「 '4차 산업혁명'과 정보인권 」 연속토론회

정보·수사기관과 미래 신기술, 어떻게 만나야 하는가

일 시 | 2017년 7월 24일(월) 오후 2시~5시

장 소 | 국회의원회관 제1세미나실

주 최 |

국회 미래창조과학방송통신위원회
변재일 의원 (더불어민주당, 충북 청주시청원구)
김성수 의원 (더불어민주당, 비례대표)
추혜선 의원 (정의당, 비례대표)
국회 안전행정위원회
진선미 의원 (더불어민주당, 서울 강동구갑)
권은희 의원 (국민의당, 광주 광산구을)
이재정 의원 (더불어민주당, 비례대표)
언론개혁시민연대, 정보인권연구소, 진보네트워크센터, 참여연대, 한국소비자단체협의회, 함께하는시민행동

후 원 | 국가인권위원회

순 서

2:00 ~ 2:10	개회	
2:10 ~ 2:20	인사말	
	사회	한상희	건국대학교 법학전문대학원 교수
2:20 ~ 3:00	발제	이호중	서강대학교 법학전문대학원 교수 정보인권연구소 이사장
3:00 ~ 4:30	토론	양홍석	참여연대 공익법센터 소장
		장여경	진보네트워크센터 정책활동가
		조현주	민주노총 법률원 변호사
		강신걸	경찰청 수사기획과장
		김민섭	국가인권위원회 인권정책과 사무관
4:30 ~ 5:00	전체토론	

「 ‘4차 산업혁명’과 정보인권 」 연속토론회를 개최하며

진선미 | 더불어민주당 국회의원
(강동구 갑)

안녕하세요. 더불어민주당의 진선미 의원입니다.

먼저 『4차 산업혁명과 정보인권』 연속토론회를 주최해주신 언론개혁시민연대, 정보인권연구소, 진보네트워크센터, 참여연대, 한국소비자단체협의회, 그리고 함께하는시민행동 관계자 여러분, 존경하는 변재일, 김성수, 이재정, 권은희, 추혜선 의원님께 감사의 말씀 드립니다. 또한 이 토론회를 후원해주신 국가인권위원회에 감사드립니다.

연속토론회의 첫 토론을 이끌어주실 한상희 교수님과 첫 발제자인 이호중 교수님을 비롯 참석자 여러분과 앞으로도 자리를 빛내주실 모든 분들께 감사의 말씀을 드립니다.

저는 국회에서 입법을 하고 있지만, 법을 통한 규제는 최소화 되어야 하고, 예측가능해야 합니다. 특히 범죄 예방과 수사 및 처벌 과정에서 정말 법개정을 통해 피해발생을 막을 수 있을까? 공권력의 권한이 커질수록 이로 인해 또 다른 인권침해가 발생하지 않을까? 다각도의 다양한 고민과 사회적 토론이 필요합니다.

특히 범죄자를 찾아내는 수사기관의 역량은 CCTV, 드론 등 기술 발전을 통해 한층 성장하고 있습니다. 기술의 발전은 법이 선언한 정의를 실현하는데 필수불가결한 요소가 되어가고 있지만, 이로 인해 발생되는 개인들의 개인정보 노출과 인권은 논의조차 제대로 이뤄지지 않고 있습니다.

날로 발전하는 기술의 힘 앞에서 갈수록 우리의 개인정보는 보호받지 못하고 있습니다. CCTV는 범죄의 사각지대를 줄여가고 있지만, 동시에 우리는 일거수일투족이 감시받고 개인정보가 무차별적으로 노출될 위협에 시달리게 되었습니다.

저는 안전하게 살 권리와 정보 인권 중 하나만을 선택하는 것은 옳지 못하며, 그럴 수도 없다고 생각합니다. 우리의 안전권과 정보인권은 불가분의 것이 아니기 때문입니다. 그렇다면 우리는 어떻게 해야 새로운 기술이 우리의 안전을 지켜주면서 동시에, 우리의 권리를 침해하지 않을까 고민해야 합니다.

4차 산업혁명에 대한 준비와 고민이 더욱 절실하고 시급한 이유입니다. 과학 기술의 발전 속도는 점점 빨라지고 있지만, 기술을 사용하는 우리는 이에 따라가지 못하는 경우가 많습니다. 이번 연속토론회는 우리의 고민을 심층적으로 논의해보고 지혜로운 해법을 만들어가기 위한 준비의 첫 시작일 것입니다. 결국 법의 정의를 구현하는 기술은 다시 규제와 법의 통제 아래에서 유효할 것이라 믿습니다.

오늘의 토론회가 미래를 준비하는 긴 여정의 힘찬 시작이 되길 바라며 다시 한 번 이 자리를 빛내주신 모든 분들을 환영합니다.

감사합니다.

시민, 노동자, 소비자의 정보인권을 보장하는 미래를 개척해야

이종회 | 진보네트워크센터 대표

‘4차 산업혁명’과 ‘개인정보 보호 강화’는 모두 다 문재인 정부의 공약입니다. 두 개의 약속을 조화시킬 수 있는 방안은 무엇일까요?

정보인권은 민주주의 회복 및 강화와 떼어놓고 생각할 수 없습니다. 인권 경시가 국민 감시를 낳고 국가 폭력이 국민 사찰로 이어질 수 있다는 것을, 우리는 지난 정권에서 목격했습니다. 국가정보기관과 수사기관에 대한 개혁이 없으면 미래 신기술은 국민에 대한 첨단감시수단이 될 것입니다. 맹목적이었던 ‘창조경제’가 부패한 정경유착으로 국민들에게 큰 충격을 주었던 역사를 기억해야 할 것입니다.

이른바 ‘4차 산업혁명’에 대한 기대가 높습니다. 그러나 어떤 ‘4차 산업혁명’이 될지는 미지수입니다. 국민들이 바라는 ‘4차 산업혁명’은 ‘정보인권’의 가치와 조화를 이루는 것입니다.

그러나 우리의 현실은 어떻습니까? 대형마트 홈플러스와 여러 개 보험회사가 정보주체 모르게 개인정보를 팔아넘겨 재판을 받고 있습니다. 미국 빅데이터 기업 IMS헬스는 우리 국민 4천 4백만 명의 민감한 처방전 정보를 사가서 지금도 이용하고 있습니다.

이것은 시민, 노동자, 소비자가 바라는 빅데이터의 미래가 아닙니다. 빅데이터 이용은 국민들에게 혜택을 가져올 수도 있지만 이를 위해서는 개인정보 보호와 균형을 이루어야 합니다. 사물이 인터넷에 연결되어 있는데 개인정보가 자기도 모르게 계속 새나간다면 국민들이 자율주행차량을 안심하고 탈 수 있겠습니까? 개인정보 보호에 대한 국가적인 감독이 강화되어야 합니다. 정보·수사기관의 미래신기술 이용이 국민에 의해 통제되어야 함은 물론입니다.

