빅브라더와 리틀시스터의 감시탑

이 창 무

"나의 단 하나의 목적은 사람들에게
그들의 이름으로, 그리고 그들의
이름에 반해 어떤 일이 벌어졌는지
알리는 것이다. 만약 당신의
이메일, 당신 부인의 전화 내역을
보고 싶다면 나는 이 시스템을
이용하기만 하면 된다.
나는 당신의 이메일, 비밀번호, 통화
기록, 신용카드까지 알 수 있다.
나는 이런 일이 일어나는
사회에 살고 싶지 않다."

전 NSA 직원 에드워드 스노든이 비밀정보수집 프로그램
'프리즘'의 존재를 세상에 알리며.

동서고금을 막론하고 모든 사회는 범죄를 예방하고 통제하여 시민들이 안전하게 살 수 있는 사회를 만들고자 합니다. 범죄를 줄이기 위한 노력은 언제나 있었습니다만 그 방식은 과거와 현재가 다릅니다. 범죄예방의 핵심에는 처벌과 감시가 있는데, 과거에는 주로 처벌을 통한 경각심 고취에 초점을 맞췄습니다. 즉 범죄자를 처벌하는 모습을 만인에게 보여줌으로써 경종을 울리는 것입니다. 현대에는 감시로 초점이 옮겨졌습니다. 범법행위를 하지 못하도록 곳곳에 감시의 눈을 심어놓는 것입니다. 범죄가 일어나면 그 눈의 기록을 통해 범죄자를 찾아내지요. 범죄와 보안을 위해 우리는 어떤 일들을 해왔는지 과거로 거슬러 올라가보겠습니다.

능지처참의 시대에서 빅브라더의 시대로

미셸 푸코로부터 시작을 해보죠. 미셸 푸코(Michel Foucault)에 대해 잘 아시는 분도 있을 테고 태어나서 처음 들으신 분들도 있을 것 같습니다. 미셸 푸코는 생김새부터 범상치 않은 인물이었습니다. 어떻게 보면 악당같이 느껴질 정도죠. 하지만 사실 제가 학자로서 범접할 수 없는 경지를 느끼게 해준 학자입니다. 그는 천재가 아닐까 싶습니다. 미셸 푸코는《광기의 역사》,《성의 역사》와 같은 책들을 썼는데, 여기서 소개해드릴 책은《감시와 처벌》입니다. 이 책은 말 그대로 감시와 처벌에 관한 책이고, 범죄와 사회, 그리고 권력을 이해하는 데 필독서라고 할 수 있습니다. 초반 50쪽까지만 읽어도 독서의 목적을 달성할 수 있는 상당히 좋은 책입니다. 무엇보다도 이 책은 아주 끔찍한 장면으로 시작합니다.

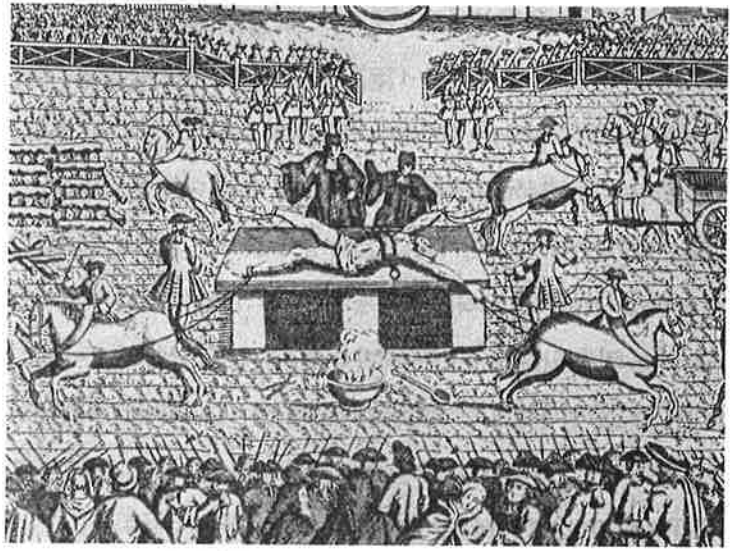
"손에 2파운드 무게의 뜨거운 밀랍으로 만든 횃불을 들고, 속옷 차림으로 노트르담 대성당의 정문 앞에 사형수 호송차로 실려 와, 공개적으로 사죄할 것 (중략) 상기한 호송차로 그레브 광장에 옮겨진 다음, 그곳에 설치될 처형대 위에서 가슴, 팔, 넓적다리, 장딴지를 뜨겁게 달군 쇠집게로 고문을 가하고, 그 오른손은 국왕을 살해하려 했을 때의 단도를 잡게 한 채, 유황불로 태워야 한다. 계속해서 쇠집게로 지진 곳에 불로 녹인 납, 펄펄 끓는 기름, 지글지글 끓는 송진, 밀랍과 유황의 용해물을 붓고, 몸은 네 마리의 말이 잡아끌어 사지를 절단하

