

진보네트워크센터, 제19대 대선 정보인권 10대 정책과제 제안

“우리는 정보인권 대통령을 바란다!”

대부분의 대통령 후보들이 “4차 산업혁명”을 얘기합니다. 그러나 우리는 대통령 후보들이 얘기하지 않는 것을 묻고자 합니다. 당신의 정보인권 정책은 무엇입니까?

빅데이터는 나에게 최적화된 서비스만 제공하지 않습니다. 내 개인정보가 나도 모르게 거래되고, 내 구매능력을 평가하는데 이용됩니다.

인터넷과 핸드폰은 더 쉽게 정보에 접근하고 다른 사람과 교류할 수 있는 능력을 가져다 주었지만, 정보·수사기관에게도 시민들을 무차별 감시할 수 있는 능력을 주었습니다.

인터넷이 처음 등장했을 때 사람들은 직접 민주주의의 가능성을 얘기했지만, 인터넷에 대한 검열과 통제는 그러한 가능성을 제약하고 있습니다.

정보인권을 외면한 4차 산업혁명은 박근혜식 창조경제와 다르지 않습니다.
진보네트워크센터는 제19대 대선 후보들에게 정보인권 10대 정책과제를 제안합니다.

제19대 대선, 정보인권 10대 정책과제

개인정보 보호

1. 개인정보 보호위원회의 독립성과 권한 강화
2. 빅데이터 시대 개인정보보호 강화
3. “개인정보없는 임의번호로” 주민등록번호 제도 개혁

정보, 수사기관 개혁과 사이버 사찰 금지

4. “해외정보 전담기관으로!” 국가정보원 개혁
5. “국정원은 손떼라!” - 사이버 보안은 일반 행정부처에서
6. 사이버사찰금지법 제정
7. 경찰의 무차별 개인정보 수집 통제

인터넷 표현의 자유 보호

8. 방송통신심의위원회 통신심의 폐지
9. 인터넷 실명제는 이제 그만!

다자간 거버넌스 활성화

10. 다자간 주소자원 거버넌스 활성화

특히, 10대 정책과제 중 다음은 정부조직 개편이 필요하기 때문에, 차기 정부 출범과 함께 이행할 것을 촉구합니다.

- 개인정보 보호위원회의 독립성과 권한 강화
- "해외정보 전담기관으로!" 국가정보원 개혁
- "국정원은 손떼라!" - 사이버 보안은 일반 행정부처에서
- 방송통신심의위원회 통신심의 폐지
- 다자간 주소자원 거버넌스 활성화

제19대 대선, 정보인권 10대 정책과제 요약

1. 개인정보 보호위원회의 독립성과 권한 강화

2011년 개인정보보호법 제정에 따라 개인정보보호위원회가 설립되었음. 그러나 인사와 예산의 독립성이 없을 뿐만 아니라, 국제적인 기준에 비추어 보았을 때 그 권한이 매우 제한적임. 행정자치부는 개인정보보호법 주무부처로서 실질적인 감독권한을 가지고 있음. 그러나 행정자치부는 스스로가 방대한 개인정보의 보유, 운영 주체로서 개인정보의 이용과 보호라는 상충된 이해관계를 가지고 있음. 개인정보 비식별조치 가이드라인을 제정하여 정보주체의 동의권을 무력화하고, 주민등록번호 체제 개편에는 소극적인 등 개인정보 보호에 역행하는 입장을 보여왔음. 행정자치부의 개인정보 감독권한을 개인정보보호위원회로 이관하여 민간과 공공부문의 통합적인 감독권을 부여하고, 인사권과 예산의 독립성을 보장해 명실상부한 개인정보의 컨트롤타워의 역할을 수행할 수 있도록 해야함.

2. 빅데이터 시대 개인정보보호 강화

대규모 개인정보 유출 증가에도 불구하고, 여전히 공공과 민간영역의 마케팅 활용을 위한 개인정보 수집과 집적, 공유가 증가하고 있음. 최근에는 흠플러스 및 IMS코리아 사건처럼 정보주체 모르게 개인정보가 유상판매 되면서 소비자들에게 큰 충격과 분노를 안겼음. 이러한 상황에서 정부는 오히려 통신·금융·의료 등 빅데이터 산업의 활성화를 위해 '개인정보를 비식별 조치'하면 동의 없이 개인정보 수집·이용·제3자 제공을 허용해 정보주체인 소비자와 이용자의 개인정보 자기결정권을 침해하고 있음. 매매 등 개인정보의 목적외 이용 규제, 개인정보 처리 로직에 대해 설명을 요구할 수 있는 권리, 프로파일링을 거부할 수 있는 권리, 생체정보를 민감정보로 특별히 보호 등의 내용을 법률에 포함하여 빅데이터 시대에 정보주체의 권리가 실효성있게 보장되도록 해야 함.

3. "개인정보없는 임의번호로" 주민등록번호 제도 개혁

주민등록번호는 서로 다른 개인정보 데이터베이스를 연결하는 열쇠로서 유출되거나 도용될 경우 그 피해가 막대함에도 불구하고, 지금까지 공공 및 민간 영역에서 무분별하게 수집되어 왔음. 거의 전 국민의 주민등록번호가 유출된 상황에서 이에 대한 근본적인 개혁이 없다면, 개인정보가 보호될 것이라는 사회적 신뢰가 낮아지고 이는 정보통신 서비스의 발전에도 저해가 될 것임.

2014년 8월, 국가인권위원회가 권고하였듯이, 주민등록번호의 체계는 △ 개인정보를 포함하지 않는 임의의 일련번호로 개편되어야 하고, △ 유출된 주민등록번호의 변경은 정보주체가 원할 경우 폭넓게 허용되어야 하며, △ 주민등록번호의 수집을 더욱 제한하는 방향으로 주민등록번호 제도가 개혁되어야 함.

4. "해외정보 전달기관으로!" 국가정보원 개혁

국가정보원은 박근혜 정부 들어서만해도, 2012년 대선 댓글 조작을 비롯한 선거 개입, 간첩 증거 조작, 이탈리아 해킹 프로그램 운용, 고 김영한 업무일지에서 드러난 민간인 사찰 등 수많은 정치개입과 권력 남용을 통해 우리 사회 민주주의와 인권을 심각하게 훼손해 왔음. 이는 국가정보원이 다른 나라 정보기관과 달리 정보권한과 더불어 수사권을 함께 보유할 뿐 아니라 국내와 해외 정보권한을 모두 독점하고 그 권한을 자의적으로 남용하는데 따름. 국정원은 여기서 그치지 않고 테러 대응, 사이버 보안 등 새로운 비밀 권한을 계속 확대해 왔음. 이탈리아 해킹 프로그램인 RCS 운용 사실이 드러났음에도 불구하고 국회가 진상규명에 실패한 것과 같이, 국회 및 법원을 비롯한 우리 사회의 국정원 감독기능은 유명무실한 상황임. 국정원에 대한 신뢰 회복을 위해서는 셀프개혁이 아니라 구조적인 개혁이 필요함. 국정원의 수사권, 국내보안정보 수집권, 기획조정권한을 폐지하고, 해외정보 전달기관으로 전문화해야 함. 또한, 국회 정보위원회의 전임·상설화 등 국회의 감독 권한을 강화해야 함.

5. "국정원은 손떼라!" - 사이버 보안은 일반 행정부처에서

국정원은 국가정보통신망에 대한 사이버보안을 담당하고 전반적인 사이버보안 컨트롤타워 역할을 하고 있음. 개인의 정보보안에서부터 인터넷 상의 사기나 해킹 등 민간 부문의 사이버 보안이 대부분을 차지하는 것을 고려할 때, 국정원이 사이버보안을 담당하는 것은 국정원의 직무범위에 벗어날 뿐만 아니라, 민간과의 협력을 저해하고 은밀한 감시와 사찰의 우려를 불러일으키고 있음. 세계 어느 나라에서도 비밀정보기관이 사이버 보안의 실질적인 컨트롤타워 역할을 맡고 있는 나라는 없음. 이에 현재 국정원이 담당하고 있는 사이버보안 역할을 투명하게 운영될 수 있는 일반 행정부처로 이관할 필요가 있음.

6. 사이버사찰금지법 제정

인터넷과 스마트폰이 시민들의 일상적인 소통수단으로 자리잡은 반면, 그만큼 개인의 사적인 데이터와 통신이 정보·수사기관에 노출될 위험성도 증가하고 있음. 특정 장소의 기지국의 통신내역정보를 싹쓸이해서 가져가는 '기지국 수사'는 집회 참가자를 추적하는데 이용되고 있고,

카카오톡과 같은 SNS 압수수색으로 범죄 혐의와 관계없이 민감한 통신 내역과 내용이 정보·수사기관의 사이버 사찰의 수단이 되고 있으며, 수사편의를 위해 통신사가 보관하고 있는 가입자 정보가 영장도 없이 제공되고 있음. 비록 범죄수사 등을 목적으로 통신정보에 대한 수사가 필요함을 인정하더라도, 이는 예외적으로 제한된 범위에서만 허용되도록 엄격한 요건과 절차가 보장되어야 함. 가입자 정보 요구시에도 영장주의가 적용되어야 하고, 감청, 압수수색, 위치정보, 통신자료 제공 등의 요건을 엄격하게 강화해야 하며, 과도한 사찰과 감시를 가능하게 하는 인터넷 패킷감청, 실시간 위치추적, 기지국 수사는 제한되어야 함.

7. 경찰의 무차별 개인정보 수집 통제

철도노조 조합원에 대한 건강보험 무영장 자료제공 사건과 장애인·활동보조인에 대한 저인망식 싹술이 자료제공 사건과 같이, 경찰은 공공기관으로부터 국민 개인정보를 제한없이 제공받아 왔으며 때로는 법원의 영장도 없이 민감한 건강정보와 수천 수만명에 달하는 방대한 양을 제공받아 왔음. 또한, 경찰은 통합관제센터 CCTV 영상정보를 법적 근거 없이 관제하거나 집회 감시 등 수집목적 외로 활용해 왔으며 드론이나 바디캠 등 이동형 영상장비를 도입하거나 개인정보 수집장치의 데이터베이스화, 지능화 및 첨단화를 추진할 때 이에 대한 입법적 통제가 전혀 이루어지고 있지 않음. 수사기관이 개인정보 수집에 대해 영장주의를 적용하는 등 사회적 통제와 감독 장치의 마련이 필요하며, 경찰의 국민 영상정보 및 개인정보 수집과 운영을 법률에 따라 통제해야 함.

8. 방송통신심의위원회 통신심의 폐지

방송통신심의위원회는 불법정보 뿐만 아니라, 유해 및 건전성의 기준으로 인터넷 상의 콘텐츠를 폭넓게 심의하고 있음. 2016년 사드 배치를 비판하는 게시물이 삭제된 것과 같이, 정부 정책이나 권력자에 대한 비판 등 정치적 표현의 자유를 침해하는 결정을 내리거나, 트위터 계정에 대한 차단과 같이 인터넷의 특성에 부합하지 않는 자의적 심의로 계속 논란을 빚어 옴. 사법부의 판단도 없이 행정기구가 자의적으로 인터넷 상의 게시물을 삭제, 차단하는 것은 국가의 검열로서 이용자의 표현의 자유와 정보 접근권을 침해하는 것임. 유엔이 권고한 바와 같이, 정치적, 상업적 및 기타 부당한 영향력으로부터 자유로운 독립기구로 방심위의 통신심의 권한을 이양해야 함. 또한, 방송통신위원회의 시정명령 권한을 폐지하고, 유해성 심의를 금지하는 등 심의대상도 축소해야 함.