인권을 보장하고 일자리도 지키는 미래는 시민과 노동자, 그리고 소비자의 힘으로 개척해 가야 할 것입니다. 이 토론회가 그 미래를 함께 열기 위한 논의의 장이 될 수 있기를 바랍니다.

감사합니다.

정보수사기관과 미래신기술의 만남
– 감시시스템과 민주주의?

이호중 | 서강대 법학전문대학원 교수, 정보인권연구소 이사장

Ⅰ. 서론

■ ICT와 정보·수사기관의 만남

• **정부는 '인공지능'과 빅데이터를 활용한 '지능형 정부' 구축 본격화**

- 선제적 행정서비스를 제공하는 '비포 서비스'(Before Service)
- IoT(사물인터넷) 전국망 구성
  * 예) 독거노인 가정에 움직임센서·가스센서 등을 설치해 119 상황실 등과 연계하는 등 사회적 약자에 대한 생활지원서비스 제공

• **치안서비스에서도 ICT의 접목 가속화 예상**

- ICT 기반으로 '스마트한" 경찰활동, 효율적인 수사와 범죄예방 강조

• 국정기획자문위 100대 과제 중에서

14 민생치안 역량 강화 및 사회적 약자 보호 (경찰청)

○ (공동체 예방치안) '17년부터 **파출소 증설 및 탄력순찰제 등 주민밀착·참여형 치안 강화, 범죄예방 환경 디자인**(CPTED) 등 예방 시스템 개선과 인프라 확충*

* △범죄예방진단팀(CPO) 역량 강화 △여성무인택배함 설치 확대 △안심귀가서비스 강화 등

○ (치안인프라 확충) '17년부터 **치안 R&D 활성화**(육안 미확인 법광원, CCTV 영상 검색 고도화 등)**로 스마트 폴리스 구현, 국과수 미설치 지역**(제주 등 11곳) **합동 감정체계 구축, 의무경찰 단계적**(5년) **감축** 및 경찰 인력 증원

- 근속승진 단축 등 경찰 처우 개선, 교정시설 과밀화 단계적 해소

Ⅱ. CCTV, 그리고 통합관제

1. CCTV 설치현황과 기술적 발전

■ CCTV의 설치 현황

• 2015년 12월 31일 기준 국가 및 지방자치단체가 공개된 장소에 설치, 운영하고 있는 CCTV는 739,232대

(2015. 12. 31. 기준)

구분	합계	설치 목적			
		범죄예방	시설안전	교통단속	교통정보수집
총계	739,232대	340,758대 (46.1%)	363,331대 (49.1%)	21,243대 (2.9%)	13,900대 (1.9%)
중앙행정기관 (교육기관 포함)	419,194대	173,649대	229,866대	7,228대	8,451대
지방자치단체	320,038대	167,109대	133,465대	14,015대	5,449대

• 민간용 CCTV까지 합치면,
전국에 설치된 CCTV는 2015년 12월 말 기준 795만 6천여대 (세계 1위)
(한국정보화진흥원, 정보화통계집)

• 차량용 블랙박스는 최근 급속한 증가추세이지만, 정확한 통계는 없음

Ⅱ. CCTV, 그리고 통합관제

1. CCTV 설치현황과 기술적 발전

■ CCTV의 기술적 발전 (1)

• 360도 회전기능과 12배 이상의 줌인(zoom-in) 기능 보편화

• 지능형 CCTV의 개발

- 사물이나 사람의 특징적인 행동을 자동으로 인식하는 기능의 CCTV
- 원격제어 PTZ(Pan Tilt Zoom) 기능 + 상황인지기능
- 영상을 실시간으로 분석하여 움직임이 있는 사람・물체를 감지・추적
- 위험상황의 징후를 포착하면 "알람 + 위험현장 자동으로 모니터 전환"

• 지능형 CCTV 인증제도 시행

- 2017년 3월 KISA에서 지능형 CCTV 소프트웨어 솔루션 인증을 실시 시작
- 인증분야 : 배회(필수항목) 침입(필수항목) 유기(선택) 쓰러짐(선택)
  싸움(선택) 방화(선택)

• 2016년 12월 말 기준 전국의 통합관제센터에 연결된 CCTV 총 174,393대, 그 중 지능형 CCTV는 9,215대(4.78%)

- 아직은 지능형 CCTV의 기술은 초보적인 수준

Ⅱ. CCTV, 그리고 통합관제

1. CCTV 설치현황과 기술적 발전

■ CCTV의 기술적 발전 (2)

- 지능형 CCTV는 다양한 기술적 수단의 접목 가능성
- 음성인식기능의 CCTV, 그러나 현행 개인정보보호법 위반
  - 2013년 충북 진천군에서는 "듣는 지능형 CCTV" 도입
  - 영상정보와 더불어, 비명 등 위험상황과 관련된 음성 및 소리정보의 인식기능

(사례) 진천군의 CCTV
- 노인이 휠체어에서 굴러 떨어지면서 소리지른 비명을 CCTV가 즉각 감지해 모니터요원에게 경고음 발령
- 모니터요원이 곧바로 인근 파출소에 상황을 전달해 노인을 구조

- CCTV와 안면인식프로그램의 결합
  - 2014년 9월 미국 FBI는 차세대신원확인(NGI: Next Generation Identification) 프로젝트 : 기존의 안면인식시스템을 넘어서 홍채, 목소리, 손금, 걸음걸이 등을 자동 인식해 특정 인물을 조회할 수 있는 시스템
  - 경찰청은 구속피의자 얼굴사진을 3D 형태로 데이터베이스화하고, CCTV에 촬영된 얼굴과 비교검색에 제공
  - CCTV에서 인식한 안면영상을 지정하여 실시간으로 CCTV를 검색, 추적하는 기술도 발전

Ⅱ. CCTV, 그리고 통합관제

2. CCTV 통합관제 시스템

■ CCTV 통합관제센터

- CCTV 통합관제센터
  = 서로 다른 공공기관이 다양한 목적에 따라 설치·운영하고 있는 영상정보처리기기(CCTV)들을 통합적으로 연계하여 집중화된 시설인 통합관제센터에서 관리하는 시스템
  (생활 안전, 법규위반 단속, 시설물 관리 등 공공목적을 위해 설치된 영상정보처리기기를 지정된 별도의 공간에서 통합관리할 수 있는 시설을 갖추고 영상정보처리기기를 이용하여 각종 사건·사고 예방 및 사후조치 등의 기능을 수행할 수 있는 시설)
- 2003년 강남구와 강남경찰서의 협의에 따라 강남구 관내의 CCTV를 통합운영하는 종합상황실을 설치한 것이 최초
- 현재는 대부분의 지자체(시군구 단위)에서 CCTV 통합관제센터 운영
  - 행정안전부 훈령에 근거
    「지방자치단체 영상정보처리기기 통합관제센터 구축 및 운영 규정」
  - 2017년까지 전국 모든 지자체에 통합관제센터 설치 완료 계획
  - 통합관제센터는 각 지자체 내에 설치하여 지자체가 운영주체이나, 경찰관 다수가 통합관제센터에 파견근무
  - 실제 통합관제센터의 CCTV 관제는 파견 경찰관의 지시에 따라 수행