게 한 뒤, 손발과 몸은 불태워 없애고 그 재는 바람에 날려버린다."

매우 끔찍하죠? 위의 글은 1757년에 루이 15세를 암살하려다가 실패한 로베르 프랑수아 다미엥을 어떻게 처형했는지 묘사한 것입니다. 우리나라와 중국은 근대 이전에 반역을 꾀한 대역죄인에게 능지형을 내렸습니다. 능지형이란 가능한 한 오랫동안 천천히 범죄자의 살점을 한 점, 한 점 도려내는 형벌이었습니다. 능지형 외에도 거열형이라는 것이 있었습니다.《감시와 처벌》에서 "네 마리의 말이 잡아끌어 사지를 절단하게 한 뒤"라는 부분이 있지요? 이것이 거열형입니다. 목과 팔다리를 밧줄로 묶고 다섯 마리의 말이나 소의 힘으로 각기 다른 방향으로 잡아당기는 것이죠.

푸코가《감시와 처벌》에서 제일 먼저 거열형을 소개한 이유가 뭘까요? 그건 처벌의 패러다임이 바뀌었다는 사실을 극적으로 보여주기 위해서라고 생각합니다. 그 이전에는 중범죄일수록 대중 앞에서 심하게 고문하고 고통스럽게 죽였죠. 유럽에서는 사형집행도 아무 때나 하지 않았습니다. 목요일 오후로 정해졌지요. 바로 그 시간이 사람이 가장 많이 모이기 때문입니다. 감히 국왕에게 역심을 품었다가는 어떤 일을 당하는지 많은 이들에게 알려주기 위함입니다.

하지만 어느 순간부터인가 권력자들은 사형 광경을 대중에게서 숨기게 되었습니다. 푸코는 이 의미심장한 변화에 주목했던 것이죠. 광장에서 수천 명의 대중이 보는 가운데 범죄자를 끔찍하게 죽이는 것은 '다수가 소수를 보던 사회'입니다. 그런데 권력을 쥔 사람들이 어



✖ 과거 최고의 형벌은 거열형과 능지형이었다. 죄수의 몸이 빠지거나 찢겨 나갈 때마다 구경꾼들에게는 범죄에 대한 경고가 각인되었을 것이다. 하지만 이제 처벌은 광장이 아니라 폐쇄 공간인 교도소에서 이루어진다. 원인은 대중에 대한 권력자들의 불안감 때문이었다.

느 순간엔가 불안감을 느끼게 되지요. 처형장에 모여서 국왕 암살범을 비난하다가 그 화살이 국왕에게 향할 수 있기 때문입니다. 프랑스 혁명도 국민들의 불만이 누적되다가 결국 터져 나온 것이죠. 국왕 자신이 단두대에 서는 결과마저 초래했죠. 이런 과정에서 사회는 '소수가 다수를 감시하는 사회'로 변했습니다. 예전에는 몸을 처벌했다면 지금은 일상을 지켜봅니다.