9. 인터넷 실명제는 이제 그만!

2012년 헌법재판소 위헌 결정으로 인터넷 게시판 실명제는 폐지되었지만, 공직선거법, 청소년보호법 등 여전히 본인확인을 의무화하는 법령이 남아있음. 강제적인 인터넷 실명제는 이용자의 표현의 자유뿐만 아니라 이용자의 자기정보통제권 역시 침해하고 있으며, 국정원 댓글 사건이나 최순실 대포폰에서 볼 수 있다시피 의도적인 불법 행위를 방지하는 효과가 없음. 한국 정부는 해외에는 유례가 없는 본인확인기관 및 아이핀(I-PIN) 제도를 통해 인터넷 상 실명확인을 사실상 부추기고 있음. 여전히 남아있는 본인확인 의무화 법령과 본인확인기관 제도를 폐지하고, 통신사업자의 주민등록번호 수집을 금지해야 함.

10. 다자간 주소자원 거버넌스 활성화

전 세계적으로 주소자원 거버넌스는 국제인터넷주소관리기구(ICANN)를 중심으로 다수 이해당사자의 참여와 합의를 기반으로 운영되고 있음. 한국에서도 초창기에는 다자간 주소자원 거버넌스가 이루어졌으나 2004년 <인터넷주소자원에관한법률> 제정으로 인해 정부주도의 거버넌스로 전환됨. 이는 국제적인 추세에도 맞지 않을 뿐만 아니라, 국내 및 국제 거버넌스 공간에서 다양한 민간 이해당사자의 자발적인 참여를 제약하는 요인이 되고 있음. 현재 한국인터넷진흥원(KISA)이 담당하고 있는 국내 주소자원 관리 업무를 민간기구가 수행하도록 독립시키고, 정부주도의 인터넷주소정책심의위원회를 상향식의 다자간 거버넌스 기구로 개편하도록 주소자원법 개정이 필요함.

제19대 대선, 정보인권 10대 정책과제

1. 개인정보 보호위원회의 독립성과 권한 강화

<현황>

- 2011년 개인정보보호법 제정에 따라 개인정보 감독기구로서 개인정보보호위원회가 설립(법 제7조 등)
- 구성 - 보호위원회는 위원장 1명, 상임위원 1명을 포함하여 3년 임기 15명 이내의 위원으로 구성하고 유일한 상임위원은 정무직 공무원(행자부)으로 임명. 위원 중 5명은 국회, 5명은 대법원장 지명, 5명은 정부 임명
- 독립성에 대한 국제 기준 - 2013년 유엔 총회가 “국가 감시를 감독할 독립적이고 효과적인 감독기구를 설립할 것”을 각국 정부에 권고하는 결의안을 채택하는 등 독립적인 개인정보 감독기구의 설립은 국제 인권규범의 하나로 부상하고 있음. 유엔은 일찌기 1990년 <UN 컴퓨터화된 개인 정보파일의 규율에 관한 지침>에서 "모든 국가들은 열거된 원칙들의 준수를 감시할 독립된 기관을 설치"하도록 결의하는 등 개인정보 감독기구의 독립을 국제사회에 권고해 왔으며, 개인정보 보호 기준을 국제적으로 선도하는 유럽연합은 <개인정보보호에 관한 유럽의회와 각료회의 지침(95/46/EC)> 제28조(감독기관), 2016년에 제정된 유럽개인정보보호규정(GDPR) 제52조(독립성) 에서 (감독기관은) "자신의 임무와 권한을 완전히 독립적으로 수행한다"고 규정하였음
- 특히 2001년 유럽이사회(Council of Europe)가 채택한 「감독기구와 국경 간 정보이동과 관련한 개인정보의 자동처리에 관한 개인 보호 협약의 추가의정서」에서는 개인정보보호 감독기관에게 필요한 구체적인 권한으로 △정보제출 요구를 포함한 조사권(investigation) △개인정보수집자에게 수정, 삭제, 폐기를 명령할 수 있는 권한, 개인정보의 유통금지 명령권, 국회나 기관에 대한 의견제시권, 공표권, 분쟁조정 권한, 침해신고의 접수 등 개입권 △법적 절차를 개시할 권한 혹은 사법기관에 소추할 권한 등을 포함하고 있음. 또한, 개인정보보호 감독기관은 이러한 권한을 완전히 독립적으로 수행해야 하는데, 이에는 감독기관의 구성, 위원의 임명방법, 임기와 해촉 조건, 충분한 자원의 배분, 외부 명령없이 결정을 채택할 수 있는지의 여부 등이 관련됨.
- 권한에 대한 국제 기준 - 세계 여러나라 개인정보 보호 관련 감독기관은 정책 기능과 시장 및 공공부문의 감독기능, 위법시정 및 권리구제 기능, 그 외에 교육, 홍보, 연구 등의 기능과 개인정보처리와 관련한 등록과 같은 행정기능을 갖고 있음. 외국의 개인정보 보호 감독 및 감독기관은 대부분 종합적인 개인정보보호 관련 감독기관으로 설립되어 운영되고 있음.

- 감독기구의 독립성과 권한은 세계적 차원에서 비즈니스를 수행하는 국내 기업의 활동에도 영향을 미칠 수 있음(대통령 산하 개인정보보호위원회의 지적. 2017. 1).
유럽개인정보보호규정(GDPR) 전문 104는 유럽연합 시민의 개인정보에 영향을 미칠 수 있는 제3국의 개인정보 보호수준에 대한 평가 이슈를 다루고 있는데, “해당 제3국은 유럽연합 내에서 보장되는 수준에 본질적으로 상응하는 적정 수준의 개인정보 보호를 보장해야” 하며, “해당 제3국은 효과적이고 독립적인 개인정보보호 감독을 보장하고 회원국의 개인정보 감독기관과의 협력 메커니즘을 가능하게 해야 한다”고 규정하였음

<문제점>

- 국제적인 기준에 비추어 보았을 때, 한국의 개인정보 감독 체계는 행정부로부터 독립적이지 못하여 그 권한에 있어 매우 제한적임. 개인정보 보호법에서도 대부분의 실질적인 감독 기능이 보호위원회가 아니라 행정자치부에 주어지며, 인터넷, 금융 등 분야별로 개인정보보호 감독기관이 별도로 존재하여 전반적으로 감독체계의 독립성이 약화되어 있음.
- 현재 개인정보보호법의 주무부처인 행정자치부는 스스로가 방대한 개인정보의 보유, 운영 주체로서 개인정보의 이용과 보호라는 상충된 이해관계를 가지고 있음. 대표적으로 행정자치부는 주민등록번호 유출과 남용으로 인한 피해가 확산되고 주민등록번호 개편 요구가 커졌음에도 불구하고, 주민등록번호 체제 개편에 소극적인 입장을 견지하고 있음.
- 국가인권위원회 역시 <2012~2016 국가인권정책기본계획(NAP) 권고안>에서 "개인정보보호위원회는 실질적으로 심의, 의결기능만을 담당하고 실질적인 개인정보보호 정책 수립, 개인정보 수집자 감독, 개인정보 침해 구제 업무는 행정안전부에서 담당하여 사실상 독립적인 기구로 보기 어려움"이라고 지적하고 있음.
- 2014년 카드3사에서 1억 5백만건 개인정보 유출사고 이후 국회 상임위 등에서 개인정보 보호 컨트롤타워 부재에 대한 문제점이 지적됨에 따라, 개인정보 분쟁조정, 기본계획 수립 기능이 행정자치부에서 보호위원회로 이관되고 개인정보 침해요인 평가제도가 새로 시행됨.
- 그러나 개인정보 보호위원회는 여전히 인사와 예산 및 조직의 독립성 부재로 인하여 정책의 독립성과 전문성이 확보되지 못함. 국제적으로 개인정보 감독기구에 경찰 및 국가정보기관 등 행정부의 감시에 대한 견제 기능이 기대되는 것과 달리 우리 개인정보 감독기구의 존재감이 미미한 이유도 이에 있음

<개선방안>

- 개인정보보호위원회의 독립성과 권한 강화
 - 행정자치부의 개인정보 감독권한을 개인정보보호위원회로 이관함으로써, 개인정보 보호위원회의 독립성과 권한을 강화하여 개인정보 보호에 대한 명실상부한 국가 컨트롤타워 수립

- 개인정보보호위원회에 △민간, 공공부문의 통합적인 감독권을 부여하고, △행정입법권을 부여하여야 함. 특히 개인정보 보호위원회의 인사, 예산상의 독립성을 보장하도록 △위원장의 상임화와 상임위원의 확대로 독립적, 전문적 업무수행 △위원의 신분보장 규정 마련 △타부처 파견 및 복귀가 아닌 개인정보 보호위원회 독자 인사권 보장 △개인정보보호위원회에 예산편성권 부여 등을 내용으로 한 개인정보보호법의 개정이 필요함

<관련 자료>

- 19대 변재일 의원 대표발의안은 개인정보 보호위원회 개선을 위해 △현재 대통령 소속으로 있는 개인정보 보호위원회를 중앙행정기관으로 격상하여 인사와 예산 및 조직의 독립성을 부여하고, △개인정보 침해에 대한 효율적인 권리구제를 위해 직권조사권, 시정조치명령권, 고발 및 징계권고권과 개인정보처리 개선권고권 등의 권한을 개인정보 보호위원회에 부여하는 등의 방안을 제시한 바 있음

2. 빅데이터 시대 개인정보보호 강화

<현황>

- 빅데이터 시대 개인정보의 상업적 이용이 크게 증가함에 따라 이로부터 이용자와 소비자를 보호하기 위한 조치들이 요구되고 있음
- 이른바 4차 산업혁명으로 거론되는 신기술의 발전은 소비자 개인정보 보호에 대한 대책과 함께 이루어지는 것이 바람직함. 유럽 개인정보 감독관(EDPS)은 빅데이터 발전이 투명성, 이용자 통제권, 프라이버시 중심설계(Privacy By Design), 책임성의 원칙 하에 이루어져야 함을 역설함



- 한국에서는 특히 흠플러스(형사재판 대법원 계류), IMS코리아 사건(형사재판 1심 진행중) 등 유통업체가 수집한 소비자 개인정보는 물론, 심지어 민감한 처방전 정보까지 국내 업체는

물론 국외 업체로 유상판매되는 사건이 증가해 왔음. 대규모 개인정보 유출 사건을 반복적으로 겪어온 국민 입장에서는 자신도 모르는 새 개인정보가 유상판매되는 일이 증가함에 따라 다가오는 빅데이터 시대 개인정보 이용에 대해 불신감이 증가하고 있음. 현재의 개인정보 보호법과 정보통신망법 등 법률들은 정보주체인 소비자와 이용자의 개인정보 자기결정권을 충분히 보장하고 있지 못함

- 반면 최근 2016년 미국과 유럽은 신기술 환경으로부터 개인정보 보호를 강화하기 위한 입법 조치들을 연달아 취함. 한국 역시 이러한 국제적 흐름에 부응할 필요성이 있음(개인정보 보호위원회, 2017. 1. 의견). 유럽은 일반 개인정보보호규정(GDPR)을 제정하여 2018년 실시를 앞두고 있으며, 빅데이터 로직에 대한 알 권리 및 프로파일링 거부권 등 정보주체의 권리를 신설함. 전통적으로 개인정보 보호에 관한 일반 법률을 두지 않았던 미국은 2016년 통신법을 개정하여 처음으로 광대역 통신망 사업자가 이용자의 개인정보를 수집 이용할 때 사전 동의를 받도록 강화함(옵트인 제도 도입)