Ⅱ. CCTV, 그리고 통합관제

2. CCTV 통합관제 시스템

■ CCTV 통합관제센터의 모습

Ⅱ. CCTV, 그리고 통합관제

2. CCTV 통합관제 시스템

■ 통합관제센터의 서비스 구성

• 목표 : 범죄 또는 재난·재해가 발생하는 등의 긴급상황 시에 "유관기관과 연계하여 신속한 합동대응"이 가능하도록 네트워킹

Ⅱ. CCTV, 그리고 통합관제

2. CCTV 통합관제 시스템

■ 행정안전부, 『'지능형 CCTV 관제 서비스 체계 구축'을 위한 정보전략계획』(2017년)

- 2016년 말 기준 전국의 통합관제센터에 연결된 CCTV 수는 174,393대
  - 관제요원 수 3,612명(3교대 근무) / 1인당 평균 145대 관제
- 행안부는 관제요원 부족으로 인한 비효율성의 문제를 적극적으로 제기

행안부 지역정보지원과장

적정 관제를 위해서는 6,852명의 관제요원이 추가돼야 하며 인건비로는 연간 1,644억 원이 더 확보 돼야 하는 실정입니다

- **2단계 사업 추진 : "육안관제"에서 "지능형 통합관제"로**
  - 전국 지자체의 통합관제센터에 공통 적용이 가능한 지능형 관제서비스 모델 개발 / 지자체 관제 모델을 공통 및 특화 서비스로 나눠 적합한 운용체계(OS) 마련
  - 통합관제센터가 안전허브(HUB)의 역할 담당

Ⅱ. CCTV, 그리고 통합관제

3. 무엇이 문제인가

■ CCTV의 개인정보 수집목적의 광범위성

- 개인정보보호법 제25조 제1항에서 영상정보처리기기의 설치목적 규율
  - '범죄의 예방'이라든가 '시설안전', '화재예방' 등 설치목적의 범위가 매우 광범위하고 추상적이라는 점에서 문제
  - 안내판만 설치하면 누구나 손쉽게 영상정보처리기기를 설치·운영
- 경찰의 일방적이고 주관적인 판단 또는 지역주민의 요구에 의하여 CCTV를 손쉽게 설치·운영
- **목적구속의 원칙 형해화**
  - 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고, 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집해야 한다는 원칙이 CCTV에 관한 한, 규제적 기능을 전혀 수행하지 못함

개인정보보호법
제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 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

Ⅱ. CCTV, 그리고 통합관제

3. 무엇이 문제인가

■ '목적외 이용'으로서 집회감시의 문제

- 개인정보보호법 제17조, 제18조는 개인정보의 목적외 이용을 제한
- 집회·시위에 대한 감시 목적으로 CCTV를 활용한 사례
  - 2013년 8월 경찰은 중구청의 통합관제센터에 상주하면서 모니터상으로 줌인 기능과 회전기능을 활용하여 대한문 앞의 집회 현장을 감시
  - 2014년 3월 15일 유성희망버스 사례에서 경부고속도로 옥천 나들목 부근에 설치된 고속도로용 CCTV가 규정 각도를 벗어나 희망버스 참가자를 감시
  - 2014년과 2015년 대규모 집회에서 경찰이 CCTV통합관제센터의 정보를 실시간으로 받아서 집회현장을 감시
- CCTV로 집회현장을 감시하는 것은 위법
  - 집회감시는 CCTV 설치의 본래의 목적이 아니며, 목적외 이용으로서도 정당한 근거가 없음
  - 집회시위의 자유에 대한 침해 야기

독일의 연방 집시법 제12a조
- 집회·시위에 대한 녹음 및 비디오감시는 공공의 안전과 질서에 대한 현저한 위험이 발생한 경우 내지 타인의 생명·신체 등 중요한 법익에 대한 구체적 위험이 존재하는 경우에 한하여, 그리고 그러한 위험을 방지하기 위하여 필요한 범위에서만 허용
- 조망촬영의 금지

Ⅱ. CCTV, 그리고 통합관제

3. 무엇이 문제인가

■ '목적외 이용'으로서 수사기관에 영상정보를 제공하는 문제

개인정보보호법 제18조 ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우

- 그런데 이 규정은 경찰이 공공기관으로부터 정보제공을 받을 수 있는 수권규정이 아니다. 개인정보처리자의 정보제공에 관한 근거규정일 뿐임.
- 수사기관의 개인정보 수집은 기본권침해처분이기 때문에 임의수사가 아니라 강제수사로 보아야 한다.
  - 현행법상 수사기관의 개인정보 수집의 법적 근거는 과연 있는가?
- 경찰관직무집행법 제2조는 근거가 되는가 – 개괄적 수권규범의 문제

경찰관직무집행법 제2조(직무의 범위) 경찰관은 다음 각호의 직무를 행한다.
1. 범죄의 예방·진압 및 수사
2. 경비·요인경호 및 대간첩작전수행
3. 치안정보의 수집·작성 및 배포
4. 교통의 단속과 위해의 방지

Ⅱ. CCTV, 그리고 통합관제

3. 무엇이 문제인가

<<CCTV 통합관제센터의 문제>>

■ 법적 근거가 없다

- 현재 통합관제센터의 구축 및 운영에 관한 명시적인 법적 근거는 없는 상태
- 개별적인 공공기관 주체들이 영상정보처리기기를 각각 운영.
  그러나, 통합관제시스템은 통합관제센터라는 별개의 조직이 운영주체가 되어 개인영상정보를 수집·이용하는 것이므로 별도의 법적 근거가 반드시 필요

- 개인정보보호위원회는 2016년 5월 통합관센터의 설치근거 법령이 없음을 이유로 김앤장 법률사무소에 용역을 의뢰해 개인영상정보호보법안을 마련
- 2016년 12월 정부는 개인영상정보보호법안 입법예고

■ 목적구속의 원칙 무력화

- 통합관제센터는 방범용, 쓰레기투기방지, 시설물관리, 주차관리, 교통정보수집 등 개별적인 목적에 따라 설치·운영되어 오던 CCTV들 통합적으로 연계하는 시스템을 구축
- 통합관제시스템에 의한 영상정보의 통합·연계는 '목적외 이용의 제한' 규정을 위반한 것임

Ⅱ. CCTV, 그리고 통합관제

3. 무엇이 문제인가

<<CCTV 통합관제센터의 문제>>

■ 다목적용 안내판이면 충분?

