronic devices.
- According to a survey conducted by the Human Rights Commission in 2013, only 28.4 percent of the respondents officially raised questions when their personal information is infringed at business sites, and 29.4 percent knew that there's a report center to protect personal information based on the law. Reveal the figures for whether related perceptions have improved

220 Written by MINBYUN-Lawyers for a Democratic Society

221 Article 25 (Limitation to Installation and Operation of Visual Data Processing Devices)

in 2019 and suggest ways to improve them.

C. Responsible ministries and agencies

- Ministry of Employment and Labor
- Personal Information Protection Committee

7. The issues of Social Minorities' Privacy Rights

1) Right to Privacy of LGBTQI Persons[222]

1-1) Criminalization of Consensual Same-sex Conduct in the Military and the Right to Privacy

A. Background

- Article 92-6 of the Military Criminal Act punishes consensual same-sex sexual conduct between men in the military and is the only provision in the country that criminalizes consensual same-sex sexual conduct. Many UN bodies have recommended the abolition of this provision. In the third Constitutional review of this article in the past 14 years, in July 2016, the Constitutional Court upheld the former 92-5 of the Act in a 5 (constitutional) to 4 (unconstitutional) decision. The government replied during the UPR, "The provision is aimed at establishing military sexual morale, not punishment for sexual orientation." In 2017, the press and media reported a crackdown on gay soldiers for violating the Military Criminal Act in the army. The military investigators tracked down gay soldiers using gay dating apps and/or social media. The investigators abused the personal data stored in victims' mobile phones, including the history of live communications and messages, to identify other persons suspected of being gay, leading to a serial investigation. One officer, known as Captain A, was prosecuted and sentenced to 6 months of imprisonment and one year of probation.

B. Recommendations

- Abolish Article 92-6 of the Military Criminal Act, which criminalizes consensual sexual acts.
- Declare moratorium of investigation based on article 92-6.

C. Responsible ministries and agencies

222 Written by Rainbow Action Against Sexual-Minority Discrimination (GongGam Human Rights Law Foundation, Korean Lawyers for Public Interest and Human Rights(KLPH), Labor Party-Sexual Politics Committee, Minority Rights Committee of the Green Party, Daegu Queer Culture Festival, Deajeon LGBTQ Human Rights Group Solongos, QUV; Solidarity of University and Youth Queer Societies in Korea, Social and Labor Committee of Jogye Order of Korean Buddhism the Korean lesbian community radio group, Lezpa, Rainbow Jesus, Rainbow Solidarity for LGBT Human Rights of Daegu, QIP Queer In Pusan, Busan Queer Festival, Gruteogi : 30+ Lesbian commuity grocommunity, Seoul Human Rights Film Festival, Seoul Queer Culture Festival Organizing Committee, Korean Anglican Church's Youngsan House of Sharing (Social Minority Life and Human Rights Center), Yeohaengja : Gender non-conforming people's community, PFLAG Korea, Advocacy for LGBTQ's rights to knowledge, Northwest, Collective for Sexual Minority Cultures PINKS, The Korean Society of Law and Policy on Sexual Orientation and Gender Identity, Sinnaneuncenter: LGBT Culture, Arts & Human Rights Center, Unninetwork, Lesbian Human Rights Group 'Byunnal' of Ewha Womans University, Open Door in JB, Sexual Minority Committee of the Justice Party, Network for Glocal Activism, LGBTQ Youth Crisis Support Center 'DDingDong', Korean Transgender Rights Organization JOGAKBO, Trans Liberation Front, Chingusai – Korean Gay Men's Human Rights Group, Lesbian Counseling Center in South Korea, Korean Sexual-Minority Culture and Rights Center(KSCRC), Youth PLHIV Community of Korea 'R', Solidarity for LGBT Human Rights of Korea, Solidarity for HIV/AIDS Human Rights Nanuri+)

- Ministry of Defense

1-2) Resident Registration Number System

A. Background

- Koreans are given a Resident Registration Number (“RRN”) consisting of 13 digits at the same time of birth registration. The number includes information such as date of birth and sex. For men born in the 1900s, the back digit starts with a 1, and for woman, the back digit begins with a 2. For people born after 2000, the latter number begins with 3 and 4 for men and women, respectively.
- Since the resident registration number (“RRN”) is an all-purpose identification number, Koreans need to disclose the ID card and the RRN in all works of life, from real estate transactions to voting. All-purpose RRN gives great difficulty to transgender people who didn’t change their legal gender due to strict and invasive criteria. Because it is difficult to show your ID card, you will be given up in various situations such as job seeking, contracting cellphones, and voting.

B. Recommendations

- Change the RRN to a random number system that does not include personal information.

C. Responsible ministries and agencies

- Ministry of the Interior and Safety

1-3) HIV/AIDS and the Right to Privacy

A. Background

- There is a clause in the Prevention of Acquired Immunodeficiency Syndrome Act to prevent the infringement of people with HIV’s privacy rights by medical personnel, but the privacy of people with HIV is frequently infringed in the medical field or prison setting.
- In general, the company cannot know the results of workers' health screenings because they are notified directly to the workers. However, sometimes, companies appoint a specific medical institution for a medical examination, and the medical personnel might leak the HIV status to the companies. Or some companies coerced the workers to submit the complete results directly to the company.
- On January 23 this year, three people living with HIV submitted a complaint to the National Human Rights Commission. Three complainants claimed that the guards violated their privacy rights during their detention in Daegu prison in 2018. They were separately confined in the room with a sign saying "special patient." The guards called them loudly as a "special patient" or sometimes "AIDS." They were not able to exercise with other prisoners, and sometimes the

guards kept a line on the playground and prevented them from crossing.

- Also, under article 19 of the act, the State party still criminalizes people with HIV with an undetectable viral load for “spreading AIDS”.

B. Recommendations

- Take necessary measures to prevent infringement of privacy rights of people living with HIV and AIDS.
- Cease the investigation, prosecution, and punishment under article 19 of the Prevention of Acquired Immunodeficiency Syndrome Act.

C. Responsible ministries and agencies

- Ministry of Health and Welfare / Korea Centers for Disease Control & Prevention

1-4) Right to Privacy and Bodily Autonomy of Transgender Persons

A. Background

- Since a 2006 Supreme Court decision,[223] the Court’s guideline presents the investigative points of the legal recognition of transgender persons. [224] The word 'investigative points' implies discretion, but the Court accepts it as a de facto prerequisite. According to the guidelines, one has to be over 19 years old, did sterilization surgery and sex reassignment surgery, non-married or divorced, doesn't have minor children. Also, even though you are an adult, you must include your parents' consent. There have been some courts that do not require external genitalia surgery since 2013, but some courts still require sex reassignment surgery, including external genitalia surgery.

B. Recommendations

- Exclude forced sterilization surgery, genital reconstructive surgery, and other surgical procedures for the precondition of legal gender recognition of transgender persons.