○ 개인정보 보호의 국제적 흐름은 EU에 의해 주도되고 있고,
 - 최근 미국도 동의 제도를 강화하는 등* 유럽의 개인정보 보호 제도에 부합하는 입장을 취하고 있는 것으로 보임
 * 미국 연방통신위원회(FCC)는 Broadband Consumer Privacy Rules('16.12.2)에서 위치·금융·건강정보 등에 대해 소비자로부터 동의를 받도록 하며(opt-in 방식), 비식별정보에 대해 HIPPA Privacy Rule보다 더 엄격한 요건을 두고 있음

○ 무역의존도가 높은 한국의 입장에서는 외국과의 실물·데이터의 교류가 필수불가결함
 - 유럽시장 참여를 위해서는 유럽과 유사하게 개인정보 보호 수준을 발전시킬 필요가 있음. 이 경우 EU 적정성 평가(adequacy test)* 통과에 유리하게 작용할 것임
 - '18.5.25.부터 GDPR(EU 개인정보 보호 일반법)이 발효되면 그 효력이 역외 국가에도 미치게 되므로, 개인정보 처리가 위법할 경우 과징금 부과 및 소송 제기 등 법률적 문제에 직면하게 됨
 * EU가 타국의 개인정보 보호 수준을 평가하여 EU 역내의 개인정보를 타국으로 이전하는 것을 허용하는 절차

(2017. 1. 개인정보 보호위원회 의견 중)

<문제점>

- 자사 고객 정보 2천4백만 건을 다수 보험사에 건당 1,980원 ~ 2,800원에 유상판매하여 231억 원의 부당이익을 올렸던 훔플러스 사건은 많은 소비자들에게 충격과 분노를 안겼음. 소비자들은 유상판매 사실을 몰랐으나 법원은 '백지 동의'나 다른 없는 현행 법률상 동의

조항에 따라 모두 무죄를 선고함(형사 2심). 이와 달리 유럽 개인정보 보호법제의 경우 개인정보 수집 및 제공을 매우 까다롭게 규정함

- 현재 우리 정보통신망법 및 개인정보보호법은 정보주체인 소비자와 이용자가 자신의 개인정보에 대하여 열람할 수 있는 권리(알 권리) 및 개인정보의 수집·이용·제공 및 판매 등 처리에 대하여 선택할 수 있는 권리(동의권)을 충분히 보장하고 있지 않음. 정보주체의 알 권리 및 동의권을 실질적으로 보호하는 이른바 ‘옵아웃 방지법’이 요구됨. 유럽연합 GDPR의 경우처럼 빅데이터 로직에 대한 알 권리 및 프로파일링 거부권에 대한 법률조항 신설도 필요함
- 특히 빅데이터 시대에는 서로 다른 개인정보가 결합 처리되는 경우가 증가하는데, 이에 대해서도 정보주체의 권리가 보장되어야 함(서울고등법원 판결). 개인이 식별되지 않는 익명 정보의 경우 현재도 동의 없이 빅데이터 처리가 가능함(서울시 심야버스 노선을 위한 빅데이터 처리 사례). 다만 암호화 등 일부 개인정보 보호 조치가 의무화되는 경우도 있으며 유럽연합의 경우에도 빅데이터 처리로부터 소비자와 이용자를 보호하기 위한 조치로서 ‘가명’의 개념을 도입하였음. 그러나 이런 조치들은 여전히 ‘개인정보’로서 그 처리에 있어 관련 법률의 적용을 받음
- 그러나 박근혜 정부는 개인정보 결합시 성명 등을 가리는 ‘비식별’ 조치를 정부 기준에 따라 형식적으로 취하는 경우 ‘개인정보 아닌 것으로 추정’하여 개인정보 관련 법률의 적용을 배제하는 ‘비식별화’ 정책을 추진해옴(2016. 6. 범정부 비식별 조치 가이드라인). 이는 빅데이터 업계가 개인정보를 정보주체 동의 없이 용이하게 상업적으로 처리할 수 있도록 보장하는 정책임. 개인정보 보호법의 적용을 배제하는 비식별화 정책은 해외에서도 그 유례를 찾아 볼 수 없으며(국가인권위원회, 2016. 11. ; 개인정보 보호위원회, 2017. 1), 개인정보 보호 규범을 왜곡함으로써 헌법상 국민의 기본권인 개인정보 자기결정권을 침해함

나. (비식별 정보의 활용) 비식별 정보는 개인정보가 아닌 정보로 추정되므로 정보주체로부터의 별도 동의없이 해당 정보를 이용하거나 제3자에게 제공할 수 있습니다.

(2016. 6. 범정부 비식별조치 가이드라인 중)

유럽연합의 「일반 개인정보보호 규정」 및 일본의 「개인정보의 보호에 관한 법률」은 비식별 정보라 하더라도 개인정보로 복원 또는 재식별될 가능성이 있으면 개인정보로 간주하며, 비식별 조치에 대한 구체적 개념 등을 규정하고 있다.

(2016. 11. 국가인권위원회 의견 중)

- 약학정보원 등은 약국과 병원에서 수집한 4천4백만 명 국민의 처방정보를 당사자인 정보주체 동의 없이 미국 빅데이터 기업인 IMS헬스에 판매하였으며, 현재 형사재판에서 암호화 비식별 조치를 취했다는 이유로 무죄를 주장하고 있음(형사 1심). 그러나 하버드대 연구진이 IMS헬스에 판매된 한국인 주민번호의 암호를 성공적으로 해제하여 우리 국민을 충격과 부끄러움에 빠뜨렸음. IMS헬스로 유출된 우리 국민 처방전 정보는 회수되지 않았으며, 이 정보는 현재도 전세계를 상대로 판매되고 있을 것으로 추정됨

정부, 개인의료정보 빅데이터 개방하겠다는데…

‘암호화된 주민번호’ 너무 쉽게 풀렸다

정부가 개인의 민감한 의료정보를 암호화 등 비식별 조치해 민간에 개방하겠다는 방침을 밝힌 가운데, 미국에서 암호화된 한국 주민등록번호를 100% 해제할 수 있다는 연구 결과가 나왔다.

국회 보건복지위원회 소속 정춘숙 의원(더불어민주당)이 25일 번역해 공개한 미국 하버드대학교 라타나 스위니 교수 연구팀의 2015년 논문 ‘처방전 데이터상 공유되는 대한민국 주민등록번호의 익명성 해제’를 보면, 연구팀은 한국인 사망자 2만3163명의 처방전 데이터의 암호화된 주민등록번호를 전부 해제하는 데 성공한 것으로 나타났다.

연구팀은 암호화된 주민등록번호를 논리적 추론 방식과 자동탐색실험, 두 가지 방식으로 모두 해제했다. 논리적 추론 방식은 각각의 자리에서 발견되는 문자의 빈도

미국 하버드대팀, 이미 지난해에 2만3천명 처방전 암호 100% 해제 “한국 주민번호 생일·성별 답겨 프로그램 몇번 돌리니 쉽게 풀려”

전문가 “민감한 개인정보 노출 위험 본인 동의 없이 공개 말아야”

를 통해 어떤 자리의 어떤 수가 어느 문자로 치환됐는지를 추론하는 방식인데, 논문은 한국의 주민등록번호는 임의번호가 아닌 생년월일과 성별 등 인구통계학적 개인 정보를 담고 있기 때문에 더 쉽게 풀 수 있었다고 밝혔다.

이에 따라 정부의 개인정보 비식별화 가

이드라인을 재검토해야 한다는 목소리가 높아질 것으로 보인다. 행정자치부는 개인정보를 비식별화(암호화)하면 이를 개인정보로 보지 않아 등의 없이도 처리할 수 있다는 가이드라인을 내렸고, 보건복지부는 이를 근거로 지난달 30일 건강보험심사평가원과 국민건강보험공단이 보유한 진료내역 등 5조 1027억건의 의료데이터를 민간에 개방해 빅데이터 산업에 활용토록 하겠다고 발표했다.

복지부는 주민등록번호 등은 가리거나 암호화에 문제없다는 입장이지만, 빅데이터의 속성상 작은 조각들이 연결돼 식별 가능한 개인정보로 변하는 것은 시간문제라는 것이 전문가들의 지적이다.

강장목 고려대 컴퓨터학과 교수는 “연구에서도 보듯이 비식별화된 정보는 언제든지 재식별의 위험성이 있다. 특히 우리나라

처럼 이미 수많은 개인정보가 유출돼 거래되고 있는 상황에서는 흩어져있는 데이터들이 연결돼 민감한 개인정보가 그대로 노출될 위험이 높다”고 지적했다. 정춘숙 의원은 “비식별화의 문제가 확인된 이상 진료기록 등 민감정보는 어떠한 경우에도 본인 동의 없이 공개해서는 안 된다”고 지적했다.

이번 논문은 또 “한국이 주민등록번호를 임의번호 체계로 개편하는 데 3조1000억~4조원의 비용이 들 것이라 추정하지만, 만약 개편하지 않는다면 이 제도와 이 제도를 사용하는 사람들에게 경제적 위험을 줄 것”이라고 지적하기도 했다. 현재 주민등록번호 체계를 임의번호로 전면 개편하도록 하는 주민등록법 개정안이 국회에 발의돼 있다.

허승 기자 raison@hani.co.kr

(한겨레 2016. 9. 25.)

- 건강한 ‘4차 산업혁명’을 위하여서는 국내외 빅데이터 업계의 무분별한 개인정보 이용으로부터 국민의 정보인권을 보장하기 위한 대책이 필요함

<개선방안>

- 빅데이터 환경을 고려한 개인정보 보호 강화
 - 4차 산업혁명 논의 속에 소비자 및 이용자의 개인정보를 보호하기 위한 제도를 도입하고 있는 유럽연합 등 다른 나라의 논의를 참고하여, 매매 등 개인정보의 목적외 이용 규제, 개인정보 처리 로직에 대해 설명을 요구할 수 있는 권리, 프로파일링을 거부할 수 있는 권리, 생체정보를 민감정보로 특별히 보호 등의 내용을 법률에 포함하여 정보주체의 권리 보장.
- 박근혜 정부의 비식별조치 가이드라인 운영 중단과 재검토

<관련 자료>

- [국가인권위원회 의견\(2016. 11.\)](#)

- [개인정보 보호위원회 의견\(2017. 1.\)](#)
- [서울 고법 “구글도 국내 개인정보 보호법 따르라”](#)

3. “개인정보없는 임의번호로” 주민등록번호 제도 개혁

<현황>

- 2014년 8월 8일, 국가인권위 국회의장 및 국무총리에 주민등록번호 제도의 근본적 개편 권고
 - 주민등록번호 수집 제한, 조세번호 등 목적별 번호 사용 권고
 - 주민등록번호를 개인정보가 포함되지 않은 임의의 일련번호로 변경
 - 주민등록번호 변경 허용
- 2015년 12월 23일, 헌법재판소는 현행 주민등록법에 헌법불합치 결정. 주민등록번호 변경을 허용하지 않는 것은 그 자체로 개인정보 자기결정권 침해라고 판시. (2017년 12월 31일까지 주민등록법 개정 권고)
- 2016년 5월 19일, 주민등록번호를 변경할 수 있도록 허용하는 주민등록법 개정안(정부안) 국회 통과.
 - 새 주민번호에 여전히 생년월일과 성별 정보 포함(13자리 중 뒤의 6자리만 변경) 하여 전체 번호 유추 가능.
 - 변경 대상자를 유출로 인해 생명·신체 및 재산, 성폭력 등과 같은 피해를 입거나 입을 우려가 있는 경우로 한정
 - 국가인권위원회 위원장도 환영과 함께, 제한적 변경에 아쉬움을 표하는 성명을 발표하여 목적별 번호, 임의번호의 도입을 요구함.
- 2016년 8월 23일, 진선미 의원, 주민등록번호 체계를 임의번호로 변경하는 내용의 주민등록법 개정안 발의 (20대 국회)