- '다목적용'이라는 방식은 목적구속의 원칙상 용인되기 어려운 것
  - 개인정보를 제한하는 조치들은 그 목적이 명확해야 하며 또한 구체적으로 특정되어 있어야 하기 때문
- CCTV 감시는 그 설치목적과는 무관한 다수 사람들의 개인영상정보를 불가피하게 수집하게 되며, 개인식별능력이 뛰어나다는 점에 비추어 보면, 그 설치목적과 영상정보의 수집방법, 정도 등은 다른 개인정보의 수집보다 규범적으로 더욱 명확하게 설정되어야 할 필요

Ⅱ. CCTV, 그리고 통합관제

3. 무엇이 문제인가

<<CCTV 통합관제센터의 문제>>

■ 사실상 전방위적인 경찰감시의 수단

• 통합관제센터의 공식적인 운영주체는 지자체장
그러나 실제 운영은 통합관제센터에 파견된 경찰관의 지휘를 받는 방식

- 관제요원의 선발・교육과 관리를 경찰서에서 담당
- 센터에 파견된 경찰관이 관제요원을 지휘・감독하는 방식

• 실시간 네트워킹

- 경찰서, 소방서, 교통정보센터, 재난관제실 등 유관기관에 영상정보의 실시간 전송을 위한 네트워크를 구축하고, 해당 기관의 운영자의 접속권한을 부여
- 경찰은 관할구역 내의 거의 모든 영상정보처리기기를 장악
- 이를 통해 집회시위에 대한 감시 또는 특정 개인에 대한 집중감시의 도구로 이용될 수 있는 위험성이 현저하게 증대

Ⅲ. ICT의 접목 – 통합관제를 넘어선 위험

1. AVNI와 통합관제의 결합

■ 차량번호자동식별/수배차량검색프로그램

• 경찰청은 전국 도로에서 운행중인 차량을 자동으로 식별·감시할 수 있는 통합 시스템 구축(2014년)

- 차량번호 자동수집이 가능한 전국의 차량방범용 CCTV 5929대에 찍히는 모든 차량정보를 경찰청 서버로 실시간 전송하는 시스템 구축
- 기존의 차량사진촬영 및 차량번호 수집장치(AVNI)와 결합하여 차량번호 뿐만 아니라 차량의 동영상도 네트워킹으로 확인 가능
- 3개월 동안 모든 차량정보를 경찰청 서버에 보관
- 이 시스템과 CCTV 통합관제센터의 결합

⇒ 특정 차량 및 탑승자에 대한 실시간 감시 가능

CCTV 통합관제시스템에서 특정 차량 추적 과정

자료: 진선미 새정치민주연합 의원실

수배차량 발생정보: 발생될 때 알람이 뜸

실시간 이동경로 확인, 영상: 특정차량의 번호를 쳤을때 이동경로가 팝업되고 사진을 볼 수 있음

Ⅲ. ICT의 접목 – 통합관제를 넘어선 위험

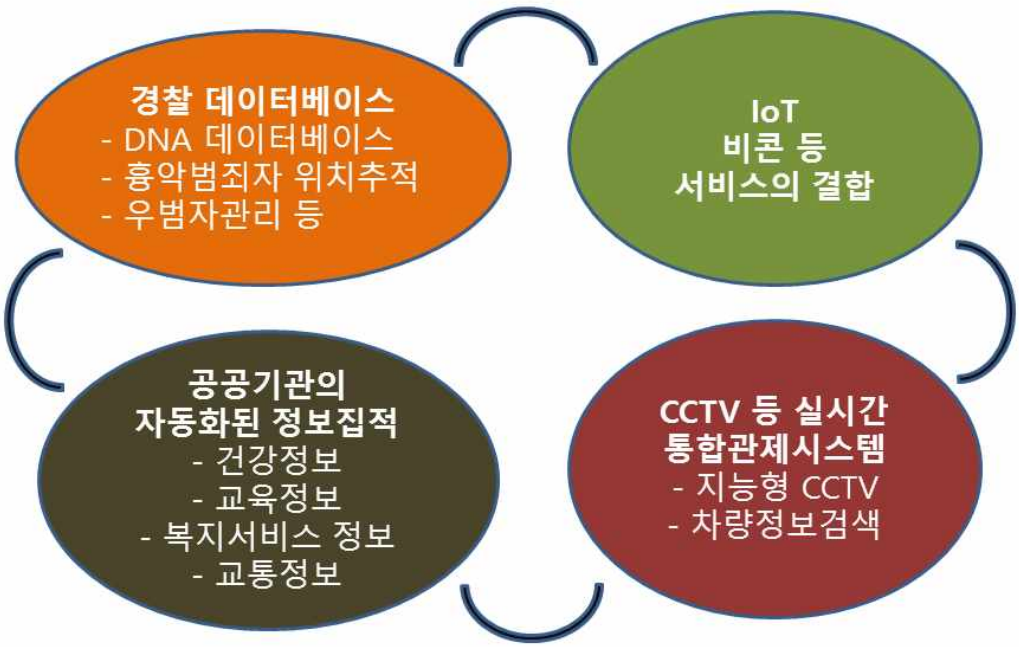
1. AVNI와 통합관제의 결합

수배차량 검색체계 개념도

Ⅲ. ICT의 접목 – 통합관제를 넘어선 위험

2. 다양한 IT 기술의 결합

■ CCTV를 넘어선 통합관제시스템의 미래 가능성



Ⅳ. 법적 제도적 통제장치 전무

1. 수사기관의 개인정보수집에 관한 법규정들

■ 개인정보처리자가 수사기관에 개인정보를 제공하는 법적 근거

개인정보보호법
제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.
② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우

Ⅳ. 법적 제도적 통제장치 전무

1. 수사기관의 개인정보수집에 관한 법규정들

■ 수사기관이 개인정보를 수집하는 법적 근거?

형사소송법 제199조(수사와 필요한 조사) ② 수사에 관하여는 공무소 기타 공사단체에 조회하여 필요한 사항의 보고를 요구할 수 있다.