C. Responsible ministries and agencies

- The Supreme Court of Korea

223 Supreme Court of Korea, 2004Su42 Decision, June 22 2006.

224 Guidelines on the Clerical Processing of Cases of Transsexuals' Application for Legal Sex Reassignment (revised on January 8, 2015 [Established Rules on Family Relationship Registration No. 435; implemented on February 1, 2015]; in Korean). English translation by Korean Society of Law and Policy on Sexual Orientation and Gender Identity is available at http://annual.sogilaw.org/review/law_list_en

2) Privacy of People Living with HIV (PLHIV)[225]

2-1) PLHIV and Violations of Privacy in the Medical Field

A. Background

- In Korea, the HIV/AIDS Prevention Act226 contains a provision against privacy infringement.
- Despite Article 7 of the HIV/AIDS Prevention Act, the privacy of people living with HIV is frequently violated in the medical field.
- The following situations and actions have occurred:
    - Hospital sending a referral to another hospital without the consent of the patient living with HIV
    - Hospital attaching a note about a patient's seropositive HIV status to a treatment referral or other records without their consent
    - Hospital notifying family members about the patient's seropositive HIV status without their consent
    - Hospital conducting an HIV-test without the consent of the patient
    - Hospital showing carelessness and negligence when notifying a patient about their HIV results
    - Hospital's medical team labelling and separating items used by PLHIV, in a way that it is possible for other people to become aware of the purpose of the separation

[References] 2016 A Survey on Medical Discrimination against HIV by National Human Rights Commission

	Mostly / Usually Yes			
	Period living with HIV (Years)			
	<5	**5~9**	**10+**	**Total**

225 Written by HIV/AIDS Activists Network Korea

226 The HIV/AIDS Prevention Act Article 7 (Prohibition against Divulgence of Confidential Information) No person falling under any of the following shall, except for cases provided for in this Act or an order issued under this Act, or in any other Act or subordinate statute, or cases where the person himself/herself has given consent, divulge any confidential information he/she has learned about such an infected person in the course of performing his/her duties not only during his/her term of office but after his/her retirement:
1. Persons who engage in affairs regarding the prevention and management of AIDS and the protection of and support to infected persons in the State or local governments;
2. Persons who have participated in the diagnosis, autopsy, medical treatment and nursing of infected persons;
3. Persons who keep and manage records regarding infected persons.

Examination/Surgical operation delay	**6**	**15**	**28**	**49**
	9.7%	**23.8%**	**35.4%**	**24.0%**
Discrimination during medical treatment in other medical divisions	**10**	**13**	**31**	**54**
	16.4%	**20.6%**	**38.8%**	**26.5%**
Discrimination by nurses	**7**	**9**	**17**	**33**
	11.3%	**14.3%**	**21.5%**	**16.2%**
Discrimination by radiation or laboratory personnel	**3**	**4**	**10**	**17**
	4.8%	**6.3%**	**12.7%**	**8.3%**
Discrimination by administrative staff	**3**	**6**	**11**	**20**
	4.8%	**9.5%**	**14.1%**	**9.9%**
Gossiping about PLHIV by hospital staff	**6**	**13**	**21**	**40**
	9.7%	**20.6%**	**26.9%**	**19.7%**
Marking of HIV into medical chart	**8**	**19**	**29**	**56**
	13.1%	**30.2%**	**37.2%**	**27.7%**
Difficulty faced when disclosing HIV status while visiting a hospital for other illnesses	**43**	**51**	**60**	**154**
	69.4%	**82.3%**	**76.9%**	**76.2%**
Wishing to move to a larger city due to inconvenience while visiting a hospital for medical treatment	**18**	**18**	**37**	**73**
	29.0%	**28.6%**	**46.8%**	**35.8%**
Stating HIV status on prescriptions against the patient's will	**11**	**14**	**29**	**54**
	17.7%	**22.2%**	**36.7%**	**26.5%**

B. Recommendations

- Actions to develop practical measures for the implementation of the HIV/AIDS Prevention Act, Article 7 (prohibition of disclosure of confidential information)

- Compulsory education for health care personnel

C. Responsible ministries and agencies

- Ministry of Health and Welfare

2-2) Privacy Infringements of PLHIV in Detention Facilities[227]

A. Background

- Despite the confidentiality provision under the HIV/AIDS Prevention Act228, Situations where a person's positive HIV status is announced to others without the person's consent are frequent within detention facilities. Furthermore, separation, discrimination, and exclusion from activities due to a person's positive HIV-status violates the human dignity and values outlined in Article 10 of the Constitution. They are also in violation of the right to seek happiness and the right to equality under Article 11 of the Constitution and a clear violation on the grounds against the 'National Human Rights Commission Act' as well as the 'Law on the Execution of a Sentence and the Treatment of an Inmate' which outlines that no one should be discriminated based on their medical history..
- Situations in detention facilities where a person's HIV status will inevitably be exposed by marking the room of the person with a label of a "special patient" (For example: by attaching a large written notice of a "special patient" to the door of the person)
- Acts of assigning exercise time separately, and drawing lines on the ground in order to separate and exclude when exercising together
- Acts of exclusion from all special interest activities, and prevention from participating in rehabilitation programs.
- Acts of assigning and isolating PLHIV inmates to live with other known PLHIV inmates
- Acts of referring to PLHIVs by calling them out as "special patients" loudly
- Acts of referring to HIV in situations where other inmates might hear and become aware of a person's positive HIV-status (For example: Talking about the name of the disease while inmates are standing in the hallway / During security checks, guards telling each other "Not to enter the

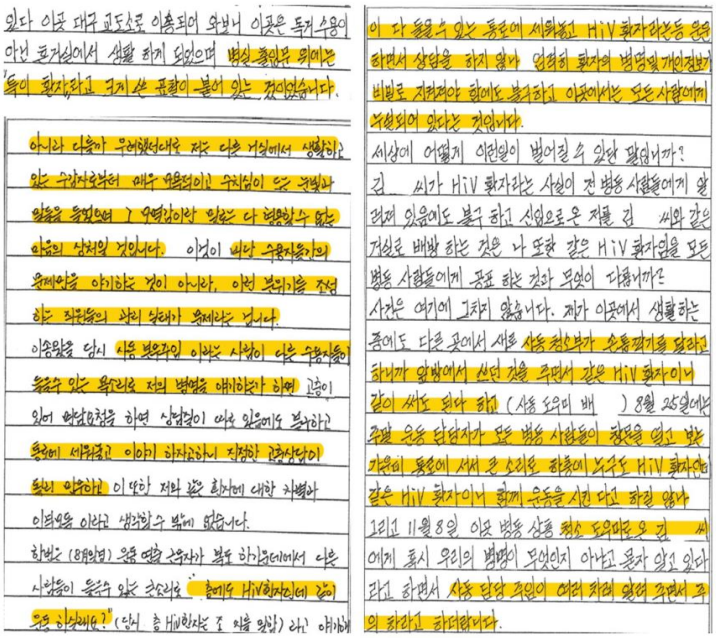
227 The following situation led to two victims and two human rights groups filing a petition with the National Human Rights Commission.

228 The HIV/AIDS Prevention Act Article 7 (Prohibition against Divulgence of Confidential Information) No person falling under any of the following shall, except for cases provided for in this Act or an order issued under this Act, or in any other Act or subordinate statute, or cases where the person himself/herself has given consent, divulge any confidential information he/she has learned about such an infected person in the course of performing his/her duties not only during his/her term of office but after his/her retirement:
1. Persons who engage in affairs regarding the prevention and management of AIDS and the protection of and support to infected persons in the State or local governments;
2. Persons who have participated in the diagnosis, autopsy, medical treatment and nursing of infected persons;
3. Persons who keep and manage records regarding infected persons.

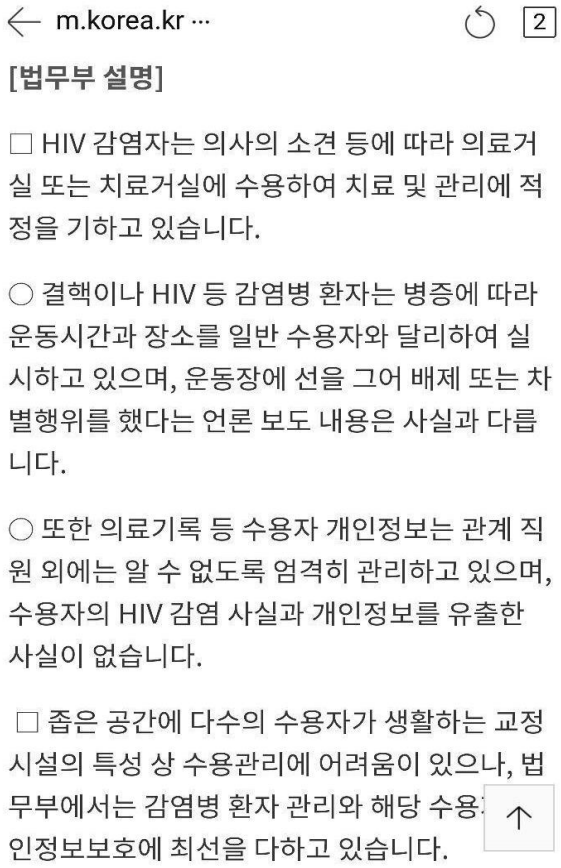
AIDS room" / A guard taking nail clippers out of a box marked with "HIV" in front of fellow inmates and pass them to a PLHIV)

- Detention facility staff wearing a mask only when coming to contact with a PLHIV
- The Ministry of Justice and the Office of Correctional Affairs exposed a person's HIV status under the person's real name in an official reply letter to their civil petition

[Reference] A letter containing the victimization of a PLHIV in a detention facility in Daegu.