<문제점>

- 주민등록번호를 비롯한 개인정보 유출 심각. 이미 유출된 개인정보에 대한 국가적 대책이 부재해 옴에 따라 보이스피싱 등 국민 피해 가중.
 - 2008년 옥션 1천8백만 건 유출,
 - 2011년 SK컴즈 네이트, 싸이월드 3천5백만 건 유출,
 - 2011년 넥슨 메이플스토리 1천3백만 건 유출,

- 2014년 롯데카드, 농협카드, KB국민카드 1억 4백만 건 유출,
- 2016년 인터파크 1천3십만 건 유출
- 주민등록번호의 과도한 수집, 서로 다른 개인정보를 연결하는 만능 식별자로서의 주민등록번호의 역할에 따라 개인정보 유출 야기.
- 2014년 8월부터 주민번호 법정주의가 시행되었으나, 통신, 금융 등 민간영역을 비롯하여 여전히 많은 법령(2014년 기준 1000여개)에서 주민등록번호 수집을 허용하고 있음. (자세한 분석은 주민등록번호 수집 법령 현황에 대한 검토 보고서 참고)
- 사실상 전 국민의 주민등록번호가 유출되었음에도 기유출된 주민등록번호에 대한 국가적 대책이 부재. 이에 주민번호 변경으로 국민들의 피해를 방지할 필요가 있음.
 - 2015년 현재 결정으로 변경 가능해짐(2017년 5월부터 시행).
 - 그러나 변경 대상에 대한 제한, 번호 변경의 제한(13자리 중 6자리만 변경 가능)으로 피해 방지 효과 의문
- 주민등록번호에 생년월일, 성별, 출생지 정보를 포함하여 의도하지 않게 개인정보가 노출되고 연령, 성별, 지역에 따른 차별 조장. 또한, 개인정보로 주민등록번호를 추정할 수 있음.
 - 2014년 서울과학기술대학교 연구, 페이스북에 공개된 개인정보를 이용하여 11만 5615명 중 45%의 주민번호 조합성공
 - 2015년 미국 하버드대학교 연구, 미국 IMS헬스에 팔린 한국인 주민번호 모델로 2만 3163개 재식별 성공 "생년월일, 성별, 지역, 검증번호 덕분에 수월했다"
 - 2009년 인식조사, 국민의 77.2%는 주민번호를 통해 성별, 생년월일 등을 알 수 있다는 사실에 "원하지 않는데도 내 정보가 노출되어서 신경이 쓰인다"고 응답
- 주무부처인 행정자치부의 미약한 의지
 - 주민등록번호의 주무부처로서 행정자치부는 주민등록번호 제도 개선에 소극적임. (만능 식별자로서 주민등록번호의 효율성 주장)
 - 2014년 금융개인정보 유출사고 이후, 지방행정연구원에 의뢰해 수행하고 있는 주민번호 개선방안 연구를 수행하였으며, 이에 대한 공청회도 개최하였지만, 주민등록번호 변경(재발급) 허용 외에 개선 의지를 보이지 않음.
- 주민등록번호의 존속을 주장하는 사람들은 주민등록번호 제도 변경으로 인한 사회적 혼란과 경제적 비용을 근거로 들고 있음. 이에 대해 다음과 같은 반론이 가능함.
 - 제도 변경에 따른 혼란을 거론하나 거의 전 국민의 주민등록번호가 유출된 현 상황이 사회적 혼란 및 비용, 국민적 피해를 계속 야기하고 있음을 간과함.
 - 주민등록번호 체계를 임의의 일련번호로 변경하더라도, 주민등록번호 변경을 원하는 사람과 신생아부터 단계적으로 적용한다면 노인 등 취약계층의 혼란 및 변경에 따른 비용을 줄일 수 있음.

- 한국지방행정연구원이 추산한 비용은 시스템 개편 비용만 6000 억원 정도인데, 이 정도면 주민등록번호 개선의 필요성에 비추어 충분히 감당할만한 비용임. 정부는 도로명 주소로의 개편이라는 전국적 개편사업을 이미 시행한 바 있음.
- 주민등록번호 수집을 더욱 제한적으로 허용한다면, 제도 변경으로 인한 사회적 비용을 더욱 줄일 수 있음.
- 현재의 주민등록번호 체계는 2100년 이후에는 포화되어, 어차피 조만간 주민등록번호 체계 개편이 되어야 함.
- 특히, 사물인터넷(IoT), 인공지능(AI), 빅데이터 등 신기술이 보편화되어 갈수록 개인정보 침해 우려가 높아지고 있는데, 한국의 경우 주민등록번호로 인해 그 피해가 더욱 심각할 것임. 주민등록번호 제도의 개혁 없이 개인정보 보호에 대한 사회적 신뢰가 형성될 수 없으며, 이에 따라 신기술과 서비스의 발전도 저해될 수밖에 없음.

<개선방안>

- 주민등록번호 제도 개혁
 - 번호체계를 개인정보가 없는 임의의 일련번호로 변경
 - 주민등록번호 변경 허용
 - 주민등록번호의 수집 제한과 영역별 식별번호 체제의 도입
- 2014년 8월 8일, 국가인권위원회 역시 위와 같은 내용의 주민등록번호 제도 개선안을 국무총리 및 국회의장에 제안함.

<관련 자료>

- 주민등록번호 제도의 문제점과 해결방안에 대한 보고서
- 주민등록번호 수집 법령 현황에 대한 검토 보고서
- 국민식별번호와 목적별 식별번호에 대한 해외사례 보고서
- 주민등록번호 제도 개혁 운동의 역사

4. “해외정보 전담기관으로!” 국가정보원 개혁

<현황>

- 2012년 대선 댓글 조작을 비롯한 선거 개입, 간첩 증거 조작, 이탈리아 해킹 프로그램 운용, 고 김영한 업무일지에서 드러난 민간인 사찰 등 국정원의 정치 개입과 권력 남용이 우리 사회 민주주의와 인권을 심각하게 훼손하여 왔음

- 이는 국가정보원이 다른 나라 정보기관과 달리 정보권한과 더불어 수사권을 함께 보유할 뿐 아니라 국내와 해외 정보권한을 모두 독점하고 그 권한을 자의적으로 남용하는데 따름. 국정원은 여기서 그치지 않고 테러 대응, 사이버 보안 등 새로운 비밀 권한을 계속 확대해 왔음
- 여러 사회적 논란에도 불구하고 국정원에 대한 사회적 통제가 실질적으로 이루어지고 있지 못하며 이 정보기관의 권한 남용을 개선하기 위한 근본적인 제도 조치도 이루어진 바 없음. 다만 1994년 김영삼 정부가 당시 국가안전기획부의 수사권 가운데 국가보안법의 찬양·고무죄와 불고지죄에 대한 수사권을 폐지하였으나 1996년 노동법·안기부법 날치기 통과로 수사권이 부활하였음. 김대중 정부와 참여정부에서 안기부 X파일 사건이 불거졌으나 국정원 개혁에는 소득이 없었음
- 세계적으로 정보기관의 권한이 막강한 것은 사실이지만 그럼에도 권한 오남용을 방지하기 위한 권한 분산과 감독 체계가 공통적으로 마련되어 있음. 특히 2013년 6월 국가안보국(NSA)의 전세계 통신망 감시가 폭로된 이후, 미국 정부는 대통령실에 자문기관을 설치하고 <세계 변동 속에서 자유와 안보>라는 제목의 보고 및 46개 권고를 발표하였음. 이를 통해 오바마 정부는 신호정보기관인 NSA의 감시 기능을 해외정보로 제한할 것을 권고하는 등 막강한 정보기관의 감시 권력을 민주적으로 통제하기 위한 개혁을 추진하였음

<문제점>

- 국회의 감독 기능 실패 - 2012년 대선 당시 국정원의 선거개입 사실이 드러났지만 2차례에 걸친 국회 '국가정보원 등 국가기관의 정치적 중립성 강화를 위한 제도개선특별위원회'(국정원 개혁특위)는 뚜렷한 성과 없이 마쳤을 뿐 아니라, 심지어 개혁특위 활동기간 중에도 국정원이 국회나 법원으로부터 아무런 통제도 받지 않고 이탈리아 해킹 프로그램(RCS)을 수입, 운영해 왔다는 사실이 드러남. 2015년 RCS 사용 논란이 불거졌으나 국정원의 비협조로 국회는 진상규명에 실패함
- 법원의 감독 기능 유명무실 - 법원은 정보기관에 비해 정보 업무에 대한 전문성이 부족할 수밖에 없어 통신감청에 대한 영장 심사조차 제대로 이루어지고 있지 못함(기각률 1% 남짓). 특정 피의자가 아니라 주거지, 근무지, 무선 공유기 등 인터넷 회선 전체에 대한 이른바 패킷 감청(Deep Packet Inspection)이 오랫동안 이루어져 왔음에도 2009년 인권단체 기자회견 전까지 그 사실이 오랫동안 알려지지 않았을 뿐더러 제대로 된 감독이 이루어지지 못해 왔음(현재 헌법심사 중).

국정원 감청 신청과 고등법원 기각률

연도	법원	청구	발부	일부기각	기각	전체 기각률
2003년	고등법원	2	2	0	0	0.00%
2004년	고등법원	2	2	0	0	0.00%
2005년	고등법원	6	6	0	0	0.00%
2006년	고등법원	1	1	0	0	0.00%
2007년	고등법원	1	1	0	0	0.00%
2008년	고등법원	3	2	1	0	0.00%
2009년	고등법원	4	4	0	0	0.00%
2010년	고등법원	4	4	0	0	0.00%
2011년	고등법원	15	13	1	1	6.67%
2012년	고등법원	7	7	0	0	0.00%
2013년	고등법원	7	7	0	0	0.00%
2014년	고등법원	11	11	0	0	0.00%
2015년	고등법원	18	18	0	0	0.00%
총계	고등법원	81	78	2	1	1.23%

출처 : 사법연감통계

*기각 원고의 청구를 이유 없다고(타당성이 없다고) 하여 물리치는 것을 기각이라고 한다.

- 국회와 법원을 비롯하여 국정원에 대한 사회적 감독 체제가 부재하다는 것은, 언제든지 국정원의 권력 남용이 가능함을 의미함.
- 더이상 국가정보기관의 민주주의 훼손과 선거 및 국내정치 개입을 방지하기 위하여 국정원의 셀프개혁을 넘어 권한 분산 등 근본적인 개혁을 비롯하여 국정원에 대한 사회적 감독을 강화하여야 함.