경찰관직무집행법 제2조(직무의 범위) 경찰관은 다음 각 호의 직무를 수행한다.
1. 국민의 생명·신체 및 재산의 보호
2. 범죄의 예방·진압 및 수사
3. 경비, 주요 인사(人士) 경호 및 대간첩·대테러 작전 수행
4. 치안정보의 수집·작성 및 배포
5. 교통 단속과 교통 위해(危害)의 방지
6. 외국 정부기관 및 국제기구와의 국제협력
7. 그 밖에 공공의 안녕과 질서 유지

개인정보보호법 제15조(개인정보의 수집 · 이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
(이하 생략)

IV. 법적 제도적 통제장치 전무

2. 법적 근거가 있는가?

■ 수사기관의 개인정보 수집의 법적 근거는 과연 있는 것인가

- 경직법 제2조는 수권규범이 아니라 직무규범의 성격
- 독일의 경우
  - 독일 연방헌법재판소가 인구조사법의 인구조사에 대해 개인정보자기결정권을 침해하는 것이라는 위헌결정을 한 후에, 국가기관의 정보수집 및 처리에 관하여 상세한 법규정을 두고 있음
  - 독일 각 주의 경찰법이 모두 경찰의 직무규정 외에 경찰의 개인정보 수집 및 처리에 관하여 상세한 규율
- 현행 경직법 제2조가 개괄적 수권조항?
- 개인정보보호법 제15조 제1항이 근거 규정?
  - 헌법재판소 결정(헌법재판소 2005.7.21. 2003헌마282 결정) 교육정보시스템(NEIS) 사건

"개인정보보호법 제15조 제1항 제3호가 경찰의 개인정보 수집 및 처리의 '일반적 수권규정'이 될 수 있다."
"개인정보의 수집 및 처리에 관해서는 원칙적으로 구체적이고 개별적인 수권규정이 필요하나, 그러한 개별적인 수권규정이 없는 경우에, 일반적 수권규정으로서 개인정보보호법 제15조 제1항 제3호 원용"

IV. 법적 제도적 통제장치 전무

2. 법적 근거가 있는가?

■ 수사기관의 개인정보 수집에 관한 통제장치가 없다!

- 형소법 제199조 제1항이 법적 근거?
  - 통설은 이 규정을 임의수사 규정으로 이해
  - 그런데 사실조회의 요청 대상이 개인정보를 포함하고 있는 경우에는 개인정보자기결정권에 대한 침해의 문제를 야기
  - 개인정보 제공은 애초에 공공기관이 개인정보를 수집한 목적을 벗어나 수사기관에 제공한 것이기 때문에 이는 '새로운' 개인정보자기결정권에 대한 침해행위에 해당
  - 따라서 수사기관의 개인정보 수집은 강제수사로 규율되어야 마땅함.
- 수사기관의 개인정보 수집은 기본권제한조치이기 때문에
  - 법률유보의 원칙에 따라 법률에 명확한 근거가 있어야 할 뿐만 아니라,
  - "필요최소한도의 제한"이라는 비례성원칙에 합치하는 범위에서만 정당화
- 경직법 제2조를 개괄적 수권조항으로 해석하고, 수사에 관해서는 형소법 제199조 제1항을 개인정보수집의 법적 근거라고 본다면, **현재의 법상황은 "총체적으로 헌법위반"**
  - 다양한 기술적 기반 위에 확장되는 수사기관의 정보수집을 통제할 법적 장치가 전무하기 때문

Ⅴ. RCS 논란을 회고하며

1. RCS논란의 시작

■ 이탈리아 공격용 보안(Offensive Security) 프로그램 회사 "Hacking Team"의 RCS – 국정원이 구입

• RCS(Remote Control System)
- PC나 스마트폰을 원격으로 제어하는 '스파이웨어'의 일종
- 원래 RCS는 PC나 스마트폰이 고장났을 때 원격제어를 통해 진단하고 치료하는 용도로 주로 사용
- RCS가 심어진 스마트폰에서는 공격자에게 스마트폰 주인과 동일한 OS 접근권한 부여

• Hacking Team 회사는 35개국 97개 기관에 RCS를 판매
- 주요 고객 : 미국, 독일, 러시아, 이스라엘, 중국, 한국 등등
- 아프리카 이디오피아 등 민주주의 후진국에도 판매
- 고객의 요청에 따라 "맞춤형 주문제작 방식"

• Hacking Team의 서버에 저장된 정보가 해킹으로 유출되어 2015.7.5. 인터넷에 공개
- 약 400 Giga 분량의 정보 유출
- 국정원이 주요 고객 중 하나
  Hacking Team과 주고받은 이메일 devilangel1004@gmail.com
  주문서 등에 기재된 "Korea Army 5163" (국정원의 대외위장용 명칭)

Ⅴ. RCS 논란을 회고하며

1. RCS논란의 시작

■ 국정원의 RCS 구입 및 사용 의혹

• 국정원은 RCS 구입 사실은 인정.
다만, 대북・대테러용으로만 사용했다고 해명
- 중국 등 해외의 외국인 대상으로만 사용
- 국내에서는 연구용으로 내부적으로만 사용

• 2015년 7월 27일 국정원이 국회 정보위 보고

"대북・대테러용 10건, 국내 실험용 31건, 공작 실패 10건"

"실시간 감청은 불가능하며 서버에 자동으로 녹음되어 녹취록을 만든다"

• 그러나 국민을 대상으로 사용했다는 의혹이 계속 제기
- 이탈리아 해킹팀에 카카오톡 해킹 기능 요구 / 안랩의 백신을 피하는 방법 주문
- 삼성 갤럭시폰 신형이 출시될 때마다 '맞춤 해킹' 방법을 문의
- '미디어오늘' 기자를 사칭한 메일의 첨부 워드파일에 스파이웨어를 심어달라고 요청
- TNI 프로그램 구입 의혹
  TNI = 스파이웨어를 침투시키기 위하여 특정 공간에서 가상의 와이파이망을 설치하는 프로그램
- 스마트폰 앱 다운로드를 통해 스파이웨어를 감염시키려 했던 정황 포착

V. RCS 논란을 회고하며

1. RCS논란의 시작

2012년 국정원-해킹팀 거래 내용

2012년 1월	3월14일	7월16일	12월6일
국정원, 라이선스 10개 구입	해킹팀, 나나테크의 35개 새 라이선스(11만 유로) 주문에 답변서 송부 (나나테크가 가격 조건에 사전 동의)	국정원, (일시적인) 라이선스 10개 추가 구입	해킹팀, "30명의 타깃 추가에 따른 요금을 알려달라. 국정원이 30명 타깃 요금은 올해 예산에서 지출하고 싶어한다"

V. RCS 논란을 회고하며

1. RCS논란의 시작

■ '미디어오늘' 기자를 사칭한 메일의 첨부 워드파일에 스파이웨어를 심어달라고 요청한 사례 (천암함 침몰에 의혹을 제기한 전문가 해킹 시도?)