[Reference] 2019.02.15 Policy Briefing by the Ministry of Justice (The denial of any human right violations was made based only on the answers from the Daegu detention centre without any correspondence from the victim.)



B. Recommendations

- <u>Discontinuation of compulsory unconsented HIV testing during one's stay in prison.</u>
    - Article 3 of the Guidelines for Medical Care of Inmates (Health examination of a new inmate) stipulates in paragraph five a requirement that: "All new inmates should be quickly commissioned to a competent health center or an inspection specialist to conduct syphilis and HIV tests." In the process, the patient is not informed of the HIV test. To take a blood sample or conduct other tests without a person's consent is a human rights violation and should therefore not be done without consent
- <u>Improvement of insufficient confidentiality regulations (Medical Information System & Boram System)</u>
    - There is an absence of specific guidelines and non-disclosure regulations in the guidelines for upkeeping, recording, and management of patient information in the prison administration system. The medical information system is linked to the corrections information system (Boram system), and other detention facilities are therefore able to look up personal information of the individual inmates, thus leading to an unregulated exposure of the medical information of PLHIV inmates.

- Restrictions on the health rights of PLHIV
    - Article 20 of the Guidelines for Medical Care of Inmates (Transfer of Hemodialysis patients) restricts the medical access of PLHIV inmates by allowing only those who are not infected by infectious disease, such as HIV/AIDS, to receive blood dialysis. However, medical access restrictions on PLHIV inmates who need hemodialysis are medically unfounded. According to the "Standard Guidelines for Infection Control in Dialysis" (2010), published by the Korea Centers for Disease Control and Prevention and the Korean Society for Hospital Infection Control: "When it comes to blood-borne infections testing, dialysis patients don't have to take regular HIV tests. In order to prevent and manage HIV, there is no need to isolate HIV patients from other patients, isolate dialysis machines or differentiate responsible medical personnel. The dialysis machine can be reused."
- Introduction of a system for gathering the requests of PLHIV to prevent recurring human rights violations
    - By replying to a call for improvement of living conditions without any further investigation "not only the Daegu prison & corrections facility but also the Office of Correctional Affairs and the Daegu Detention center is ignoring and not even pretending to hear the voices of the inmates no matter how many times they file petitions and appeals" the inmates are suffering severe mental distress and have lamented their condition as follows. "I can't help but to deplore the fact that they are ignoring the prisoner's suffering and believe in false reports from Daegu prison staff without a single on-site investigation."
- In order to prevent the recurrence of PLHIV's human rights violations, the Ministry of Justice should provide training for prison officers
- There should be a national investigation of all the human rights violations against PLHIV whom are in custody by the Ministry of Justice
- Guidelines should be prepared to ensure the health and human/privacy rights of PLHIV in detention facilities

C. Responsible ministries and agencies

- Ministry of Justice

2-3) Privacy of Youth PLHIV

A. Background

The HIV/AIDS Prevention Act

Article 8-2 (Notification of Results of Medical Examinations)

① No person who has conducted a medical examination of AIDS shall notify any person, other than the person himself/herself subject to the medical examination, of the results of such medical examination: Provided, that where a person subject to the medical examination is a person who lives communally in a military camp, correctional institution, etc., the person who has conducted the medical examination shall notify the head of the relevant institution of the results of such medical examination, and where **the person subject to the medical examination is a minor**, feeble-minded person or mentally disabled person, **the person who has conducted the medical examination shall notify his/her legal representative of the results of such medical examination.**

- When an adolescent is diagnosed with HIV, due to this legislation their family members may be notified without their consent.

B. Recommendations

- Comprehensive sex education with correct and accurate information about HIV/AIDS and the human rights of the people living with HIV
- Abolition of the legal clause that requires the legal representative of the adolescent to be notified about medical conditions without consent of the teenager
- Establishing a national support system to ensure the protection of human rights of adolescents living with HIV

C. Responsible ministries and agencies

- Ministry of Health and Welfare, Ministry of Gender Equality and Family

2-4) Privacy of PLHIV in the Labor Field

A. Background

The HIV/AIDS Prevention Act

Article 8-2 (On notifying diagnosis results)

① No person who has conducted a medical examination of HIV/AIDS shall notify any person, other than the person himself/herself subject to the medical examination, of the

results of such medical examination: Provided, that where a person subject to the medical examination is a person who lives communally in a military camp, correctional institution, etc., the person who has conducted the medical examination shall notify the head of the relevant institution of the results of such medical examination, and where the person subject to the medical examination is a minor, feeble-minded person or mentally disabled person, the person who has conducted the medical examination shall notify his/her legal representative of the results of such medical examination.

② In cases of notification of the results of a medical examination under paragraph (1), notification to a person judged as an infected person shall be given by a method that may keep the results of the medical examination confidential, such as notification through an interview.

③ **No employer is allowed to request a worker to submit a written report generated from a medical examination of HIV.**

- Despite Article 8 paragraph 2 and 3 of the AIDS Prevention Act, there are many situations in which a person's HIV status can be exposed.
- A situation in which an HIV test is forcibly included into the recruitment medical examination
- Conditions where HIV screening is compulsory in the regular workplace health examination items after employment

B. Recommendations

- Establishment of measures to ensure that the AIDS Prevention Act (Article 8, paragraphs 2 and 3) are implemented properly to prevent infringement of labor rights
- Establishment of institutional mechanisms to prevent mandatory HIV screening in recruitment and workplace health examinations

C. Responsible ministries and agencies

- Ministry of Employment and Labor, Ministry of Health and Welfare

2-5) Privacy of Soldiers and Paramilitary Personnel Living with HIV

A. Background

The HIV/AIDS Prevention Act

Article 8-2 (On notifying diagnosis results)

① No person who has conducted a medical examination of HIV/AIDS shall notify any person, other than the person himself/herself subject to the medical examination, of the results of such medical examination: Provided, that **where a person subject to the medical examination is a person who lives communally in a military camp**, correctional institution, etc., the person who has conducted the medical examination shall notify the head of the relevant institution of the results of such medical examination, and where the person subject to the medical examination is a minor, feeble-minded person or mentally disabled person, the person who has conducted the medical examination shall notify his/her legal representative of the results of such medical examination.

② In cases of notification of the results of a medical examination under paragraph (1), notification to a person judged as an infected person shall be given by a method that may keep the results of the medical examination confidential, such as notification through an interview.

③ No employer is allowed to request a worker to submit a written report generated from a medical examination of HIV.

- In the case that a soldier, or paramilitary personnel is found to be HIV positive, their HIV status is notified to the head of the appropriate department. PLHIVs are exempt from military duty and therefore most of the situations occur when a person finds out about their HIV infection after joining the military.
- Situations in which the military informs other people of a person's HIV status without their consent
- Formation of an atmosphere that generates fear about HIV/AIDS and excludes people living with HIV (For example: Ordering someone to clean up the place they have stayed in with bleach.)