<개선방안>

- 국정원 개혁
 - 국가정보원법 제3조의 직무범위 조항의 개정을 통해 국정원의 국내 문제 개입권한 폐지. 즉, 국내보안정보 수집권의 폐지, 수사권 폐지, 기획조정권한의 폐지 등
 - 국정원은 해외정보를 전담하는 기관으로 전문화.
 - 국정원의 사이버 보안 관련 권한을 사이버 보안을 전담하는 일반 정부부처로 이관 (사이버 보안 부분 참조)
- 국회의 국정원에 대한 감독 강화
 - 국회 정보위원회의 전임·상설화 (2013년 12월 국정원 개혁특위를 통하여 당시 새누리당과 새정치민주연합의 합의 내용)

- 정보위 소속 보좌진의 회의 참석과 정보위 회의록 및 국정원 예산 열람 허용

<관련 자료>

- 국가정보원 개혁을 위한 시민사회 청원
- 20대 국회에서 국정원에 대한 민주적 통제 장치 마련을 요청하는 공개서한을 원내 각당에 발송
- [\[토론회\] 리셋! 국가정보원 \(2017.3.8\)](#)

5. “국정원은 손떼라!” - 사이버 보안은 일반 행정부처에서

<현황>

- 현재 국내에는 민간 영역의 사이버 보안을 규율하는 ‘정보통신망 이용촉진 및 정보보호 등에관한법률’, 국가기반시설의 사이버 보안을 위한 ‘정보통신기반보호법’, 공공 영역의 사이버 보안을 규율하는 ‘국가사이버안전관리규정’에 따라 사이버 보안을 위한 대응 체제가 갖추어져 있음.

	관할 영역	관할 부처
정보통신망법	민간 정보통신망 일반	미래창조과학부
정보통신기반보호법	민간 기반시설	미래창조과학부
	공공 기반시설	국가정보원
국가사이버안전관리규정	공공 정보통신망	국가정보원

- 국가정보원은 ‘국가사이버안전관리규정’에 따라 국가사이버안전 관련 정책 및 관리의 총괄·조정 역할을 맡아 국가사이버안전기본계획 수립·시행하고, 국가사이버안전전략회의 및 대책회의를 운영하며, 실무적으로도 국가사이버안전센터를 운영하고 있음. 또한, ‘정보통신기반보호법’에 따라 공공분야 주요정보통신기반시설의 사이버 보안을 담당하고 있음.
- 현재 국정원이 국내 사이버 보안과 관련하여 맡고 있는 역할은 다음과 같음.

❖ 국가사이버안전 관련 정책 및 관리 총괄·조정 (국가사이버안전관리규정)

- > 국가사이버안전기본계획 수립·시행
- > 국가사이버안전전략회의 및 대책회의 운영
- > 국가사이버안전센터 운영
- ❖ 공공분야 주요정보통신기반시설의 사이버 보안 (정보통신기반보호법)
- ❖ 공공기관 정보보안 관리실태 평가
- ❖ 국가·공공기관이 도입하는 정보보호시스템에 대한 보안적합성 검증
- ❖ 암호모듈 검증
- ❖ 보안관제 및 사이버 공격 정보 수집
- ❖ 정보보호제품 평가·인증에 관여

- 2015년 4월 이후, 정부는 국가 사이버 안보 태세 강화 종합대책을 마련하였는데, 이에 따라 국가안보실 중심의 전반적인 사이버안보 컨트롤타워 기능을 보다 강화하기 위해 국가안보실 산하에 사이버안보비서관을 신설하고 국가안보실과 국가사이버안전센터를 통해 국가적인 사이버안보 정책의 수립·시행·평가를 일원화하는 방식으로 사이버안보 수행체계를 변화시켰음. 그러나 이러한 변화는 ‘국가사이버안전관리규정’이나 법제에 반영되어 있지 않으며, 이 체제에서도 실질적인 컨트롤타워 역할은 국가정보원이 맡고 있음.

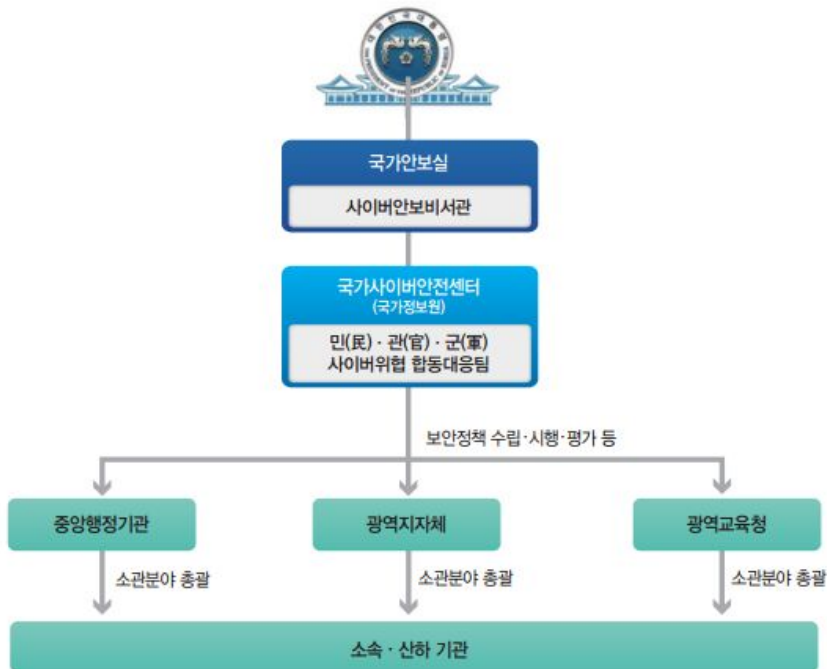


그림 : 2015년 4월 이후 국가 사이버안보 수행체계의 변화 (출처 : 2015 국가정보보호백서)

- 2016년 9월 1일, 국가정보원은 「국가 사이버안보 기본법」 제정(안)을 입법예고하였으며, 이를 수정한 「국가사이버안보법(안)」이 2017년 1월 3일 국회에 발의되어 있음.

<문제점>

- 국정원의 사이버 보안 역할은 법에서 규정한 자신의 직무 범위를 벗어난 것임. 비록 특정 사이버 공격이 국가안보에 영향을 미칠 수 있으나, 사이버 보안이 개인의 정보보안에서부터 인터넷 상의 사기나 해킹 등 민간 부문의 사이버 보안이 대부분을 차지하는 것을 고려할 때, 사이버 보안 업무 전체를 국가안보적 시각에서 바라보는 것은 협소한 시각임. 예를 들어, 암호모듈 검증 업무를 보더라도, 과거에는 비밀 정보요원만이 암호를 사용해 왔다면, 인터넷이 보편화된 현재에는 일반 기업 뿐만 아니라 개인 이용자의 통신 보안을 위해서도 암호 사용이 일반화된 상황에서 여전히 국정원이 과거의 관행대로 ‘암호자재’의 관리 업무를 담당하는 것은 적절하지 않음.
- 사이버 보안 정책의 투명성과 사회적 감독 기능이 약화됨. 비밀정보기관으로서 국정원은 조직, 인력, 예산, 사업 등 모든 측면에서 투명하게 공개되지 않기 때문에, 여타 정부부처에 비해 언론이나 국회에 의한 감독과 견제 기능이 약할 수밖에 없음. 실제로 국내 사이버 보안 관련하여 국정원이 수행하고 있는 정책 자료, 사업 내용, 예산 등이 투명하게 공개되고 있지 않음. 이에 따라 사이버 보안 영역에서도 국정원의 권한 남용을 우려할 수 밖에 없고, 사이버 보안 정책에 대한 합리적인 토론이 가능하지 않기 때문에 오히려 국내 사이버 보안에 부정적인 영향을 초래하고 있음.
- 사이버 보안을 위한 이해관계자와의 협력과 민간의 자율성을 저해함. 미국, 영국, 일본 등 세계 주요 선진국들은 사이버 보안 정책의 수립과 집행 과정에서 다양한 이해관계자의 참여와 민간의 자율성을 강조하고 있음. 네트워크의 운영이나 기술 개발이 주로 민간 영역에서 이루어지고 있기 때문임. 그러나 비밀정보기관인 국정원이 국가 사이버 보안의 총괄·조정 역할을 맡고 있는 상황에서는 이해관계자와의 협력이나 민간의 자율성을 기대할 수 있을지 의문임.
- 세계 주요 선진국들은 사이버 보안 전략을 수립하면서 기본권의 보장, 인터넷의 개방과 혁신, 민주적인 거버넌스를 핵심적인 가치로 내세우고 있음. 밀행성과 은밀성이라는 정보기관의 특성은 이해관계자와의 협력이나 이러한 핵심적인 가치와 충돌할 수밖에 없음.
- 국정원에 의한 감시와 사찰, 인권 침해가 우려됨. 사이버 보안 업무의 경우 보안관제나 침해사고 분석 등의 과정에서 기업비밀이나 이용자 개인정보 등이 유출되거나 악용될 위험성이 큼. 은밀한 감시와 사찰이 가능한 사이버 공간의 특성 상 국정원이 보안 업무를 담당하게 된다면, 권한 남용에 대한 우려가 더 커질 수 밖에 없음.
- 세계 어느 나라에서도 비밀정보기관이 사이버 보안의 실질적인 컨트롤타워 역할을 맡고 있는 나라는 없음. 예를 들어, 미국의 경우 백악관 산하에 사이버 보안국(Cybersecurity Directorate)과 사이버보안조정관(Cybersecurity Coordinator)을 두어 컨트롤타워 역할을 하고 있고, 국가기반시설의 사이버 보안은 국토안보부가 담당하고 있으며, 보안기술 표준과 관련한 업무는 상무부의 국립표준기술원(NIST) 등이 맡고 있음.

<개선방안>

- 국정원의 사이버 보안 권한을 일반 행정부처로 이관
 - 사이버 보안 관련 국정원 권한의 이관은 보다 근본적인 국정원 개혁이 전제가 되어야 함. 국정원 개혁 방향에 대해서는 <국가정보원 개혁> 부분 참조.
 - 국가 정보통신망의 사이버보안에 대한 책임, 정보보호시스템에 대한 인증, 암호 인증 등 현재 국정원이 담당하고 있는 사이버 보안 관련 역할도 일반 행정부처(예를 들어, 미래창조과학부, 국민안전처, 혹은 사이버보안청과 같은 별도의 부처 신설 등)로 이관되어야 함.
 - 일반 행정부처로 이관하더라도, 현재와 같이 전체 국가통신망에 대한 감시 권한을 두는 것은 위험함. 사이버보안 담당 부처는 가이드라인 제시 및 감독, 지원의 역할을 하고, 각 부처 및 민간의 기관들은 자신의 상황에 맞게 사이버 보안 대책을 수립, 이행해야 함.
 - 국정원은 특정 사이버 공격이 북한 혹은 다른 해외 국가에 의한 것으로 밝혀졌을 경우에만 관여할 수 있도록 그 역할이 제한되어야 함.
- 체계적인 사이버 보안 전략 수립
 - 지금까지 수차례 사이버 안보 종합대책이 세워졌지만, 대규모 사이버 보안 사고가 발생할 때마다 임시방편적으로 만들어졌으며, 이는 사이버 보안 '전략'이라기 보다는 '종합대책' 수준임. 또한, 용어에서 드러나듯이, 사이버 보안에 대한 전체적 관점이 아닌, '국가안보'에 편향된 관점으로 수립되었음.
 - 주요 선진국들은 사이버 보안을 위한 원칙으로 인터넷의 개방성과 혁신, 프라이버시권을 비롯한 인권 존중, 공공과 민간의 협력, 투명하고 민주적인 거버넌스, 국제협력과 신뢰 등의 원칙을 강조하고 있음. 우리의 사이버 보안 전략도 이러한 가치에 기반하여 종합적으로 수립될 필요가 있음.
- 사이버 보안 관련 법제의 체계적인 개편
 - 현재 사이버 보안 관련 법령들은 용어의 정의도 통일되어 있지 않고, 중복적인 내용도 많음. 사이버 보안 전략에 기반하여 관련 법령이 체계성과 상호 일관성을 갖도록 정비되어야 함.
 - 사이버 보안 정책의 수립과 집행은 공개적이고, 관련 이해관계자들의 자유로운 참여와 협력에 기반하여 이루어져야 함.