• 2013년 10월 7일 국정원 직원 데빌엔젤이 해킹팀 직원과 주고받은 연락 내용.
- 3일 전 해킹팀이 제작해준 '천안함 문의'(Cheonan-ham inquiry) 스파이웨어를 목표물에 발송한 뒤 기다려 보겠다는 내용, 그리고 다른 감시타겟에 보낼 '천안함 문의' 스파이웨어를 하나 더 만들어 달라는 내용

Cheonan-ham (Cheonan Ship) inquiry.docx (37 KB)

Department: Exploit requests
Staff (Owner): Bruno Muschitiello
Type: Issue
Status: In Progress
Priority: Medium
Template group: Default
Created: 02 October 2013 01:14 AM
Updated: 07 October 2013 02:18 AM

OK. I'll wait for some time for the target I've already sent the exploit.
I hope to send the exploit to one more target.
I created one more silent installer.
Give me the exploit doc document.

Thanks.

■ RCS 해킹프로그램의 작동방식과 수집가능한 정보

- RCS 해킹프로그램의 작동
  <1> 사용자의 PC나 컴퓨터에 원격조종을 가능하게 하는 스파이웨어 침투
  <2> 그것과 연결된 컴퓨터시스템을 통하여 사용자의 PC나 스마트폰을 원격조종하여 정보를 빼내감

- 수집가능한 정보
  - RCS 해킹프로그램은 컴퓨터나 스마트폰에 해당 스파이웨어를 침투시키는데 성공한다면 감시자는 컴퓨터나 스마트폰을 통해서 유통되거나 저장되어 있는 거의 모든 정보를 검색하고 수집
  - 컴퓨터나 스마트폰의 사용자가 인터넷에 접속하는 경우에 정보통신망을 통해서 이루어지는 전화통화나 메시지 송수신의 내용은 실시간으로 감시자에 전달
  - 스마트폰에 내장된 카메라를 원격조종하여 사용자 몰래 사용자의 상태나 주변상황에 관한 화상정보를 전송받을 수 있음
  - 컴퓨터나 스마트폰에 저장된 정보도 사용자 몰래 검색하고 수집
    이 과정에서 사용자가 사용하는 아이디나 비밀번호도 수집 가능

- 사용자가 데이터를 암호화하여 저장하는 경우에도,
  - 감시자는 사용자가 특정시점에 데이터를 사용하는 것과 동일한 방법으로 데이터에 접근할 수 있기 때문에
    암호화되기 전 단계에서 정보를 수집할 수 있음.

V. RCS 논란을 회고하며
2. RCS의 작동방식과 성격

■ 스파이웨어 침투 방법

- 피싱URL, 스미싱URL로 접속하도록 하는 방법
- MS 워드파일이나 파워포인트파일 등으로 위장하여 해당 파일을 다운로드할 때 스파이웨어를 설치하는 방법
- 특정 앱을 설치하도록 하여 스파이웨어가 설치되도록 하는 방법
- 무선랜인 와이파이망을 조작해 와이파이 접속시 스파이웨어가 설치되도록 하는 방법

○ 피싱이나 스미싱 방식은 특정한 대상자에게 문자나 메일을 보내는 방식이라서 대상자를 특정하여 작동하는 것인 반면에, 앱설치나 와이파이망 침입 형태의 스파이웨어 감염은 불특정 다수의 시민을 상대로 스파이웨어를 감염시킬 수 있다.

■ 감청으로 가능한 범위를 초과한 정보수집, 인격에 대한 전방위사찰

- RCS는 통화내용이나 메시지에 대해 실시간으로 내용을 확보하는 기능은 감청에 해당. 그러나 RCS를 통해 수집하는 정보는 그것에 한정되지 않는다.
  - 스마트폰의 카메라를 작동시켜 촬영한 정보의 수집
  - 사실상 컴퓨터나 스마트폰에 저장·사용되는 모든 정보의 탐지와 유출가능
  ⇒ 컴퓨터나 스마트폰 사용자의 인격에 관한 전방위적 사이버감시

- 이는 통신비밀 및 프라이버시의 자유를 침해하는 것을 훨씬 넘어서는 기본권 침해효과를 수반
  - 핸드폰이나 컴퓨터는 단순한 통화매체 또는 정보저장매체의 기능을 넘어서서 사실상 사용자의 모든 생활에 관한 정보를 담고 있다.
  - 사용자들은 카카오톡 등 메신저서비스를 통하여 다양한 정보를 주고받으며, 페이스북, 블로그 등에 자신의 생활에 관한 다양한 정보를 올리기도 한다.
  - 수많은 사진과 동영상, 일기와 같은 지극히 사적인 정보도 핸드폰이나 컴퓨터에 저장된다.
  - 그러므로 핸드폰이나 컴퓨터는 사용자의 인격과 긴밀하게 결합된 매체라는 특성을 지니고 있다.

■ 독일 연방헌법재판소의 접근 : "IT-기본권"

- BVerfG v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07.
  - 노르트라인-베스트팔렌 주의 헌법보호법률(Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) 제5조 제2항에서 헌법보호청에게 정보기술시스템에의 비밀 접근을 허용하는 규정을 도입한 것(이 규정은 2006년 12월 20일 발효)에 대한 헌법소원 사건

- 독일 연방헌법재판소는 "정보기술 시스템의 기밀성과 무결성을 보장받을 수 있는 권리(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)"라는 개념 도입
  - 사용자의 컴퓨터시스템에 스파이웨어를 설치하는 방식으로 비밀리에 사용자의 정보기술시스템에 접근하여 정보를 검색·수집하는 행위에 대해 헌법적으로 인정되는 통신비밀의 자유, 프라이버시권, 개인정보자기결정권 등의 개별적인 기본권을 언급하는 것만으로는 인격권보호에 충분하지 못하다는 문제의식
  - 개인용 PC나 스마트폰은 오늘날 그 정보기술시스템이 정보통신망으로 연결되어 사용되면서 인격권 발현에 있어서 커다란 중요성을 지닌다
  - 컴퓨터나 스마트폰의 정보에 대한 온라인수색으로 수집된 정보들이 축적되면 이는 사용자의 인격을 추론케 할 정도의 것
  - 그리고 사용자가 SNS 서비스에 접속하는 경우에 해킹프로그램에 의하여 그 관련정보를 수집하는 경우에는 수많은 대화참여자에 관한 정보를 무한정하게 수집한다는 점에서 그 기본권침해는 매우 광범위하게 확산

■ 독일 연방헌법재판소의 접근 : "IT-기본권"

- 그래서 독일 연방헌법재판소는 감시자가 네트워크 비밀접속을 통하여 사용자의 컴퓨터나 스마트폰에 저장된 정보를 수집하는 경우에는
  - 통신비밀의 보호라는 기본권으로는 충분히 보호될 수 없고
  - 또한 해킹 프로그램에 의하여 비밀리에 수집되는 정보는 프라이버시에 속하는 정보에 국한되는 것도 아니기 때문에, 프라이버시 보호라는 기본권으로도 한계가 있으며
  - 개인정보에 관한 정보적 자기결정권이라는 기본권 테제로도 인격권 침해에 대한 충분한 보호가 불가능하다고 말한다.