오늘날 처벌은 인도주의란 미명 아래 몸에서 정신으로 그 대상이 바뀌었습니다. 푸코가 주목하는 부분입니다. 현대 사회가 감시 사회로 바뀌었다는 것이죠. 푸코가 이 책을 쓴 지는 40년이 더 됐지만 지금 상당 부분이 푸코가 주장하는 비슷한 방식으로 바뀌고 있죠. 물론 아직도 이런 방식이 남아 있습니다. ISIL(이라크 레반트 이슬람 국가, 통칭 IS)이나 북한에서는 아직도 공개처형을 하죠. 하지만 세상은 푸코가 주장하는 것처럼 크게 바뀌었습니다. 소수가 다수를 감시하는 사회로 바뀐 것이죠. 이런 입장을 나타내는 용어로 파놉티콘(Panopticon)이란 말이 있습니다. 여기서 'pan'이라는 것은 모든 것을 뜻합니다. 그리고 'opticon'은 본다는 의미죠. 즉 파놉티콘이란 모든 것을 다 본다는 뜻입니다. 현미경과 망원경을 섞어놓은 상상의 기계입니다. 누가 이걸 주장했냐 하면 바로 제러미 벤담입니다. 최대 다수의 최대 행복이라는 이론을 주장한 사람입니다. 벤담은 파놉티콘의 원리를 이용해 소수가 쉽게 수용자들을 감시할 수 있는 감옥 설계도를 만들었습니다. 특허를 내서 돈도 많이 벌 생각이었습니다. 당시에는 안타

깝게도 그 설계도를 사겠다는 곳이 별로 없었죠. 그렇지만 현대 거의 모든 나라의 감옥은 벤담의 감옥 설계도처럼 생겼습니다. 소수가 다수를 감시하는 구조입니다.

옛날 감옥은 던전(dungeon)이라고 부르는, 감시가 용이하지 않은 구조로 되어 있었습니다. 하지만 요즘에는 몇 명이 수천 명을 감시할 수 있는 모습으로 바뀌었습니다. '모든 것을 보는 눈(All Seeing Eye of God)'이라는, 소설《다빈치 코드》에 나오는 눈이 있습니다. 프리메이슨이라는 비밀결사조직의 표식에서도 나옵니다. 이 표식의 눈은 이른바 승리의 눈입니다. 이 눈은 미국의 1달러 뒷면에도 이미지가 표시돼 있습니다. 여기에는 숱한 음모론도 끼어듭니다. 오바마가 프리메이슨이다, 등등의 여러 가지 이야기들이 있습니다. 뭐가 되었건 근대 이후 사회가 감시하는 체제로 바뀌게 되었다는 겁니다.

지금 시대의 '모든 것을 보는 눈'은 소셜 필터링입니다. 기업의 신입 사원 모집에 지원했다고 가정해봅시다. 이때 인사팀은 단순하게 지원 서류만 심사하는 것이 아니라 지원자의 SNS 활동을 쭉 모니터링하게 됩니다. 이 사람들이 과거에 어떤 기록을 남겼는지 점검하는 거죠. 이를테면 어떤 사람이 대기업 신입사원 모집에 지원을 합니다. 그런데 이 사람이 SNS를 통해 예전에 이 대기업 욕을 많이 했습니다. 그런데 막상 면접에서는 "뽑아만 주신다면 죽도록 열심히 하겠습니다"라고 하게 마련입니다. 이러면 떨어질 가능성이 높아진다는 거죠. 앞으로 취업준비를 위해서도 특히 SNS는 조심해서 활용해야 합니다.

욕 같은 것을 아무렇게나 적으면 훗날 발목이 잡힐 수 있습니다.