<관련 자료>

- [정보인권연구소 보고서] 국가정보원과 국내 사이버 보안정책 개혁 방안

6. 사이버사찰금지법 제정

<현황>

- 2014년 카카오톡 사이버 망명은 정보·수사기관의 사이버사찰에 대한 국민적 불신에서 유래함. 통신비밀보호법 및 전기통신사업법 등 현행 법제도는 정보·수사기관의 필요에 따라 전기통신에 대해 광범위한 사찰과 정보 수집을 허용하고 있음.
- [2014년 2월, 국가인권위원회는 다음과 같이 통신자료 및 통신사실확인자료 제도 개선을 권고하였음](#)
 - 1. 「전기통신사업법」 중 제83조 제3항을 삭제하는 내용의 법 개정을 추진할 것
 - 2. 「통신비밀보호법」 중 다음의 내용을 반영하는 법 개정을 추진할 것
 - 가. ‘가입자정보’, ‘실시간위치정보’의 정의규정을 신설하는 것
 - 나. 제2조 제11호 중 바.목과 사.목에서 ‘실시간위치정보’를 제외하는 것
 - 다. 제13조와 관련하여 검사 또는 사법경찰관이 범죄수사를 목적으로 가입자정보 및 통신사실확인자료(실시간위치정보는 제외한다)의 제공을 요청할 수 있는 요건을 “피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당사건과 관계가 있다고 인정할 수 있는 것”에 한정하는 것
 - 라. 범죄의 수사를 목적으로 하는 ‘실시간위치정보’제공의 요청은 위 다.항의 요건 외에 보충성의 요건을 갖춘 경우로 한정하는 것
- 2015년 11월, UN 자유권위원회는 한국 정부에 다음과 같이 권고하였음
 - 42. 위원회는 전기통신사업법 제83조제3항에 따라 수사기관이 수사목적은 이유로 영장 없이 전기통신사업자에게 이용자 정보를 요구한다는 것에 대해 우려한다. 집회 참가자들을 특정하기 위한 소위 "기지국 수사"의 집행 및 이에 대한 불충분한 규제, 그리고 폭넓은 감청의 이용, 특히 국정원에 의한 감청과 이에 대한 불충분한 규제에 대해서도 우려한다(제17조 및 제21조).
 - 43. 대한민국 정부는 국가 안보를 위한 감시를 포함해 모든 감시가 규약에 부합하도록 보장하기 위해 필요한 법 개정을 하여야 한다. 특히 이용자 정보는 영장이 있을 때만 제공해야 하고, 국정원의 통신수사를 감독할 수 있는 기제를 도입해야 하며 기지국 수사가 자의적으로 이루어지지 않도록 보호수단을 강화해야 한다.
- 2014년 6월, 특히 스마트폰에 보관된 사생활과 통신내용에 대한 보호가 민감한 인권 문제로 부상함에 따라 미국 연방대법원은 “휴대전화에 저장된 개인정보”가 수정헌법 4조에 의해 보호된다고 판결함

<문제점>

- 통신자료
 - 전기통신사업법 제83조 제3항에 의해 연간 1천만 명 이상의 통신가입자 정보(2015년 기준)가 정보·수사기관에 제공되고 있음. 현재 이 제도는 성명, 아이디, 주소, 주민등록번호 등 통신가입자 정보를 정보·수사기관에 제공하는 요건이나 절차에 법원 등 외부의 통제와 감독 장치를 전혀 두고 있지 않으며, 정부에 비판적인 인터넷 이용자의 신원을 파악하고 사찰하는 데 악용되고 있다는 비판도 받아 왔음. 2016년 그 피해 대상이 특별히 수사대상으로 소환된 적 없는 국회의원, 기자, 평범한 직장인을 광범위하게 아우른다는 사실이 드러나 큰 사회적 논란이 일었고 2016년 5월 [500명의 청구인이 통신자료 제공에 대하여 헌법소원을 청구](#)하여 현재 심사 중임. 이 문제에 대하여 국가인권위원회 및 유엔이 개선을 권고하였고 국회에 다수의 개선입법안이 발의되어 있으나 관련 제도 개선이 이루어지고 있지 않음
- 통신제한조치(감청)
 - 정보·수사기관들은 법률에 열거된 범죄에 한해 법원의 허가를 득한 후 감청을 집행할 수 있지만 그 기각률이 매우 낮아 충분히 통제되고 있다고 보기 어려움. 특히 감청의 경우 일반 범죄수사를 하지 않는 국가정보원이 통신사를 통한 국가감청 집행의 98%를 점유하고 있어(2015년 미래창조과학부 집계 기준) 비밀정보기관에 의한 감청 오남용에 대한 국민들의 우려가 계속되어 왔음. 통신사를 통하지 않는 직접 감청 집행의 경우 그 통계가 한번도 국민 앞에 공개된 바 없으며 2016년 테러방지법 통과 이후 관련 집행 통계도 집계된 바 없어 비밀 감청에 대한 의구심이 커지고 있음. 국가정보원의 감청 기법 가운데 자택, 근무지, 와이브로 모바일 공유기 등 인터넷회선 전체에 대해 이루어지는 [패킷 감청에 대해서는 2011년에 이어 2016년 두번째로 헌법소원이 청구](#)되어 현재 심사 중임. 이런 상황에서 국정원은 감청 편의를 위해 통신사업자로 하여금 정보·수사기관을 위한 감청설비를 의무적으로 구비하도록 하는 내용으로 통신비밀보호법 개정을 추진해 왔음
- 통신사실확인자료
 - ‘수사상 필요한 경우’ 광범위하게 허용되는 통신사실확인자료의 경우, 통화내역은 물론 특히 위치정보의 제공에 남용되고 있어 문제가 심각함. 우선 경찰은 집회 참가자의 신원을 파악하기 위하여 대상자를 특정하지 않고 집회 장소 주변의 무선 기지국에서 신호가 잡히는 모든 휴대전화 내역을 제공받는 일명 ‘기지국수사’를 실시하여 왔음. 2012년 민주통합당 등 정당 집회 현장에서 [기지국수사의 대상이 된 인터넷언론 기자가 헌법소원을 청구](#)하여 현재 심사 중임. 또한 몇 달간에 걸쳐 대상자의 장래 위치를 실시간으로 추적하는 수사기법(요건이 엄격하지 않은) 통신사실확인자료 제공 절차와 요건에 의해 남용되어 왔음. [2012년 희망버스 활동가들과 그 가족을 대상으로 이루어진 실시간 위치추적](#)에 대한 헌법소원이 제기된 데 이어 [2014년에는 철도노조 조합원 및 초등학생을 포함한 그 가족을](#)

[대상으로 광범위하게 이루어진 실시간 위치추적](#)에 대하여 헌법소원이 제기되어 현재 심사 중임

- 압수수색
 - 이메일 및 카카오톡 등 송수신이 완료된 통신 내용의 경우 압수수색영장에 의해 정보·수사기관에 제공되어 왔으며 스마트폰 모바일 환경의 확산에 따라 많은 국민들에게 민감한 문제로 부상하였음. 그러나 당사자 및 그 통신 상대방에 대한 통지권과 당사자 참여권 보장이 부족함. 특히 모바일 메신저 등 디지털 매체에 대한 압수수색은 한번에 다수인에 대한 광범위한 대중 감시(mass surveillance)가 가능하여 위헌 논란이 있음. 2014년 12월 [카카오톡에 대한 대규모 압수수색에 대한 헌법소원이 청구](#)되어 현재 심사 중임

<개선방안>

- 통신감시에 대한 엄격한 통제
 - 시민들이 일상생활을 영위하는 사이버 공간에서 국가 감시를 견제하고 정보인권을 보장할 수 있도록 관련 법제를 개선할 필요가 있음. 감청, 압수수색, 위치정보, 통신자료 등 정보·수사기관의 정보취득은 예외적으로 제한된 범위에서만 허용되도록 통제해야 하며, 특히 이메일과 메신저 등 전기통신은 시민들의 프라이버시와 통신비밀의 자유가 강하게 보장되어야 하는 영역으로서 그 압수·수색·검증에 대해서 엄격한 요건과 절차가 보장되어야 함
- 가입자 정보 제공시 영장주의 적용
 - 정보수사기관이 통신사 및 인터넷 서비스 제공자에게 가입자 정보(통신자료)를 요청할 때 법원의 허가를 받도록 전기통신사업법(혹은 통신비밀보호법)을 개정해야 함.
- 범죄수사 목적의 통신 정보 제공의 엄격한 통제
 - 범죄수사를 목적으로 통신정보의 제공이 필요하다고 할지라도, 이는 필요성(necessary)과 비례성(proportionality) 요건을 갖추어야 함. 감청(통신제한조치), 통신내역(통신사실확인자료), 위치정보 등의 제공 요건을 현재보다 엄격하게 강화하고, 법원과 국회의 감독 권한을 강화함으로써 범죄수사 목적으로 제공되는 통신 정보가 정보수사기관에 의해 오남용되지 않고 이용자의 기본권을 보호할 수 있도록 통신비밀보호법을 개정해야 함. 특히, 개인에 대한 과도한 사찰과 감시를 가능하게 하는 인터넷 패킷감청, 실시간 위치추적, 기지국 수사는 제한되어야 함.
 - 메신저, 이메일 등 송수신이 완료된 통신내용의 경우에도 감청 수준으로 엄격하게 통제하여, 일반적인 압수수색보다 더욱 엄격한 요건 하에 이루어질 수 있도록 하며,

정보주체가 압수수색에 참여할 수 있도록 집행참여권과 이의제기권을 보장하는 방향으로 통신비밀보호법이 개정되어야 함.

- 정보주체의 권리 강화
 - 사이버 수사 집행 종료 후 모든 정보주체에게 일정기간(예를 들어 30일) 이내에 그 사실을 통지함으로써, 정보주체의 최소한의 권리를 보장하는 방향으로 통신비밀보호법이 개정되어야 함.

<관련 자료>

- 사이버 사찰을 금지하기 위한 입법을 청원합니다.