- 독일 연방헌법재판소의 위헌결정
  - 노르트라인-베스트팔렌 주의 헌법보호법률(Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) 제5조 제2항 제11호에 대해서는 위헌결정
  - 그러나 과잉금지 원칙에 비추어 스파이웨어 침투에 의한 해킹이 허용될 수 있는 엄격한 요건 설정
    1) 첫째, 매우 중대한 보호법익에 대한 매우 구체적인 위험이 존재하는 경우로 한정되어야 하며,
    2) 둘째, 절차적으로는 판사의 허가에 의해야 국가기관이 집행해야 하고,
    3) 셋째, 프라이버시의 핵심영역을 보호하기 위한 보호조치가 마련되어야 한다는 점을 지적

V. RCS 논란을 회고하며 3. RCS의 허용 여부에 관한 논란

■ RCS 사용은 '감청'으로 허용될 수 있는가? (독일의 논란)

- 독일에서도 과거에 해킹프로그램에 의한 온라인수색이 감청(독일형소법 제100a조) 규정에 의하여 허용될 수 있는지에 대하여 많은 논란
- 독일 연방대법원 판례(2006년)
  "해킹프로그램의 사용은 독일 형사소송법상의 감청 규정에 의하여 정당화될 수 없다"
  - 개인 사용자의 컴퓨터에 저장된 정보는 감청의 대상이 되는 전기통신의 범위를 넘어서는 것으로 감청으로 허용될 수는 없다는 것.
- 그래서 RCS와 같은 해킹툴을 이용한 온라인수색을 허용하는 법적 근거를 새로이 마련하는 입법적 추진
  - das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten(연방수사국 및 범죄수사 업무에 관한 연방과 각 주의 협력에 관한 법률)
    제20k조(정보기술시스템에 대한 비밀침입)
    해킹툴을 이용한 비밀감시의 요건 : "개인의 생명·신체나 자유에 대한 구체적인 위험을 방지하기 위한 목적 또는 공공 법익에 대한 구체적인 위험이 존재하고 그것이 국가의 존립과 기본질서 내지 인류의 존립기반을 위협하는 경우"
  - 연방과 주의 헌법보호청법률들에도 RCS해킹툴 사용을 허용하는 규정 존재

VI. 문제의 핵심은 감시와 수색의 일상화

1. 감시의 광폭성과 일상화

■ 주목해야 할 문제지대는 '수색'과 '감시'!!

• 오늘날 디지털정보의 문제지대는 단지 개인정보의 수집이라는 차원을 넘어 빅데이터 분석과 AI 및 IoT 기술의 결합을 통하여 정보수사기관의 수색과 감시권능이 점점 더 고도의 네트워킹시스템으로 구축된다는 점에 있다.

• **대량감시 + 표적감시의 체계화**

- 사실상 모든 시민에 대한 개인정보의 집적과 분석
- 빅데이터 분석을 통한 개인 프로파일링 구축
- 위험한 인물과 위험한 행동에 관한 디지털규범의 정립
- RCS 등 위험한 사람에 대한 표적 감시기술의 고도화

그러므로 우리가 앞으로 직면하게 될 현실적인 문제는 네트워크화되어 유통·수집되는 디지털정보에 관한 포괄적인 탐색을 통한 감시시스템을 어떻게 제어할 것인가의 문제

VI. 문제의 핵심은 감시와 수색의 일상화

1. 감시의 광폭성과 일상화

■ Smart City = Smart Surveillance !

• 범죄예방, 비용절감 등의 목적으로 ICT 기반 공공서비스 시스템 구축

- 시민 중심의 맞춤형 서비스 제공
  = 개인정보의 대량 집적과 분석에 기반 = 감시의 체계화, 일상화
- CCTV를 비롯한 감시센서의 전략적 배치
- 시민들의 일상생활에 관한 전면적인 정보수집을 통한 감시시스템 구축

• 국가는 단지 대량으로 개인정보 수집하는 것뿐만 아니라, 정보의 자동수집 및 네트워킹으로 대량의 정보를 집적하고 실시간 분석

- 범죄예방 / 위해방지 / 교통관리 / 에너지관리 등 모든 정부섹터에서 필요한 정보의 대량수집과 정보공유시스템 발전

• "전자 판옵티콘(electronic PanOpticon)"

- 프라이버시 침해, 익명활동의 자유란 불가능

VI. 문제의 핵심은 감시와 수색의 일상화

1. 감시의 광폭성과 일상화

■ 경찰의 감시기술의 발전

- ICT 기반 정보집적 시스템은 정보·수사기관이 다룰 수 있는 정보의 양과 정보유형의 비약적 증대 초래
  - 경찰활동의 성격 변화
    규제 중심(징벌) → 빅데이터와 실시간 감시센서 기반의 위험관리(보험)
- 선제적 경찰활동(proactive policing)
  - 상시적 감시체계를 기반으로 경찰의 예방적 선제개입 가능
  - 가부장적 국가후견주의 강화
- 예견적 경찰활동(predictive policing)
  - 빅데이터 분석을 통한 장래의 범죄위험성 예측(지역, 사람)
  - 스마트폰의 위치기반 서비스의 확대
    → 개인의 활동동선에 관한 정보의 집적과 감시
  - 잠재적 위험인물 및 잠재적 위험행동에 관한 프로파일링 구축
  - 테러위험인물, 흉악범죄 위험인물 등에 대한 집중감시 투입

VI. 문제의 핵심은 감시와 수색의 일상화

1. 감시의 광폭성과 일상화

■ 야기되는 문제 (1)

- 전통적으로 체포나 수색은 구체적인 사실에 근거한 범죄혐의 필요
  그러나 ICT 기반 경찰활동은 위험수치화에 따른 위험관리
  - 범죄혐의 VS. 빅데이터 알고리즘
  - 뉴욕시의 빅데이터 기반 불심검문 프로그램에 대해 연방법원은 인종차별적이라는 이유에서 위헌이라고 판결
    * *Floyd v. City of New York*, 959 Supp.2d 540, 562(2013)
- 대량감시 시스템
  - 개인정보 수집에 관한 자발적 동의는 무의미해지는 상황
  - 치안 등 공동서비스의 효율성 논리에 압도되는 상황

VI. 문제의 핵심은 감시와 수색의 일상화

1. 감시의 광폭성과 일상화

■ 야기되는 문제 (2)