B. Recommendations

- As the Korea Centers for Disease Control and Prevention states, there is no risk of transmission while cohabiting with PLHIV, and therefore the notification clause should be repealed
- There should be correct and accurate education in relation to HIV/AIDS as well as the human rights of PLHIV for the persons concerned

C. Responsible ministries and agencies

- Ministry of National Defense, Military Manpower Administration, National Police Agency

2-6) Control of and Intervention to PLHIV's Private Domain (sexual acts) by the State

A. Background

- Article 19, Prohibition against Carrying and Spreading HIV/AIDS, of the HIV/AIDS Prevention Act punishes PLHIVs engaging in "sexual acts without a condom".
- In accordance with the U=U campaign, it has been proven that the possibility of a person living with HIV under anti-retroviral treatment transmitting HIV is 0%. Despite this, due to Article 19 (Prohibition against Carrying and Spreading HIV/AIDS) of the HIV/AIDS Prevention Act, PLHIVs engaging in "sexual acts without a condom" can be penalised. This is the case even if the other party involved has been informed by the person living with HIV of their HIV-status in advance, and has afterwards willingly consented to sex with the person living with HIV. Furthermore, this is also the case when as a result of the sexual act no transmission of HIV has occurred. The law is a clear violation of privacy of PLHIVs by the state.

B. Recommendations

- Abolition of article 19, Prohibition against Carrying and Spreading AIDS, of the HIV/AIDS Prevention Act.

C. Responsible ministries and agencies

- Ministry of Justice

3) Infringement on Democratic People's Republic of Korea ("DPRK") Defectors' Right to Privacy[229]

A. Background

- On April 12th, 2016, 12 employees and 1 manager of a North Korean restaurant in China entered Republic of Korea ("ROK") en masse, and their entry into South Korea was made public via emergency briefing by the Ministry of Unification.
- In the event that DPRK defectors enter ROK, the Ministry of Unification determines the details of protection and support if the National Intelligence Service ("NIS") conducts an investigation and decides to provide protection and settlement support without disclosing the identity of a person concerned nor the facts and details concerning his or her entry into ROK.
- However, just for the DPRK employees who entered ROK on April 2016, their entry into ROK was disclosed immediately afterwards, and the photo of them entering the Centre for Protection of DPRK Defectors ("Centre") was disclosed by the media. The identity of a photographer remains

229 Written by MINBYUN-Lawyers for a Democratic Society

unknown, but the photo was released to the media and continue to be cited in related news articles. (Appendix 1: Photo)

- The employees had no idea that the photo would be released to the media, nor were they aware of how the photo of them entering the Centre ended up being reported. The photo reveals enough to allow anyone who knows the individuals in the photo to recognize that person, and some of the employees indeed received questions, asking if they are the ones in the released photo by their acquaintances.
- The NIS operates and manages the Centre, and related Acts and subordinate statute only allow the NIS to investigate the DPRK defectors, while, in principle, the Ministry of Unification is in charge of protection and support work for DPRK defectors. Nevertheless, the NIS, having extensive authority to identify and investigate DPRK defectors, arbitrarily decides whether or not to disclose information about DPRK defectors as well as the contents be disclosed. (Appendix 2: Related Acts and subordinate statute)
- Unlike the purpose of policy and laws, which aims to protect and support DPRK defectors, it has become difficult to control the process of NIS in its collection and utilization of personal information of DPRK defectors, for NIS has an administrative control over the Centre. Also, it is difficult to predict who will be the subject of the NIS' management because a standard of judgment for determining 'a person who may have a significant impact on National Security' is vague and is left to the NIS' discretion. In the case of the above-mentioned DPRK employees, the NIS continues to manage them at the Centre even though it is hard to consider their experience at a North Korean restaurant in China as having 'a significant impact on national security'.

B. Recommendations

- It is not appropriate for the NIS to have an administrative control over the Centre and to conduct investigations on DPRK defectors while collecting and managing relevant information without establishing specific criteria. It is necessary to establish a uniform management system for relevant information, including personal information of DPRK defectors, and have the Ministry of Unification, which is the ministry in charge of protection and settlement support for DPRK defectors, take responsibility of the work.

C. Responsible ministries and agencies

- National Intelligence Services
- Ministry of Unification

4) Infringement of Right to Privacy for Foreign Criminal Suspect[230]

4-1) Fire Accident of Oil Reservoir in Goyang-si

230 Written by MINBYUN-Laywers for a Democratic Society

A. Background

- On October 7th, 2018, one of the 14 outdoor gasoline tanks at Gyeongin branch office of Daehan Oil Pipeline Corporation in Hwajeon-dong, Goyang-si, Gyeonggi Province, exploded in a fire (hereinafter referred to as “Goyang Reservoir fire”). The Goyang Reservoir fire was a disastrous fire, and since the fire was caused by gasoline, it was very difficult to extinguish. The police pointed out a wind lamp blown by a foreign laborer several hours before the fire as a culprit for Goyang Reservoir fire and made an emergency arrest of the said foreign laborer on October 8th.
- The police disclosed to the press A’s name, nationality, age, occupation, income and location of arrest immediately after the emergency arrest of A.
- Goyang Reservoir fire was covered extensively by the press, receiving nationwide media attention. The press highlighted A’s nationality in the related news articles and continuously used the expression “person from OOO(country name)". Some media reported detailed personal information on A, including age, workplace and residence, and some media even went so far as disclosing A's face.
- The police continued to release A's statement and investigation details to the media, which was reported in real time.
- Problem of Police Department
    - According to the ‘Regulations on the Investigation Communication for the Protection of Human Rights (No. 774 of Directives of Ministry of Justice)’, when it comes to communicating about the case under investigation, only a minimum necessary to achieve the purpose should be disclosed and be disclosed in an accurate manner, and it should not commit human rights violation, such as causing injury to the honor of the person involved in the case or disrupting the investigation (Article 13). Therefore, in principle, the investigation team cannot disclose any and all details of the investigation, including the facts of the allegation and the investigation situation, before filing an indictment (Article 9). If the person involved in the case should be disclosed inevitably, anonymity should be used in principle, and disclosure of the details, such as the character and private life, criminal records, contents of a statement or any evidences of the person involved in the case, is prohibited unless there exists special circumstances (Article 19). Also, it is prohibited to discriminate, without any rational reason, on the grounds of gender, religion, age, disability, social status, region of birth, race, nationality, political opinion, etc. (Article 6).
    - The police disclosed the details of the Goyang Reservoir fire investigation to the press, even though the case did not satisfy the criteria for applying the disclosure exception, then the police released A's real name, nationality, age, occupation, income, and location of arrest. The police's disclosure of investigation information is a violation of the ‘Regulations on the Investigation Communication for the Protection of Human Rights as well as a violation of A's right to informational self-determination.
    - In particular, the police emphasized A's nationality and status of being a foreign laborer, and the press also highlighted such facts extensively. This is a discrimination on the grounds of region of origin, race, nationality and social status.
    - The National Human Rights Commission of Korea (NHRC) has issued a decision on May

17th, 2019, recognizing that the police has violated A's privacy.

- Problem of Press
  - The media violated A's right to informational self-determination by reckless reporting of A's personal information, which was released by the police.
  - According to the Reporting Guidelines for the Protection of Human Rights jointly prepared by the National Human Rights Commission and the Journalists Association of Korea, the press should exercise caution in its choice of terms and expression to prevent human rights violations due to stereotypes or social prejudice (Article 6 of the Reporting Guidelines for the Protection of Human Rights). In addition, the press should not promote negative images of, or discriminate against, the immigrants based on the flimsiest of evidence or an inaccurate speculation (Article 5 of the Code of Human Rights). However, the press focused its coverage intensively on A's nationality and the status of being a foreign laborer. For example, even though the wind lantern that A flew was a wind lamp used at the event of B Elementary School on the previous day, the name of B Elementary School was rarely reported, while the nationality of A was reported over a thousand times. Consequently, the press promoted a negative image of immigrants by focusing its coverage on the nationality of A and the status of being a foreign laborer, which had no relation to Goyang Oil Reservoir.