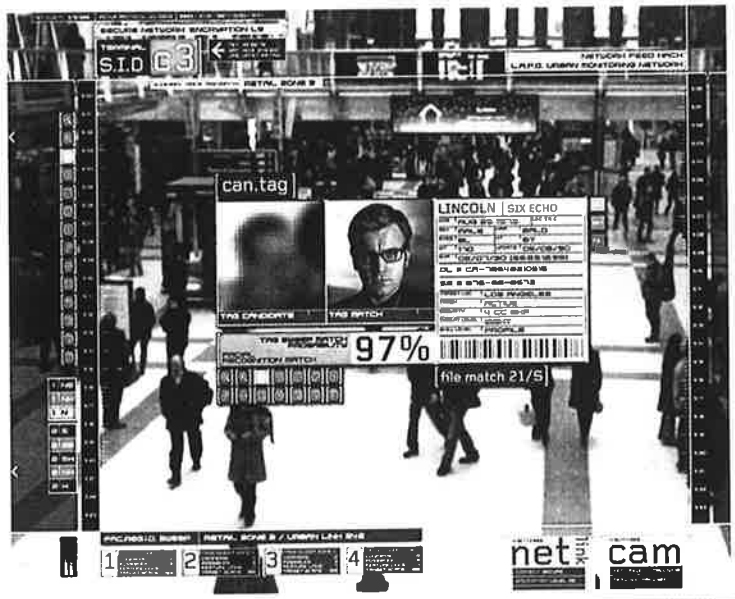
빅브라더가 당신을 감시하는 미래

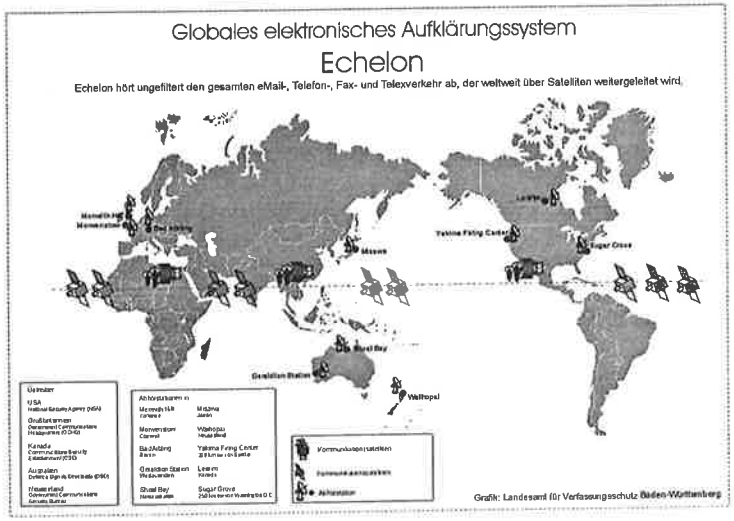
지금은 감시 사회입니다. 감시는 사람이 아니라 기계들이 합니다. 최근 정보보안이란 단어를 많이 들어보셨을 겁니다. 해킹 보안도 많이 이야기가 나오지만 외부에서 안으로 침투해서 들어오는 경우보다는 내부에서 바깥으로 빠져나가는 경우가 더 많습니다. 그래서 방화벽과 같은 프로그램을 이용해 외부에서 오는 걸 막기도 하지만 내부에서 바깥으로 데이터를 빼 가는 것을 막는 프로그램도 많습니다. DLP, ERM 등의 프로그램들이 안에서 바깥으로 빼내지 못하게 모니터링하는 것입니다. 그런데 회사에서는 사원들이 쓰는 메신저, 이메일 등도 정보보안이라는 명복으로 실시간 모니터링을 하고 있습니다. 정보사회의 어두운 면들이 되겠지요.

'빅브라더'라는 유명한 용어가 있습니다. 조지 오웰의《1984》에 나오는 것이죠. "Big brother is watching you." 빅브라더가 항상 지켜보고 있다는 뜻입니다. 뒤에서 자세히 다루겠지만, 위키리크스 등이 나오고 난 다음에 미국 국가정보국(NSA)의 도청 사실을 폭로한 에드워드 스노든이 낸 책이《더 이상 숨을 곳이 없다》입니다. 2015년 6월에 코엑스에서 IT보안과 관련한 전시회가 열렸습니다. 전시된 여