• **프라이버시 침해**

- 개별적인 정보수집체계들이 네트워크로 통합됨으로써, 개인에 대한 프로파일링 및 표적 감시의 가능성 급증
- 빅데이터의 비실명화 처리에도 불구하고, 다른 정보들과 결합하여 개인식별정보로 재등장
- 게다가, 정보수사기관은 이미 다른 공공기관이 수집한 개인정보를 '수사상의 필요'를 근거로 하여 법원의 영장없이 수집가능

• **자율성 침해**

- 강력한 정보통합시스템과 빅데이터 알고리즘의 규범화를 통한 국가후견주의 강화
  ⇒ 이는 개인의 행동의 자율성에 대한 위축효과 수반
- 특히 예견적 경찰활동은 아무리 선의에 기초한 것이라 하더라도, 억압적 성격을 지닐 수밖에 없음.
- 거부하는 개인은 … 위험인물로 낙인

VI. 문제의 핵심은 감시와 수색의 일상화

2. 판옵티콘 사회

■ 판옵티콘 사회

• 도처에 깔린 감시의 시선들

- 경찰감시의 편재성(omnipresence)
- 감시를 거부하기란 불가능한 사회
- 감시는 더 이상 비밀스런 사찰의 문제가 아니라, 범죄예방과 질서유지 목적으로 행하는 선제적, 예견적 경찰활동의 핵심

• 현 단계에서 정보・수사기관의 주요 관심사는 관련 정보를 분류, 분석할 수 있는 시스템을 "우선 로딩"하는 것

- 지능형 통합관제시스템, 각종 경찰데이터베이스 구축 등

• 감시의 질적 변화 : **알고리즘에 의한 감시로**

- 자동화된 정보수집
  ⇒ 사회적 행동의 분류(위험 유형의 분류와 수치화)
  ⇒ 선제적 ・예견적 경찰개입

Ⅵ. 문제의 핵심은 감시와 수색의 일상화

2. 판옵티콘 사회

■ 분류에 의한 통제와 표적 감시

• **빅데이터 알고리즘의 규범화 "Minority Report"**

- 행동의 사회적 맥락의 제거 / 경직성
- feature creep에 의한 알고리즘의 왜곡과 차별의 위험
- 법집행의 책무성(accountability) 소멸 가능성

• **감시의 시선 + 감시권력의 편향적 선택**

- "usual suspect"
- 위험한 행동에 관한 social sorting과 선제적 개입 정당화

* 예) 영국의 E-CAF(Common Assessment Framework) 시스템
- 아동에 대한 데이터베이스 구축
(경찰조치, 사회복지서비스, 학교생활 등의 정보 통합)
- 이를 통해 경찰은 아동 개개인의 장래의 범죄위험성에 관한 위험측정 및 프로파일링을 만들고,
이에 기초한 국가의 사전개입조치 시행

Ⅶ. 어떻게 대응할 것인가

1. 통합관제에 관한 기존 대응의 한계

■ CCTV 통합관제센터에 관한 국가인권위원회의 제언

(2013년 정보인권보고서)

- **나약함의 극치**

○ 행정안전부와 지자체가 공동으로 추진하는 'CCTV통합관제센터' 설치 문제점 발생

- 통합관제센터의 책임주체 불분명, CCTV 설치목적의 다목적화, 지자체・경찰・군부대 간 정보 공유 기준・조건・절차 미비, 해킹・정보유출 등에 대한 방지장치 미흡 등 설치 및 운영상 문제점 발생

○ 인권단체, 개인정보전문가, 인권위원회, 관련행정기관 등이 참여하는 지자체 CCTV 통합관제센터 설치・운영협의체 구성・운영으로 인권침해요소 최소화

- 지자체 CCTV 통합관제센터 설치・운영 목적 구체화
- 개인영상정보 공유 최소화 및 공유・제공 요건・절차 마련
- 개별 CCTV별로 운영결과를 매년 투명하게 지역주민과 언론에 공개
- 설치・운영 목표의 설정, 관리・운영지침 제정・운영 등에 있어서 지역주민・인권단체・지역전문가등의 참여 보장

Ⅶ. 어떻게 대응할 것인가

1. 통합관제에 관한 기존 대응의 한계

■ 개인영상정보보호법에 대한 비판적 대응

- 개인정보보호위원회, 행정자치부에 `개인영상정보보호법` 제정 보류를 권고
  - 개인영상정보 보호원칙, 안전성 확보 조치 등 일부 조항이 기존 개인정보보호법과 유사하거나 중복
  - 영상정보 수집·이용에 관한 일부 조항이 개인정보보호법 위반
  - 개인영상정보 삭제, 영상정보처리기기 설치·운영 등에 관한 일부 조항을 수정·보완해 개인정보보호법에 편입시키는 것이 바람직함.

- 진보넷 등 시민사회단체, 개인영상정보보호법 제정에 반대 입장 표명
  - 개인영상정보보호법 제정의 핵심은 CCTV 통합관제센터 설치의 법적 근거를 마련하는 것인데, 이는 전방위적 감시의 일상화 우려
  - CCTV의 임의조작 가능성을 폭넓게 인정
  - 개인영상정보의 제3자 제공 요건을 현행 개인정보보호법보다 완화

- 이것은 **아주 작은 저항**에 불과할 것!

Ⅶ. 어떻게 대응할 것인가

2. 민주주의적 접근 필요

■ 개인정보보호법에 의한 규제는 근본적인 한계에 봉착

- 이미 국가기관의 정보수집과 분석을 위하여 개인정보수집의 동의 요건에 대한 예외 및 제3자 제공을 폭넓게 인정
- 게다가, CCTV 및 정보공유네트워킹의 증대는 정보주체들의 동의라는 요건을 무색하게 만드는 상황에 직면
- 지능형 전자정부라는 정책방향 속에서 개인정보 수집체계는 더욱 고도화될 것이며, "효율성 테제"에 의하여 정보공유와 처리에 관한 예외를 허용하는 법적 근거를 만드는 것은 그리 어렵지 않은 일이 될 것

■ 민주주의와 인권적 접근
- 개별적 기술수단에 관한 사회적 민주적 통제의 과정 필요

- 개인정보 수집 및 처리의 자동화 금지 및 프로파일링의 금지
- 빅데이터 알고리즘에 관한 투명한 사회적 합의 과정 필요
- 프라이버시는 안전을 위한 희생물이 아니라, 국가가 지켜야 할 '안전(Safety)'의 최우선 과제라는 사회적 인식 확산
- 선제적 감시기술의 허용 여부에 관한 엄밀한 검증 및 사회적 투명성 보장, 그리고 감시대상자의 법적 불복 수단의 마련

메모

메모

메모

메모