B. Recommendations

- Police must comply with the Regulations for Investigation Communication for the Protection of Human Rights. In addition, there is a need to find practical ways to impose sanctions on the press release in violation of the Guidelines for Investigation Communication
- It is necessary to find a way to compel the press to stringently comply with the Reporting Guidelines for the Protection of Human Rights

C. Responsible ministries and agencies

- Police Department
- Press Arbitration Commission Committee

5) Infringement of Right to Privacy for Children

5-1) Specific Student Record and National Education Information System[231]

A. Background

231 Written by ASUNARO: Action for Youth Rights of Korea

- Schools are required to make a “Specific Student Record” for each student. The problem is that excessive items are required, which results in the collection and recording of student’s detailed personal information.

1. Personal Data – Name, Sex, Resident Registration Number, Address / Name and birthdate of family member/ Special Note

2. Education Information – When a student entered or graduated which school.

3. Attendance – Number of School Days, Absence, Tardy, Early Leave, Casue (Disease/ Unexcused/ Other)

4. Awards

5. Certificates and Licenses– acquisition of certificates and licenses, Completiion of National Competency Standard

6. Career Interests

7. Creative Activities – Independent activities, volunteer, club activities, career activities, student body activities, special activities, etc.

8. Academic Information – Academic rating (grades) / Detail and special note for each subject

9. Reading Record (Until 2016, title of book and short report; since 2017, only title of book)

10. Behavioral characteristic and overall opinion (opinion of each home room teacher)

- This information recorded in the Special Student Report are collected and recorded without the student’s consent and there is no institutional method for the student to affect the process in anyway.
- This Special Student Report is saved at the online educational system named NEIS, which results in the government collecting every student’s personal data. Also, the information stored in NEIS can be viewed by parents or persons in charge even against the wishes of the students.
- The information collected in NEIS is preserved near permanently. The state is collecting student’s personal information without consent and is keeping them without a termination date.

B. Recommendation

- Reduction of information recorded on the Special Student Report
- Institutional method for the student to be involved in the contents of the Special Student Report, such as objection procedures or countermeasures.
- Procedures to limiting collection of personal information by NEIS against student’s with and limiting third-party, such as parents, access to such information against student’s wish.
- Procedures for discarding information in NEIS according to student’s wish.

C. Responsible ministries and agencies

- Ministry of Education

5-2) Routine violation of privacy through school regulation[232]

A. Background

- Routine privacy infringement, such as name badge, inspection of personal belongings and inspection of diaries, occurs in the name of school regulation or custom.
- Most school's regulation require students put on a fixed-type name badge to the uniform and also requires to wear uniform while commuting to schools. As a result, information such as the name of school in attendance, class, and name is exposed to many and unspecified people against the student's wish. In 2010, the National Human Rights Committee pointed this out as human rights violation, temporarily resulting in a decrease of such practice, but the practice of requiring fixed-type name badge has been increasing recently.
- In the "Factual Survey of Student's Human Rights Guarantee in Schools" conducted in 2016 by the National Human Rights Committee, 17.6% of the students surveyed responded that there was an inspection of personal belongings without consent. In areas where a Student's Human Rights Ordinance is in effect, this is prohibited, but in other areas, this occurs based on school regulation or school conventions.
- There is a strong tendency in elementary schools to require to write diaries and to inspect them. The National Human Rights Committee deemed this a human rights violation in 2008 but not much have improved since then.

B. Recommendation

- Effective national law such as Student's Human Rights Law that prohibits inspection of personal belongings, inspection of diaries, and name badges.
- Enactment and revision of school rules regarding student's life should require student's agreement.

C. Responsible ministries and agencies

- Ministry of Education

5-3) CCTV in Child Care Center[233]

A. Background

- In April 2015, the National assembly passed the Child Care Act, which required the installation of

232 Written by ASUNARO: Action for Youth Rights of Korea
233 Written by ASUNARO: Action for Youth Rights of Korea

CCTV.

- As a result, all activities of the children and employees at child care centers are recorded and violates the privacy of children and employees.
- In particular, privacy infringement is maximized due to repeated use of the recorded footage in media coverage on child abuse.
- Despite the requirement of CCTV installation, the total number of child care center abuse and the percentage of such abuse in total child abuse case has increased (National Child Abuse Status Report) and effectiveness of such policy is in question.

B. Recommendation

- Repealing CCTV installation requirement.
- There needs to be a realistic policy to improve education conditions such as improvement of teachers pay and respecting child's intention.

C. Responsible ministries and agencies

- Ministry of Interior and Safety/Ministry of Education

5-4) Privacy related to Sex[234]

A. Background

- According to the "Love is not prohibited under the age of 19 – Study on the Oppression of Teenager's Love" conducted by Asunaro in September~ November of 2010, 81.3 % of middle and high schools in Gwanak, Seoul and 86.7% of middle and high schools in Hwaseong, Gyeonggido have school rules with an article penalizing "indecent heterosexual relation," "indecent activity between boys and girls," contacting, expressing interest, meeting, physical contact between members of the same or opposite sex, sharing rooms, or sex. Such oppressive regulation regarding student's sexual privacy exists in many middle and high schools.
- There has been reports of schools attempting to trackdown LGBT students.

B. Recommendation

- National and effective Student's Human Rights Law that prohibits school's interference with student's sexual activities and discrimination of LGBT students.
- Enactment and revision of school rules regarding student's life should require student's agreement.

234 Written by ASUNARO: Action for Youth Rights of Korea

C. Responsible ministries and agencies

- Ministry of Education

5-5) The right to informational self-determination for children under the age of 14[235]

A. Background

- Under the Personal Information Protection Act Article 22 Paragraph 6, in order for a personal information controller to process the personal information of children under the age of 14, the consent of the child's legal representative is needed.
- According to the said Act's Enforcement Decree Article 17 Paragraph 4, the personal information controller can collect the child's legal representative's name and contact information from the child without the consent of the legal representative.
- According to these laws, the information of a child under the age of 14 is processed regardless of the child's intention.
- For example, in 2017, Chosun University conducted a research with government funding on the relationship between juvenile crime and genetics. In this process, the researchers collected 800 middle school student's biological and genetic information, such as epithelial cells from the oral cavity and tracked the student's development for 5 years, causing great concern the student's invasion of privacy. However, the University only received consent from the legal representatives, without regard to the student's opinion. As a result, NGO's have submitted a complaint to the National Human Rights Committee that such studies violate the privacy rights of children.

B. Recommendation

- In order to guarantee the right to informational self-determination for children under the age of 14, there needs to be a procedure to check the child's intentions, along with the consent of the legal representative. The method of providing explanation about personal information processing and checking the child's intention should take the child's age and development into account.
- In case of checking the child's intention is impossible, there should be a procedure for determining whether the consent of the legal representative is against the will of the child, based on the principle of the best interest of the child.