러 첨단장비 가운데 IOT(Internet of things) 관련 기술장비들이 있었습니다. IOT는 우리말로 사물인터넷이라고 하며 기기에 부착돼 있는 센서를 통해 기기가 서로 연결이 되는 것이 특징입니다. 또한 편리성을 증진시키는 데 목적이 있습니다. 그러나 각종 첨단기술 장비는 앞의 '모든 것을 보는 눈'이라는 말처럼 모든 것을 다 보는 눈이 되고 있습니다. 이런 사실을 폭로한 사람이 바로 에드워드 스노든입니다. 그는 미국의 CIA에서 일하던 사람입니다. 스노든은 미국의 NSA란 정보기관에서 프리즘이란 걸 통해 구글, 트위터, 페이스북 등등의 모든 것을 모니터링한다는 사실을 폭로했습니다.

이른바 에셜론이라는 프로젝트는 인공위성 등을 통해서 전 세계를 작은 목소리까지도 수집하는 시스템입니다. 첩보위성을 통해서 전화나 팩스, 이메일을 모니터링을 하는 건데요, 이런 걸 '파이브 아이스(Five Eyes)'라고 합니다. 다섯 개의 눈은 여기에 속해 있는 미국, 영국, 캐나다, 호주, 뉴질랜드를 뜻합니다. 이 다섯 개 나라 사이에는 공통점이 있습니다. 영어를 쓰는 앵글로색슨족이며 미국을 제외하면 과거 영연방국가들입니다. 이런 것들을 가지고 만든 영화가 바로 〈본 얼티메이텀〉입니다. 영화를 보신 독자는 잘 아시겠지만 주인공 제이슨 본을 포함해 런던이나 세계 곳곳을 CCTV로 감시합니다. 얼굴 인식 프로그램으로 자기들이 찾는 사람을 순간순간 확인할 수 있습니다. 물론 영화에 나오는 이야기인데 이것의 모티브는 에셜론 프로젝트입니다. 세계 곳곳을 감시하는 장치죠.





1 영화 〈본 얼티메이텀〉에 등장하는 NSA의 전 세계 도청망.
2 영화 〈본 얼티메이텀〉 속 전 세계 감청망의 모티브가 된 에셜론 프로젝트.

우리나라도 최근 몇 년 사이에 각종 개인정보를 비롯한 정보 침해 사건들이 많이 터져 나오고 있습니다. 2014년 1월에는 국민카드, 농협, 롯데카드 등에서 1억 개 이상의 개인정보가 단 한 번에 유출이 되었습니다. 그런데 유출 방법이 터무니없었습니다. 일반적으로 신용카드 회사는 부정사용을 막기 위해 컴퓨터 프로그램을 개발해 설치합니다. FDS(Fraud Detection System)라고 부르는 부정행위 적발 프로그램입니다. 이 프로그램은 자동으로 부정사용을 실시간으로 적발하는 기능을 수행합니다. 이를테면 신용카드로 하루 사이에 냉장고를 두 개 샀다는 정보가 들어옵니다. 그럼 정상적이지 않죠? 하루에 냉장고 두 개를 사는 일은 거의 없습니다. 그래서 신용카드를 가진 사람에게 전화를 해서 신용카드 사용 내역을 확인합니다. 이처럼 정상 패턴을 벗어나는 것이 있으면 확인을 하는 것입니다. 다른 예를 들자면, 신용카드를 부산에서 쓰고 한 시간 후에 서울에서 또 사용했다는 정보가 들어옵니다. 당연히 정상적인 경우가 아니기 때문에 적발을 합니다. 그런데 이 프로그램을 신용카드 회사가 직접 만든 것이 아니라 외주용역을 줬습니다. 당연히 용역회사에 고객들의 정보를 줘야겠죠? 이 과정에서 자동적발 프로그램 개발을 맡은 외주 용역회사의 직원이 고객 정보를 다른 곳에 팔아넘겼습니다. 고양이에게 생선을 맡긴 꼴입니다. 우리나라는 만 17세 이상 국민은 누구나 주민등록을 하죠. 우리나라 모든 국민 주민등록번호는 중국에서 찾을 수 있다는 이야기가 있습니다. 하도 많이 공개가 되어 있기 때문입니다.