7. 경찰의 무차별 개인정보 수집 통제

<현황>

- 1999년 대법원은 누구든지 “자기의 얼굴 기타 모습을 함부로 촬영당하지 않을 자유”를 가진다고 하면서, “수사기관이 범죄를 수사함에 있어 현재 범행이 행하여지고 있거나 행하여진 직후이고, 증거보전의 필요성 및 긴급성이 있으며, 일반적으로 허용되는 상당한 방법에 의하여 촬영을 한 경우”를 제외하고는 원칙적으로 영장주의가 적용된다고 판시하였음(99도2317 판결).
- 그러나 경찰은 경찰법 3조 및 경찰관직무집행법 2조에 의거 “치안정보의 수집·작성 및 배포”라는 명분으로 수사 이외에도 범죄예방 명목으로 다양한 국민 개인정보 시스템을 구축 운영하고 있음
- 경찰은 CCTV, 차량번호자동인식장치, 블랙박스, 채증장비, 바디캠 등 다양한 장비를 이용하여 국민의 개인정보를 점점 더 방대하고 수집하고 있으며 이중 일부는 데이터베이스로 집적하거나 지능화하여 정밀하게 분석되는 데 사용하고 있음. 문제는 경찰이 방대한 개인정보를 처리하면서도 각각의 수집, 사용 및 제한에 대해 구체적으로 규정한 법률적 근거를 마련하고 있지 않다는 것임. 경찰이 구체적인 법률 없이 경찰법 및 경직법의 포괄 규정이나 자체적인 지침에 의해서만 관행적으로 개인정보를 처리하기 때문에 오남용과 정보인권 침해 논란이 계속되어 왔음

<문제점>

- 경찰, 과도한 집회 채증 논란
 - 채증 후 신원 식별 방식 방식을 둘러싼 의문점
 - 경찰, CCTV로 집회 감시 논란
- 경찰, 영상정보 광범위한 수집과 지능화

- [전국민 차량번호판을 자동으로 인식하여 과거 이동경로까지 추적](#)
- [전국 CCTV 통합관리 및 지능화 추진 \(이글아이\)](#)
- [택배회사 블랙박스를 무제한 제공받기도](#)
- [경찰, 웨어러블 카메라\(일명 '바디캠'\) 도입 논란](#)
 - [개인정보보호위원회는 경찰은 영상·음성정보를 수집하지 아니하면 공무집행방해죄의 수사가 불가능하거나 현저히 곤란한 경우에 필요한 최소한의 범위에서 바디캠을 사용할 수 있고, 웨어러블 카메라를 대여하지 아니하면 범죄피해자 보호가 불가능하거나 현저히 곤란한 경우 범죄피해자에게 이를 대여할 수 있다고 결정\(2015. 6. 8. 2015-10-18 결정\)](#)
- 개인정보 보호원칙에서 가장 문제가 되는 부분은, 경찰이 교통단속, 물류운송 등 개인정보가 본래 수집된 목적을 넘어서서 무제한으로 제공받고 있는데 이에 대한 법률적 통제(범죄예방)나 적법절차(법관이 발부한 영장으로 통제) 등이 준수되고 있지 않다는 것
- 특히 지방자치단체에서 설립한 CCTV는 본래 시설안전, 주차단속 등 그 설치 목적별로 수집 및 운영되고 있었음. 그런데 이명박 정부의 방침으로 지방자치단체별로 통합관제센터가 구축되면서 본래 목적을 넘어서는 “목적외” 영상정보처리가 만연해졌음. 특히 법률상 제3자인 경찰이 영상을 실시간으로 상시제공받거나 때로는 통합관제센터를 사실상 운영하면서 영상 조작에도 관여하는 것으로 드러났음
 - [전국 CCTV 통합관제센터 운영지침 등 대부분 현행법률 위반으로 드러나](#)
 - 전국 지방자치단체가 운영하는 CCTV 통합관제센터가 경찰 상주 및 지휘 하에 운영되는 것으로 밝혀진 가운데, [관제업무에 고엽제전우회, 재향군인회 등 부적합한 단체가 용역관제를 하고 군부대와도 불법적인 정보연계를 하고 있는 것으로 드러나](#)
 - [정부, CCTV 통합관제센터 불법성 인정](#)
 - 개인정보보호위원회는 지방자치단체가 교통정보 수집, 교통단속, 범죄예방을 목적으로 수집하는 CCTV 통합관제센터 영상을 경찰서, 소방서, 군부대에 상시 제공하거나 직접 조작하도록 할 수 없다고 보았음(개인정보보호위원회 2015. 11.23. 제2015-19-33호 결정, 2015. 6. 8. 제2015-10-17호 결정 등). 다만 관련 법률 규정에 근거하여 재난재해 또는 구급상황 발생 시 현장 확인 목적으로, 긴급차량 출동 시 출동 경로 분석 목적으로, 교통사고 등 범죄수사와 공소제기 목적으로, 통합방위훈련 기간에 훈련 상황 확인 목적으로 전용회선을 통하여 위 영상을 제공하는 것은 가능하다고 보았음(개인정보보호위원회 CCTV 관련 결정례 분석)
- 나아가 ['박 대통령 비난 낙서범' 잡겠다고 기초수급자 수천명 정보를 요구](#)하는 등 경찰은 법원의 영장 없이 공공기관으로부터 국민 개인정보를 제한없이 제공받아 왔으며 때로는 민감한 건강정보와 수천 수만명에 달하는 방대한 양을 제공받아 왔음.
 - [철도노조 조합원에 대한 건강보험 무영장 자료제공 사건과 장애인·활동보조인에 대한 저인망식 싹술이 자료제공](#) 사건에 대하여서는 헌법소원이 제기되어 심사 중임

- [범죄정보관리시스템\(CIMS\)의 경우 범죄예방을 구실로 <형의 실효등에 관한 법률> 등 기존 법률이 허용하는 범위를 넘어서 피해자, 참고인 등 방대한 국민 정보를 경찰이 자의적으로 보관 운영해 왔다는 점에서 논란이 일어옴](#)
 - 현재도 구체적인 법적 근거 없이 <수사첩보 수집 및 처리 규칙>에 의해 운영되는 CIAS의 경우 검거 실적을 원하는 경찰의 마구잡이 입력 또는 조회로 인해 피해가 발생하고 있음
- 특히 최근 경찰은 범죄 통계를 이유로 빅데이터로 SNS 게시내용 등 국민 개인정보를 무작위로 수집할 계획을 밝혀 논란이 일고 있음
 - [한국 경찰, '마이내리티 리포트' 만든다](#)
 - [SNS 등 온갖 개인정보 긁어모아...위험한 범죄예측 시도](#)
- 그간 국민의 집회시위권리 행사에 보여온 경찰권의 남용과 그 폭력적인 행사에 대하여 국민의 분노와 불신이 쌓여 왔음에도 불구하고, 경찰의 정보 권한 오남용에 대해서 아무런 사회적 통제 및 제도적 대책이 존재하지 않음

<개선방안>

- 수사기관의 개인정보 무영장 수집 통제
 - 공공기관이 보유한 개인정보에 대한 경찰의 무영장 수집에 대하여 법원 등 사회적 통제와 감독 장치 마련 (개인정보보호법 제18조 제2항 제7호 개정)
- 법률에 따른 개인정보 보호
 - 경찰의 영상장비 및 데이터베이스 운용에 대하여 원점부터 필수성과 비례성 검토 및 법률에 따른 통제 추진
- 경찰 개혁
 - 권한 분산 및 경찰위원회 실질화 등 경찰 개혁 추진

8. 방송통신심의위원회 통신심의 폐지

<현황>

- 2008년 이명박 정부의 출범과 더불어 과거 정보통신윤리위원회가 담당하였던 통신분야 내용심의 기능을 이어받은 방송통신심의위원회 출범. 국회 추천 6인을 비롯한 9인의 위원으로 구성되지만 통신 분야의 전문성을 가진 심의위원이 위촉된 사례는 매우 희소함.
- [방심위의 권고에 대한 민간 사업자의 이행률은 99% 이상](#)이며, 방심위의 삭제 및 차단 권고 건수는 2014년 132,884건, 2015년 148,751건으로 계속 증가하고 있음.

- 방심위는 스스로 민간 자율기구라 주장하고 있으나 법원과 헌법재판소 재판에서 이 기구가 행정기관이며 인터넷 행정심의 역시 행정조치라는 점이 확인됨(헌재 2012. 2. 23. 2011헌가13, 판례집 24-1상, 25, 33-33)
- 한편, 방송통신위원회는 불법정보라고 판단되는 게시물에 대해 법원의 판단없이 삭제를 명령할 수 있음(정보통신망법 제44조의7)

<문제점>

- 사법부의 판단도 없이 행정기구가 자의적으로 인터넷 상의 게시물을 삭제, 차단하는 것은 국가의 검열로서 이용자의 표현의 자유와 정보접근권을 침해함.
- 방심위는 정보통신망법 제44조의 7에서 규정한 불법정보 뿐만 아니라, 유해 및 건전성의 기준으로 폭넓게 심의하고 있음(방송통신위원회의 설치 및 운영에 관한 법률 제21조). 이에 따라 정부 정책이나 권력자에 대한 비판 등 정치적 표현의 자유를 침해하는 결정이나 트위터 계정에 대한 차단 등 인터넷 통신의 매체 특성에 부합하지 않는 자의적 심의로 논란을 계속 빚어옴
- 대통령에 대한 욕설을 연상시킨다는 이유로 트위터 계정 2MB18nomA(<http://twitter.com/2MB18Noma>)에 대한 국내 인터넷 접속을 차단하거나(2011년) 사드에 대한 비판적 게시물을 삭제하는 등(2016년) 이 기구는 실제로 표현의 자유를 침해하는 결정을 다수 내려 왔음.
- 2010년 국가인권위원회는 방심위의 통신심의 권한을 “정보통신 서비스 제공자 및 게시물 관리 사업자 대표들과 시민사회 대표들이 함께 구성하는 민간자율심의기구에 이양”할 것을 권고하였으나 이행되지 않았음
- 2011년 유엔 의사표현의 자유 특별보고관은 방송통신심의위원회가 정부에 비판적인 정보를 삭제하는 사실상 사후 검열 기구로서 기능할 우려가 있다고 지적하고 “사법적 심사를 포함하여 남용을 방지할 수 있는 적절한 안전장치를 갖추고 있으며 어떠한 정치적, 상업적 및 기타 부당한 영향력으로부터도 자유로운 독립 기구에게 이양할 것을 권고”함. 2013년 유엔은 보편적 정례 인권검토(UPR)에서도 같은 내용으로 권고함

<개선방안>

- 방송통신심의위원회 통신심의 폐지
 - 유엔이 권고한 바와 같이, 정치적, 상업적 및 기타 부당한 영향력으로부터 자유로운 독립기구로 방송통신심의위원회의 통신심의 기능을 이양함.
- 방송통신위원회의 시정명령 권한 폐지
- 심의대상 축소
 - 명예훼손 등 특정 당사자가 관련된 게시물(개인의 권리침해 게시물)의 경우에는 심의기관에 의한 심의 보다는 임시조치 및 분쟁조정 제도 활용

- 불법적이지 않은 게시물에 대한 유해성 심의 금지.

<관련 자료>

- 국가인권위원회 정보통신심의제도 개선권고 (2010. 10.)

9. 인터넷 실명제는 이제 그만!