C. Responsible ministries and agency

235 Written by ASUNARO: Action for Youth Rights of Korea

- Ministry of Interior and Safety

5-6) Minor's Smartphone Monitoring Provisions and Smartphone Monitoring Apps[236]

A. Background

- The Telecommunications Business Act (TBA) and its Enforcement Decree came into effect on April 16, 2015, which made it mandatory for telecoms to install monitoring apps on minors' mobile phones. Article 32-7 of the TBA237 states that communications business operators must provide means to block harmful or obscene contents when selling mobile phones to juveniles, and prescribes any necessary matters to be specified in the Enforcement Decree. Article 37-8 of the Enforcement Decree238 sets out the procedure in more detail. The telecoms must inform juveniles and their legal representatives (normally the parents) about the blocking means, and check the installation of chosen means. However, the Decree does not stop here but further obligates telecoms to notify the legal representatives if the means was deleted or disabled for more than 15 days.
- "Blocking means" refers to a smartphone application. Most of those blocking apps currently on the market not only block harmful contents but also have features such as usage monitoring and location tracking that are excessively infringing on minors' privacy and collecting personal information.
    - Such spying or monitoring apps are often vulnerable and are targeted by hackers, thus exposing minors to security risks such as data breach and hacking. In particular, according to the Citizen Lab at Munk School of Global Affairs, University of Toronto239, the "Smart Sheriff" developed and distributed by the government had 26 security

236 Written by Open Net Korea
237 Telecommunications Business Act Article 32-7 (Blocking of Media Products Harmful to Juveniles) ① Any telecommunication business operator using allocated frequencies under the Radio Waves Act must provide the means to block the media products harmful to juveniles under Article 2 Subparagraph 3 of the Juvenile Protection Act and the obscene information under Article 44-7(1)1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. when entering into a contract on telecommunications service with a juvenile under the Juvenile Protection Act.
238 Enforcement Decree of the Telecommunications Business Act Article 37-8 (Methods and Procedures for Providing Means to Block Media Products Harmful to Juveniles, etc.) ① According to Article 32-7(1) of the Act, a telecommunication business operator entering into a contract on telecommunications service with a juvenile under the Juvenile Protection Act must provide means to block the juvenile's access to the media products harmful to juveniles under the Juvenile Protection Act and the illegal obscene information under Article 44-7(1)1 of the ICNA ("Information harmful to juveniles") through the telecommunication service on the juvenile's mobile communications device such as a software blocking information harmful to juveniles.
② Procedures prescribed below must be followed when providing the blocking means under (1):
1. At the point of signing the contract:
a. Notification to the juvenile and his/her legal representative regarding types, features, etc. of the blocking means; and
b. Check on the installation of the blocking means.
2. After closing the contract: Monthly notification to the legal representative if the blocking means was deleted or had not been operated for more than 15 days.
239 https://citizenlab.ca/2015/09/press-release-security-privacy-issues-in-smart-sheriff-south-korea/

vulnerabilities. In addition, apps offered by KT and LGU +, two of the three major telecoms in Korea, are also found to be vulnerable240.

- Minor's Smartphone Monitoring provisions require telecoms to install monitoring apps on minors' smartphones and allow them to monitor what information minors search and access and in consequence make them infringe the privacy of minors. Moreover, telecoms have to collect, store, and use the personal information of the minor and the legal representative (parents) and infringe on their right to informational self-determination. Furthermore, monitoring apps not only block harmful contents but also occasionally block legal and educational contents and this restricts the minor's right to access information. Lastly, the provisions do not allow the minor or the parent to opt-out and thus infringe on the parents' right to education of their children.
- Open Net filed a constitutional complaint on behalf of two minors and a parent in August 2016 and the case is currently pending at the Constitutional Court.
- Minor's Smartphone Monitoring provisions were introduced to protect children from harmful contents. Nevertheless, telecoms are required to install monitoring apps regardless of the will of a minor or his/her parent and notify the parent of removal or deactivation. Such a mandate is very paternalistic and unprecedented around the world.
- Moreover, when even stricter security standards should be applied to apps used by kids and teenagers needing protection, the government encourages the use of vulnerable apps, which could result in exposing more minors to security risks.

B. Recommendations

- Abolish the Minor Smartphone Monitoring provisions that greatly infringe on the privacy of minors.
- Establish security standards for smartphone monitoring apps (control apps) that expose minors to security risks, and conduct security audits on existing apps.

C. Responsible ministries and agencies

- Korea Communications Commission
- Korea Internet & Security Agency

6) The violations of the rights of privacy for the victims of sex crime by media coverages and the problems of publications of the crime facts[241]

A. Backgrounds

- The current situation of the violations of the rights of privacy of the victims of sex crime by

240 https://citizenlab.ca/2017/11/still-safer-without-kt-olleh-kidsafe-clean-mobile-plus/
241 Written by MINBYUN-Lawyers for a Democratic Society

media coverages in Korea.

- Recently, there have been many problems related to sex crime coverages in various sectors of Korean Society. For example, the media discloses personal information, such as the information of suspects, victims, the family members of victims, and so on, or reports private areas not suitable for the coverages.
- The media uses a person's real name when they report-by using a title, such as 'ooo(a person's name) case'- without concerning whether the person is an ordinary person or a celebrity, which can stigmatize the person socially.
- The distortion of facts is happening and it can spread immediately through Internet and social medias
- At this time, the violations of the rights of privacy of suspects, victims or a close person, such as a family member

- The victim's civil lawsuits for remedy
  - Even though the victims of the sexual crime coverages, whose privacy rights are violated, can file a civil lawsuit against disseminators -compensation of damages, or deleting the news articles, it is difficult for the victims to get a timely relief. The reparation of the rights of privacy is also difficult since the personal information already spreads extensively in most cases.
  - In 2012, there was a case that an elementary school student was raped by a man in Naju, Korea. In the case, the victim and the family members filed a civil lawsuits against the media and the court ordered the compensations and delete some of the coverages' contents.
  - In this lawsuit case, the court recognized that the media violated the victim's privacy rights extensively by reporting following contents without anyone's consent: ① Satellite photos and the broadcasting of disordered condition of the house- both inside and outside-through the windowed door ② Broadcasting of the victim's wounded face, the trace of violence, such as the tooth marks bitten by the perpetrator ③ Victim's picture diary, book review, the drawings on notes that were not related to the crime.
  - However, it has taken much time to get the final decision of the court: The decision of the first trial was announced in 2014 and the decision of the second trial was declared in 2015.

- Regulations through sanctions, corrective orders, etc.
  - There are regulations, such as the review of broadcasting by the Korea Communications Commission according to Broadcasting Act and Broadcasting Review Code, and corrective orders by press arbitration commission according to the Act on Press Arbitration and remedies, etc. for Damage Caused by Press Reports
  - These regulations provide rapid sanctions and recommendations compared to civil lawsuits. However, these regulations also suffer from inevitable limitations as after-the-fact remedies and the reparation of the victim's rights are not sufficient.

- There are no regulations on one-person media, such as a media using YouTube, in addition to the civil and criminal procedures.
- The consideration of regulatory means to foreign and platform operations is also necessary.

- Self-regulations of the media and the publication of facts of suspected crimes by investigative agencies
  - Each media has its own coverage guidelines, broadcasting guidelines, codes of ethical standards, and so on. However, the self-regulations often do not work well due to the nature of self-regulations.
  - The publication of facts of suspected crimes are regulated not by laws, but by administrative rules. It results in the extensive publications of facts by investigative agencies and therefore there have been many violations of suspect's personality rights.
  - The Criminal Act criminalizes the wrong publication of facts of suspected crimes by investigative agencies, no indictment was made for prosecution cases during the period from 2013 to August 2018 according to the report which Ministry of Justice submitted to the National Assembly.

B. Recommendations

- There are concerns that it may violate the freedom of expression if the law regulates and restricts the broadcastings or coverages of the media in advance. Therefore, the self-regulations of the media should be preferred. Provide specific plans to prevent the violations of privacy rights when the self-regulations fail
- Provide specific plans to prevent the violations of privacy rights by one-person media.
- Provide specific plans to prevent the violations of privacy rights by foreign and Platform operators
- Provide information related to the specific plans that can prevent the violations of personal rights of suspects due to the unjust publication of the facts of suspected crimes by investigative agencies

C. Responsible ministries and agencies

- the Korea Communications Commission
- Press Arbitration Commission
- Ministry of Culture, Sports and Tourism
- Ministry of Justice

7) Privacy of Women[242]

Online Gender-Based Violence and Privacy

A gender-based approach must be adopted regarding the right to privacy. In any case, infringements of women's right to privacy should be regarded as a grave violation of fundamental rights, whether the perpetrator is the state, a corporation or an individual. Privacy principles must be applied to include the experiences of women in contemplating privacy. However, the Korean discourse on the right to privacy has rather excluded women in its discussion.