당신의 하루가 낱낱이 기록되고 있다

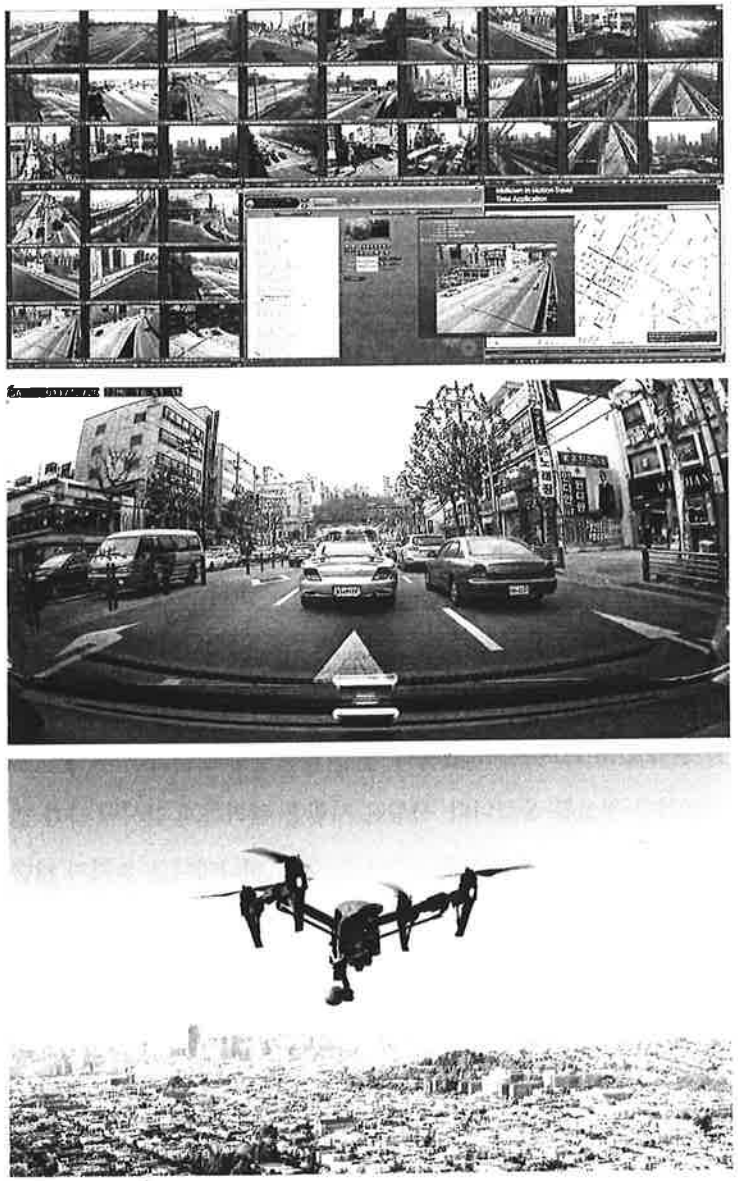
스파이라고 하면 영화 〈킹스맨〉이나 〈미션 임파서블〉처럼 첨단장비와 초인에 가까운 능력을 가진 사람을 떠올립니다. 하지만 전형적인 스파이는 평범한 사람이 대부분입니다. 기밀을 빼돌릴 때 첨단장비가 쓰이는 경우도 드뭅니다. 보통은 매우 평범한 방법으로 정보를 빼돌리죠. 정보 유출이 흔하다 보니 이 글을 읽고 계신 분들도 이미 각종 개인정보가 상당수 털린 상태라고 볼 수 있습니다. 인터넷 커뮤니티나 인터넷 쇼핑몰, 금융 산업계에서 저장된 고객의 이름, 성별, 주소, 전화번호와 더불어 쇼핑 습관이나 최근 온라인 쇼핑몰 구매목록까지 수많은 정보들이 본인도 모르는 사이에 상당수 유출됐다고 봐야 할 것입니다.