<현황>

- 2012년 헌법재판소의 위헌 결정으로 정보통신망법상 제한적 본인확인제(정보통신망법 제44조의5)가 폐지되었음. 헌법재판소는 상시적인 인터넷 실명제가 “본인확인이라는 방법으로 게시판 이용자의 표현의 자유를 사전에 제한하여 의사표현 자체를 위축시키고 그 결과 헌법으로 보호되는 표현까지도 억제함으로써 민주주의의 근간을 이루는 자유로운 여론 형성을 방해”하고 익명 표현의 자유를 침해한다고 보았음
- 그러나 여전히 인터넷/휴대전화 실명제가 광범위하게 운영되고 있음. 우선 의무적 실명제로 공직선거법을 비롯하여, 인터넷주소자원관리법, 청소년보호법, 게임산업진흥에관한법률, 전기통신사업법 등에서 본인확인을 의무화하고 있음. 이는 게임 과몰입 등 인터넷으로 인한 사회문제가 발생할 때마다 본인확인제가 손쉬운 해법으로 선호되어 왔기 때문임. 그러나 헌법재판소가 지적하였듯이 국민식별번호인 주민등록번호를 토대로 한 본인확인제는 우리나라에서만 가능한 기형적 제도로써, “그 입법목적은 달성할 다른 수단이 있음에도 불구하고 모든 게시판 이용자의 본인확인정보를 수집하여 장기간 보관하도록 함으로써 본래의 입법목적과 관계없이 개인정보가 유출될 위험에 놓이게 하고 다른 목적에 활용될 수 있도록 하며, 수사편의 등에 치우쳐 모든 국민을 잠재적 범죄자와 같이 취급하는바, 목적달성에 필요한 범위를 넘는 과도한 제한을 하는 것으로서 침해의 최소성이 인정되지 아니한다”고 할 것임
- 본인확인이 의무적이지 않은 인터넷 공간에서도 실명제가 사실상 널리 운영되면서 익명 표현의 자유와 개인정보 자기결정권이 여전히 침해되고 있음. 국민식별번호를 인터넷 서비스에 사용하고 있지 않은 세계 대다수 나라와 달리 한국에서는 정부가 직접 아이핀(I-PIN), 마이핀(My-PIN) 제도를 운용하고 본인확인기관을 지정(정보통신망법 제23조의 3)하면서 이런 현상을 직접 부추기고 있음
- 유엔 표현의자유 특별보고관은 2015년 보고서(A/HRC/29/32)에서, 휴대전화 실명제(SIM card registration policy)가 “이용자의 익명성을 직접적으로 침해하며, 정부가 개인과 언론인들을 감시하는데 이용”될 수 있음을 우려하며, “이용자가 통신수단이나 온라인 서비스에 접근하기 위한 조건으로 신원 확인을 하거나, 휴대전화 실명제를 의무화하지 말 것”을 권고하였음

<문제점>

- 2012년 헌법재판소가 판시한 바와 같이 의무적인 본인확인 제도는 익명 표현의 자유와 개인정보 자기결정권을 침해하고 있음
- 강제적인 인터넷 실명제는 이용자의 표현의 자유뿐만 아니라 이용자의 자기정보통제권 역시 침해하고 있으며, 국정원 댓글 사건이나 최순실 대포폰 논란에서 볼 수 있다시피 의도적인 불법 행위를 방지하는 효과가 없음
- 특히 선거법상 인터넷 실명제는 선관위의 폐지 의견과 19대 국회 정개특위의 폐지 결정에도 불구하고, 아직 폐지되지 않고 있음. 2012년 대통령 선거 당시 국가정보원의 댓글 가입 사건에서 보았듯이 포털 사이트에서 운영 중이던 실명제는 부정선거를 방지하는 효과가 없었을 뿐 아니라, 신분 노출 우려가 있는 비판적 의견 소지자와 사회적 약자의 표현의 자유 행사를 위축시킬 뿐임
- 한편, 쇼핑몰 등 주요 인터넷 사이트에서는 본인확인이 의무적이지 않음에도 여전히 본인확인 시스템을 유지하고 있음. 해외의 주요 인터넷 사이트들이 본인확인 없이도 큰 문제 없이 운영되고 있는 사실을 고려할 때, 국내 인터넷 사이트들의 본인확인은 과도한 개인정보 수집이라고 할 수 있음. 그러나 정부는 이를 규제하기는 커녕, 본인확인기관 및 아이핀과 마이핀 제도를 통해 이를 부추기고 있음. 민간업체들이 본인확인이 필요한 경우 자신의 목적에 맞는 본인확인 방법을 스스로 찾아야 마땅하며, 정부가 민간 서비스 용도의 본인확인 기관을 지정하는 것은 전 세계에 유례가 없음.
- 아이핀과 마이핀은 ‘주민등록번호 대체수단’으로서 고안된 것이나, 이 역시 주민등록번호를 기반으로 하고 있어, 통신사 및 금융기관 등 민간업체의 주민등록번호 수집을 허용하는 근거가 되고 있음(정보통신망법 제23조의 2). 통신사, 금융기관 등 본인확인기관은 주민등록번호 및 이용자의 사이트 가입 내역이라는 민감한 정보를 보유하는 특혜를 누리고 있을 뿐 아니라, 주민등록번호를 토대로 수집한 개인정보를 수집 목적 외로 영리적으로 활용하고 있는 실정임. 또한, 이용자의 사이트 가입 내역이 특정 업체에 집중 관리되면서, 이러한 정보가 유출되거나 보유기관에 의해 남용될 위험이 있으며, 영장 없이 정보·수사기관에 제공됨으로써 이용자의 정보인권이 침해될 우려가 있음.
- 이동통신 서비스의 경우에는 주로 채권추심 목적으로 주민등록번호를 수집해왔으나, 휴대전화의 부정이용을 방지한다는 이유에서 2014년 전기통신사업법 개정(제32조의 4)으로 휴대전화 실명제(가입시 본인확인 의무화 및 통신사의 개인정보 등록)가 시행되고 있음. 모바일 인터넷이 보편화된 시대에 휴대전화 실명제는 이용자의 프라이버시에 치명적인 영향을 미칠 수 있음. 2014년 미국 연방대법원에서 지적하였듯이 휴대전화에는 개인의 민감한 모든 정보들이 기록될 수 있기 때문에, 사생활 침해나 국가 감시 노출 위험성이 과거보다 크게 증가함. 범죄수사를 명분으로 휴대전화 실명제가 필요하다고 주장하지만, 이미 최순실-박근혜 비리 관련자들의 광범위한 대포폰 사용에서 알 수 있듯이, 실제

범죄자들은 휴대전화 실명제를 우회할 수 있음. 수사가 필요한 경우에는 실제 명의자와 무관하게, 통신사실확인자료 조회를 통해 실사용자를 추적하는 것이 가능함

<개선방안>

- 인터넷 실명제 폐지
 - 선거법상 인터넷 실명제를 비롯한 인터넷 상 본인확인 의무화 폐지 (공직선거법, 청소년보호법, 게임산업진흥법 등 개정)
- I-PIN, 마이핀 등 본인확인기관 제도 폐지 (정보통신망법 개정)
- 휴대전화 실명제 폐지(전기통신사업법 개정) 및 통신사의 주민등록번호 수집 금지

10. 다자간 주소자원 거버넌스 활성화

<현황>

- IP주소, 도메인 네임 등 인터넷 주소자원의 관리(거버넌스)는 전 세계적으로 민간을 중심으로 한 다자간(멀티스тей크홀더) 거버넌스 방식으로 이루어지고 있음. 세계 주소자원 관리를 위한 국제기구인 국제인터넷주소관리기구(ICANN) 역시 유엔 산하의 정부간 기구가 아니라, 업계, 기술계, 학계, 시민사회, 정부 등 다양한 이해당사자의 개방적인 참여를 바탕으로 상향식(Bottom-Up)으로 관련 정책을 논의하는 비정부 기구임.
- 다수 이해당사자 (멀티스тей크홀더) 기반, 합의(Consensus) 기반 거버넌스는 국내외 인터넷 거버넌스의 원칙으로서 다수의 국제 포럼(유엔, 유럽평의회, G8 등)에서 인정하고 있으며, ICANN 및 유엔 인터넷거버넌스포럼(IGF)의 운영 원칙이 되고 있음.
- 2014년 브라질 상파울로에서 개최된 '인터넷 거버넌스의 미래에 대한 세계 멀티스тей크홀더 회의(일명 '넷문디얼' 회의)'의 합의문은 인터넷 거버넌스의 원칙을 다음과 같이 규정하고 있음.
 - 멀티스тей크홀더 접근
 - 개방적, 참여적, 합의기반 거버넌스
 - 투명성
 - 책임성(Accountable)
 - 포용성(Inclusive)과 동등성
 - 분산성 : 분산적이고 탈중심적 거버넌스
 - 협력과 의미있는 참여
- 한국 역시 인터넷 도입 초기부터 세계적인 흐름에 맞게 민간 중심의 주소자원 거버넌스를 수행해 왔음. 인터넷 도입 초기 학계를 중심으로 이루어진 주소자원 거버넌스는 99년

재단법인 한국인터넷정보센터(KRNIC)의 설립과 함께, 거버넌스 기구인 주소위원회(NNC)를 통해 정부, 업계, 학계, 시민사회 등 다양한 이해당사자가 참여하는 방식으로 발전함.

- 그러나 한국 정부는 당시 거버넌스 기구인 ‘주소위원회’의 반대에도 불구하고, 2004년 <인터넷주소자원어관한법률(주소자원법)>을 통과시킴으로써 이후 ‘정부 주도의 거버넌스’로 전환됨.
- 당시 ‘주소위원회’에 참여하였던 민간 전문가들은 정부와의 협의를 통해 동 법률 시행령에 ‘인터넷주소정책 실무위원회’를 두고 민간의 자발적 참여 전통을 이어가려고 하였으나, 2년만에 인터넷주소정책실무위원회는 중단됨.
- 2014년 브라질에서 개최된 ‘인터넷 거버넌스의 미래에 대한 세계 멀티스тей크홀더 회의’ 이후, 한국에서도 다자간 인터넷 거버넌스 실현을 위한 노력이 시작됨. 2014년 구성된 다자간인터넷거버넌스협의회(KIGA)는 국내에서 상향식의 다자간 인터넷 거버넌스를 실현하기 위해, 학계, 기술계, 업계, 시민사회, 정부 등 다양한 이해당사자의 자발적인 참여를 기반으로 구성되었으며, 다자간 정책 대화의 촉진을 위해 매년 한국 인터넷거버넌스포럼을 개최하고 있음.
- 현재 주소자원법상 ‘인터넷주소정책 심의위원회’가 존재하지만 위원 선임이 하향식으로 이루어지는 등 실질적인 다자간 거버넌스 기구로서는 한계가 있으며, KIGA의 주소자원분과를 통해 주소자원 관련 정책이 논의되고 있음. 현재 KIGA 주소자원분과와 인터넷주소정책심의위원회의 상호 소통을 위한 노력이 진행되고 있음.

<문제점>

- 세계적인 인터넷 환경에서 다자간 거버넌스는 공공정책의 민주성 뿐만 아니라, 실효성을 위해서도 도입할 필요가 있으며, 주소자원 영역을 시작으로 다른 공공정책 영역에도 확산될 필요가 있음.
- 정부 주도의 거버넌스가 이루어질 경우, 정부에 의해 선택된 사람들 외에는 자발적으로 인터넷 거버넌스에 참여할 동기가 약화될 수밖에 없음. 일부 민간 참여자들의 참여 노력이 지속되고 있음에도 불구하고, 2004년 주소자원법 신설 이후 민간의 참여가 위축될 수 밖에 없었음.
- 이는 세계적인 인터넷 거버넌스 공간에서도 한국의 위상과 역할의 약화를 가져올 수밖에 없음. 다른 나라의 경우 ICANN, 세계전기통신연합(ITU), OECD 등 세계 인터넷 거버넌스 포럼에 민간 영역의 비정부 이해관계자가 활발히 참여하고 있는데, 한국은 이에 참여하여 한국 비정부 이해관계자의 목소리를 낼 경험과 역량이 축적될 수 없기 때문임.

<개선방안>

- 주소자원 관리업무를 다자간 거버넌스 기구로 이양

- 현재 한국인터넷진흥원(KISA)이 담당하고 있는 국내 주소자원 관리 업무를 (과거 재단법인 KRNIC과 같은) 민간기구가 수행하도록 독립시키고, 정부주도의 인터넷주소정책심의위원회를 상향식의 다자간 거버넌스 기구로 개편함. (주소자원법 개정 필요).
- 정부가 국내 인터넷 주소자원에 관한 최종적인 감독권한은 보유하되, 특별한 문제가 없는 한 일상적인 거버넌스는 다자간 거버넌스 기구를 통해 이루어질 수 있도록 보장함.
- 다자간 거버넌스 지원
 - 국내 및 세계 인터넷 거버넌스에 한국의 이해당사자들이 활발히 참여할 수 있도록 재정적, 정책적 지원이 필요함. 또한, 한국에서 KIGA와 같은 상향식의 다자간 인터넷거버넌스가 뿌리내릴 수 있도록 법적 근거를 마련하고, 정부 정책 담당자의 적극적인 협력이 필요함.