The Korea Cyber Sexual Violence Response Centre (KSCVR) mainly focuses on "cyber sexual violence". Cyber Sexual violence is a form of online gender-based violence, which violates numerous rights, the right to privacy included. Women's right to privacy is adversely affected in online spaces. Cyber sexual violence cases illustrated below demonstrate that cyber sexual violence itself is a grave violation of the right to privacy.

In the cases of violation of women's right to privacy perpetrated by "male users", it can be seen that women's personal data are collected and processed without regard to due process. Women do not possess means to overlook how and for what purposes their data is collected. Women do not possess the right to demand access to, correct or remove their personal information. Online platform businesses and the state have yet to adopt measures to protect women's right to privacy.

The invasion of women's right to privacy has long been regarded as "men's rights" or as "inevitable". Even today, efforts to protect women's right to privacy are often taken as attempts to oppress "freedom of speech" or "men's right to privacy".

For instance, measures to block access to websites which existed to distribute non-consensual intimate images and therefore where manifest violations of privacy occurred, faced heavy resistance by male users on the ground that such measures were a "violation of the freedom of speech" and an "infringement of privacy". The argument went that blocking access to such websites which its main users are men, will result in violating male internet user's privacy. Through this argument, it can be observed that while the principle that privacy must be absolutely protected even in the state of a mere possibility of its violation, is applied to men, women who are already experiencing actual concrete violations are excluded from its application.

Furthermore, violations of women's right to privacy have become a means of profit under the current misogynistic social structure. The Korean society has long uncritically perceived non-consensually distributed intimate images as a genre in pornography, leading to a formation of an industry which deals with such images as its main product. In 2018, the relationship between businesses that take advantage of such violations of women's privacy to raise profit was exposed and has been named as the "Web-Hard Cartel".

There is a need to further expose the violations of women's right to privacy occurring in Korea and to further re-establish the concept of the right to privacy to include women's experiences. Korea must "adopt an intersectional approach that recognizes the specific benefits,

242 Written by Korean Cyber Sexual Violence Response Center

experiences and threats to the right to privacy according to gender, and overarching privacy and human rights principles."[243]

In addressing gender-based violence in online spaces, public intervention towards the invasion of privacy between individuals and infringements between individuals and businesses plays a crucial role. The existing discussion on invasion of the right to privacy which focused on corporation and state power as the main perpetuator, must be expanded be able to address the current rape culture. To women, rape culture is equivalent to the notion of Big Brother. When corporations and the state neglect and condone its existence, the scope of battle for women's right to privacy inevitably expands from corporations and the state to include individual internet users.

The current status quo cannot be adequately addressed by superficial temporary measures. The state must establish the view that one is not granted extraterritorial rights in online spaces, and everyone holds the right to be protected from infringements of privacy online. Based on a holistic understanding of online spaces, the state must establish a state level vision and adopt systematic and comprehensive measures to end violence against women.

7-1) Violations of women's right to privacy perpetrated by male internet users

A. Background

- Violations of right to privacy using private sexual images
- According to the Supreme Prosecutor's Office, for the past 10 years, the percentage of sexual crimes committed through cameras has seen the largest increase out of all sexual crime cases. In 2008, camera-based sexual crimes have accounted for 4.6% out of all sexual crime cases, but has steadily increased to reach 24.9% in 2015. The number declined to 17.9% in 2016, but again increased to 20.2% in 2017. Camera-based sexual crime case statistics include illegal filming and distribution. There are two types of illegal filming; one which takes place in daily public spaces such as bathrooms, public transportations, and the other which takes place in private spaces to film sexual acts.
    - From 30 April 2018 to 31 December 2018, the Digital Sexual Violence Victim Support Centre of the Women's Human Rights Institute of Korea under the Korean Ministry of Gender Equality and Family, reported 5,687 cases of violation. Among them, 2,267 were regarding non-consensual distribution of sexual images online. The Centre reported to have deleted 28,879 posts containing non-consensual sexual images.
    - The "2018 Digital Sexual Violence Victim Support Report" was drafted based on these 28,879 posts. One out of every five posts contained information identifying the victim. Breaches of personal data through non-consensual distribution of sexual

243 27 February 2019, Joseph Cannatacithe, Special Rapporteur on the rights to privacy [The right to privacy: a gender perspective – Report of the Special Rapporteur on the right to privacy]

images were found in 6700 cases, accounting for 23.2% of all cases. Publicly disclosing the victim's name was the most common in personal data breach cases (47.8%), followed by the revealing the victim's nickname (23.7%), and address (9.3%).

- Over half of the reported victims experienced multiple forms of victimizations including non-consensual filming, distribution, threats to distribute intimate images and cyber-bullying. In cases where the perpetrator intended to use sexual images to exercise control over the victim, in 803 cases (14.1%), the victims faced threats to further distribute intimate images. As warrants of search and seizure or arrest are seldom issued, the perpetrators often eliminate evidence, or distribute the images.
- The victim subject to threats to distribute intimate images suffer from anxiety that the image will be distributed regardless. Because the perpetrator possesses the image file, there is a huge difficulty in nullifying the perpetrator's threat. There are no accessible measures in the current criminal law for the victim to assert control over control intimate images of themselves owned by others, and therefore the perpetrators are not legally obliged to delete the images.
- Children and teenagers are exposed to online sexual grooming through stranger chat apps, and often send intimate images of themselves to perpetrators. In some cases, by the child or teenager reports to a victim support center, over 200 body or masturbation images are already sent. The perpetrator who gains these images through such online grooming uses these images to threaten the victim into handing over more images, or sells them to overseas hosted websites. There is no law penalizing online grooming itself. Such cases can be legally dealt with when additional victimization occur such as when the perpetrator threatens to distribute or actually distributes the images.
- The Digital Sexual Violence Victim Support Centre under the Ministry of Gender Equality and Family does not provide deletion support to minors without their legal guardian's consent. In other words, after the images are distributed, minors must notify their legal guardians in order to access support. Therefore, justice is inaccessible to underage victims who face difficulty in notifying their legal guardians.
- Cybercrime is condoned because the state cannot specifically identify the perpetrator. There are cases where the investigative authorities assert that "the perpetrator cannot be charged unless the victim themselves can identify the perpetrator". Even after taking into account such instances where the victim's report itself is rejected and the perpetrators are not charged, only in 52 cases out of 164 cases reported from January 2018 to August 2018, charges were made against perpetrators (total 66 perpetrators charged).

Case 1. An adult male user approached the victim on a stranger chat application, a 15-

year-old female teenager. At first, he requested the victim's name, age, attending school and intimate images showing the victim's face. The perpetrator then requested photos of the victim's genitals, which the victim declined. Then, the perpetrator threatened to distribute the photos of the victim's breasts, and threatened the victim that the victim could not take legal measures against him as the images were voluntarily sent. Due to such threats, the victim had to send genital photos to the perpetrator on demand.

Case 2. The victim, female, filmed intimate videos with her male partner based on the promise that they would delete the videos at the end of their relationship. However, the victim was notified by a friend that the video was widely distributed online, with over ten thousand hits on multiple websites, many of which contained comments that harassed or mocked the victim. The victim tried to delete the video, but despite repeated attempts, the video continued to spread. The victim felt discouraged and suffered from despair that she would face perpetual victimization.