최근 기술이 발달하면서 개인 사생활 침해가 더욱 심각해지고 있습니다. 주된 요인은 급증하고 있는 CCTV입니다. CCTV의 화질이 낮고 식별이 어려운 것은 옛날 이야기입니다. 요즘 CCTV는 해상도가 Full HD급입니다. 적외선을 이용해 밤에도 사람을 식별할 수 있는 장치도 있습니다. 세계에서 CCTV가 가장 많은 국가는 어디일까요? 흔히 영국이라고 이야기합니다. 영국의 CCTV 수가 얼마인지는 아무도 모릅니다. 공공장소 외에도 기업이나 개인이 설치한 것도 많기 때문입니다. 다만 최소한 500만 개 이상일 것이라고 추정합니다. 재미있는 것은 소설《1984》에서 미래의 정보권력인 빅브라더를 예

견한 조지 오웰의 생가도 반경 180m 내에 설치된 32개의 CCTV로부터 감시를 받고 있다는 것입니다.

블랙박스 역시 CCTV 못지않게 문제가 될 수 있습니다. 집에서 직장 혹은 학교에 갔다가 다시 집으로 돌아오기까지, 하루 이동경로를 생각해봅시다. 거의 모든 주차장, 대로, 버스 정류장, 고속도로 등 차가 있는 곳이라면 어디든지 블랙박스가 있습니다. 우리의 이동경로가 모자이크처럼 이 차, 저 차의 블랙박스 메모리카드에 저장되고 있는 것이죠.

우리 일상에 대한 감시는 땅을 벗어나 이제 하늘로 진출했습니다. 바로 드론 때문입니다. 실제로 드론을 제조하는 기업들은 주변을 감시할 수 있고 도둑을 막을 수 있다고 광고를 하고 있습니다. 앞으로 드론은 매우 많아질 것입니다. 쓰임새가 점점 다방면으로 확산되고 있기 때문입니다. 미국 최대의 온라인 쇼핑몰 아마존닷컴은 이미 상품을 드론으로 배달하고 있습니다. 영국의 도미노피자는 드론으로 피자 세 판을 배달하는 영상을 공개했습니다. 경비원 역할을 앞으로는 드론이 할 것이라는 전망도 있습니다. 배터리만 충분하다면 드론은 경비구역을 언제나 감시하고 통제할 수 있기 때문입니다. 또한 카메라 성능도 100m 거리에서 동전을 감지하고 식별할 수 있을 정도로 뛰어납니다. 이제 우리는 지하철에서도, 마트 주차장에서도, 15층 건물 옥상에서도 언제나 감시를 당하고 있습니다. 기계와 문명을 뒤로하고 산으로 들어가도 감시는 계속됩니다. 스파이 인공위성이 지



✖ 당신이 누구든지, 어디에서 뭘 하든지, 언제나 감시당하고 있다는 사실을 잊지 말아야 한다. 누군가는 지금도 당신을 지켜보고 있다.

공공기관 CCTV 설치 현황(2013년말)		택시내 영상기록장치(블랙박스) 설치현황(2012년)			
구분	설치대수	구분	택시 대수	설치대수	
				외부	내부
범죄예방	260,098				
시설관리 및 화재예방	278,002				
교통단속	10,512	개인	163,623	125,709	10,744
교통단속교통정보수집·분석·제공	17,111				
합계	565,723	일반	85,503	84,081	8,108

자료: e-나라지표, 국토해양부

구를 돌며 사진을 찍고 있기 때문이죠.

다시 CCTV 이야기로 돌아가보겠습니다. 우리 일상을 감시하는 도구는 여러 가지가 있지만 그중에서 CCTV만큼 효율적이고 비약적으로 발전을 거듭하며 큰 위협이 되는 것도 없습니다. 동작 감시형 CCTV는 특정 공간에 가상의 선을 그어놓고 감시하는 지능형 CCTV입니다. 만약 그 특정 공간에서 누군가가 선을 넘어 금지된 구역에 침범하면 경보를 울립니다. 사람은 사람을 완벽하게 감시할 수가 없습니다. 하지만 이런 지능형 CCTV는 동작 하나하나를 놓치지 않습니다. 엉겁결에 CCTV가 그어놓은 안 보이는 선을 1cm라도 넘는 순간 경보가 울리고 곧 보안요원들이 들이닥칠 겁니다. 선을 넘지 않았다고 변명해봤자 소용이 없습니다. 동작을 감지하고 경보를 울리는 순간 CCTV는 모든 것을 기록으로 남깁니다.