- Violations of right to privacy through the distribution of manipulated sexual images
  - Women's images uploaded on social media, or profile pictures on chat apps are collected without consent to be manipulated as sexual images. Forms of such abuse include merging the victim's face with a naked body of another women, graphically adding semen onto a facial image or editing the facial expression to implicate sexual activity. Because the perpetrator is a male acquaintance in most cases, such acts are also referred to as 'acquaintance shaming (raping)'. The victim's personal information is distributed along with the image. In many cases the victim is subject to intense cyber-bullying as other users are openly encouraged to join in in the harassment. Such posts often contain false defaming information. After upload, the post is circulated through comments and shares, gathering numerous additional sexual insults.
  - According to the Digital Sexual Violence Victim Support Centre's victim support cases from 30 April 2018 to 31 December 2018, image manipulation accounted for 153 (2.7%) cases out of total 5,687 cases and cyber-bullying accounted for 251 (4.4%).
  - The distribution of such images often occurs in anonymous open chat rooms. The access to such chat rooms are circulated among male users. Therefore, the victim cannot grasp how much and where their personal data is distributed. Because the breach of privacy occurs beyond the victim's knowledge, the aforementioned data (2.7%) should be regarded not as the total cases of occurrence, but rather the total cases perceived.
  - Manipulating images is not punishable by the Sexual Crime Act. Laws on cyber defamation or insult may be applied. Therefore, the victim cannot assert the rights as a victim as provided in the Sexual Crime Act. The victimization is regarded as

trivial on the grounds that the original image was taken by the victim.

Case 1. A group chat in the chat application Telegram consisted of around 300 people who gathered photos of their female acquaintances to manipulate into sexual images in order to harass the victims. One male user uploads an image and other users download and reupload the image with their genitals or semen added into the picture. In this case, one user broke into the victim's school, ejaculated onto the victim's gym kit, and uploaded the pictures on the group chat. The users would help manipulate each other's acquaintance's photos, trade or sell such images.

- Violation of the right to privacy by Cyber stalking
  - Online stalking manifests in collecting and processing the victim's personal data without consent. Stalking includes not only attempts of unwanted contact, verbal assault and threats made through online forums, direct messaging, emailing and other methods of communication, but also stealing personal data and online impersonation.
  - Due to lack of effort and expertise on the part of the cybercrime investigative agencies, tracking and identifying the anonymous perpetrator remain difficult. There is no law directly applicable to stealing images and to online impersonation.

Case 1. An anonymous perpetrator repeatedly harassed the victim through messaging on social media by sending sexual images and messages. The perpetrator posted images of the victim's daily lives filmed secretly. Every time the account was reported and taken down; the perpetrator simply opened a new account to harass the victim. Furthermore, the perpetrator used the victim's images to impersonate the victim and uploaded the victim's personal information on an internet prostitution website. The victim had no effective accessible means to stop the messages and the continuous distribution of her personal data and images online.

B. Recommendations

- Increase resources and adopt capacity building measures to enhance cybercrime investigation capabilities
- Penalize possession and implement measures to assure deletion, take action to guarantee victim's rights to control their own images
- Adopt a support system which provides support to minors who cannot gain consent from or are unwilling to notify their legal guardians
- Take legal action to penalize the distribution of and threat to distribute manipulated sexual images

- Take Proactive steps to prevent violations of right to privacy occurring beyond the victim's knowledge

C. Responsible ministries and agencies

- National Police Agency
- Ministry of Justice
- Ministry of Gender Equality and Family
- Ministry of Science and ICT
- Korea Communications Commission

7-2) Traffic in Women in Online Platforms

A. Background

- Korea bans the display and distribution of 'obscene material', but at the same time 'domestic pornography' has flourished. Films containing intimate activities of actual couples, most of them filmed without the women's consent are widely distributed and has been established as a genre and preference in pornography. Such private material filmed and distributed without consent are named 'domestic pornography'.
- Since 2000, such demand for and distribution of 'domestic pornography' led to the creation of a massive industry. The increased accessibility of digital devices such as tablets and smartphones along with Korea's fast improving internet technology accelerated the growth of the 'domestic pornography' market.
- The non-consensual distribution of sexual images, which is a collective crime committed by all those who participate in its production, creation and consumption has been conceived as a male recreational activity, and men have perceived the consumption of 'domestic pornography' as a right. It must be noted that it is precisely this social context in which 'domestic pornography' became an industry where men could legally purchase 'domestic pornography' that gave rise to and fueled such conception.
- Some cases that demonstrate this conception are as such. As the Telecommunications Business Act was amended in 2014 to demand web portals, peer to peer file hosting websites ("Web-Hards") and social media to implement a filtering system to restrict search results for "domestic pornography", male user dominated websites attacked the amendment, referring to the legislation as "masturbation regulation law".
- These users argued that the rise of the internet "democratized" the access to non-consensual intimate images, and therefore, such regulations are regressive as they infringe upon men's fundamental right to sexual pleasure and perpetuates economic

inequality in accessing sexual material. Such arguments are manifestations of what Gayle Rubin referred to as 'the traffic in Women' (2011/2015). According to Rubin, women are objectified as items for trade to strengthen the homosocial bond between men. Online platforms distributing non-consensual intimate images are a modernized manifestation of traffic-in-women. Internet amplifies the scope of influence of non-consensually distributed images, which then allows such images to reproduce oppressive images of women's sexuality and ultimately expands the scope of women traded by men.

- Web-Hards
  - Web-Hards are domestic file sharing platforms, which raise profit through distributing non-consensually shared intimate images. For every copyrighted content, 70% of the profit is vested to the copyright owner, and the remaining 30% of the profit is shared among the Web-Hards and the content uploader. However, in the case of non-consensually shared intimate images, Web-Hards can take 70% of the profit, because these images are not copyrighted – rendering non-consensual intimate images a huge source of profit.
  - Furthermore, Web-Hards began to gather non-consensually distributed intimate images themselves or hired 'heavy-uploaders' who specialised in uploading such content. As such, Web-Hards were able to seize full profit arising from the distribution of non-consensual intimate images.
  - The KCSVRC's 2017 Web-Hard monitoring data shows that over a million 'domestic pornography' was distributed, and each Web-Hard distributed over ten thousand 'domestic pornography' on average. One leading Web-Hard website's reported income statement exceeded 30 billion KRW, while the leading Web-Hard enterprises' income surpassed 100 billion KRW.
- Offshore Hosted Pornographic Websites
  - Offshore hosted pornographic websites are illegal websites which use foreign servers in order to evade domestic law and investigative authorities, and therefore can be more audacious in distributing non-consensual intimate images. Such websites distribute massive amounts of non-consensual material, advertising them with keywords such as 'domestic porn', 'non-professional porn', 'leaked porn', 'minor porn'. One of the most well-known websites is "Soranet". Soranet had over a million registered users that gathered to share secretly produced images of their female family members and friends. The website was taken down in 2016 due to public indignation, but numerous similar websites remain operative. Among the 206 victims the KCSVRC supported, over 300 offshore hosted pornographic websites were found distributing the victim's images.
  - Such websites raise profit through Bitcoin, arranging prostitution, advertising sex toys and gambling services. In the case of Soranet, it raised over 10 million KRW

worth of advertisement profits daily.

B. Recommendations

- Implement the 'UN Guiding Principles on Business and Human Rights' and avoid infringing on the human rights of all persons affected by their practices, with effective consideration of the gender-specific impact of their activities.
- The current law punishes business operators for knowingly refusing to take action while being clearly aware of distribution of illegal material on their reported business by a fine not exceeding 20 million KRW. This measure lacks efficacy due to the industry's massive profitability. The current law needs to be amended to effectively regulate illegal online platform businesses.
- Increase responsibility of online platform businesses for a sustainable online platform culture even regarding misogyny and areas of not yet criminalized forms of violence against women.
- A systematic measure is required to concretely block access to offshore hosted pornographic websites distributing illegal information, to arrest the website operator and to close down the website for the sake of the victim's right to remedy.

C. Responsible ministries and agencies

- Ministry of Justice
- Ministry of Science and ICT
- Korea Communications Commission
- Korean Communications Standards Commission
- National Police Agency