영국에 설치된 CCTV 중에는 사람의 걸음걸이를 감시하는 것도

있습니다. 밤길을 걷고 있는데 뒤에서 누가 쫓아오면 무섭잖아요? 그런 일을 방지하기 위해서 앞서가는 사람과 뒤에 가는 사람 사이의 거리가 평균보다 갑자기 짧아지면 경보가 울립니다. 움직임을 감지해서 나중에 필요한 부분만 볼 수 있는 CCTV도 있습니다. 국내의 한 보안업체에서 최근에 개발했습니다. 예를 들어 공장에서 유해한 화학물질을 다룰 경우 반드시 방독면을 착용하도록 합니다. 하지만 때때로 불편하다고 안 쓰는 직원이 있을 수 있습니다. 이런 경우를 적발하는 CCTV입니다. 먼저 감시 대상이 직원인지 확인하고, 방독면을 썼는지 확인하고, 규정을 위반했을 경우에 이름을 식별하여 경고를 보냅니다. 외부자가 기업 내부에 들어올 수도 있겠죠? 방문자 유니폼을 입지 않았거나 출입카드가 없는 외부자가 보이면 곧바로 경보를 울립니다. 달리면 안 되는 곳에서는 사람들의 이동 속도를 계산하고 있다가 일반적인 도보 속도를 초과했다고 판단되면 경보를 울립니다. 이런 지능형 CCTV는 이미 우리 일상으로 파고들고 있습니다.

빅 데이터와 강철 울타리

미국 뉴욕 경시청은 마이크로소프트와 함께 실시간 범죄 감시 통합시스템(DAS)이라는 것을 개발했습니다. DAS의 원리는

감시와 빅 데이터입니다. 3000개 이상의 CCTV를 비롯해 신고전화, 용의자 체포기록, 자동차 번호판 추적 등의 방대한 데이터를 수집하고 분석하여 범죄를 예측하고 범죄자를 검거하는 것입니다. 예를 들어 용의자의 차량번호를 입력하면 뉴욕 전체의 차량번호를 검색해서 찾아냅니다. 차량번호가 1234일 경우 이를 검색하면 그 차량의 위치를 찾아서 계속 따라가면서 감시합니다. 비단 차량번호만이 아닙니다. 만약 제 얼굴을 테러 범죄자 데이터로 입력하면 제가 어디에 가든지 검색되고 실시간으로 추적됩니다. 범죄자를 쉽게 찾고 범죄율를 낮추기 위한 혁신적인 시스템으로 소개했지만, 이 시스템은 사실 많은 우려가 있습니다. 용의자라는 이유만으로 24시간 동안 도시 전역에서 행동 하나하나를 감시당해야 하니까요. 하지만 현재 미국에서는 테러 방지가 개인의 권리와 자유에 우선하고 있습니다.

첨단 감시 시스템은 우리나라도 예외가 아닙니다. 현재 한국 마이크로소프트와 LG CNS가 협력하여 한국의 DAS를 만들고 있습니다. 이 시스템은 뉴욕 DAS의 장점을 취하고 SNS 정보까지 수집하고 분석할지도 모릅니다. SNS에서 실시간으로 등록되는 글과 사진은 움직이는 CCTV와 같기 때문에 기존 DAS의 감시 기능을 강화해줄 것으로 예상합니다. 반면에 그만큼 개인의 사생활 침해와 인권 침해가 걱정되는 시스템이기도 합니다.

바이퍼(Viper) CCTV는 줌인을 할 수 있는 기구입니다. 뉴욕의 주변에는 CCTV가 울타리처럼 놓아져 있어서 강철 고리(ring of steel)라고

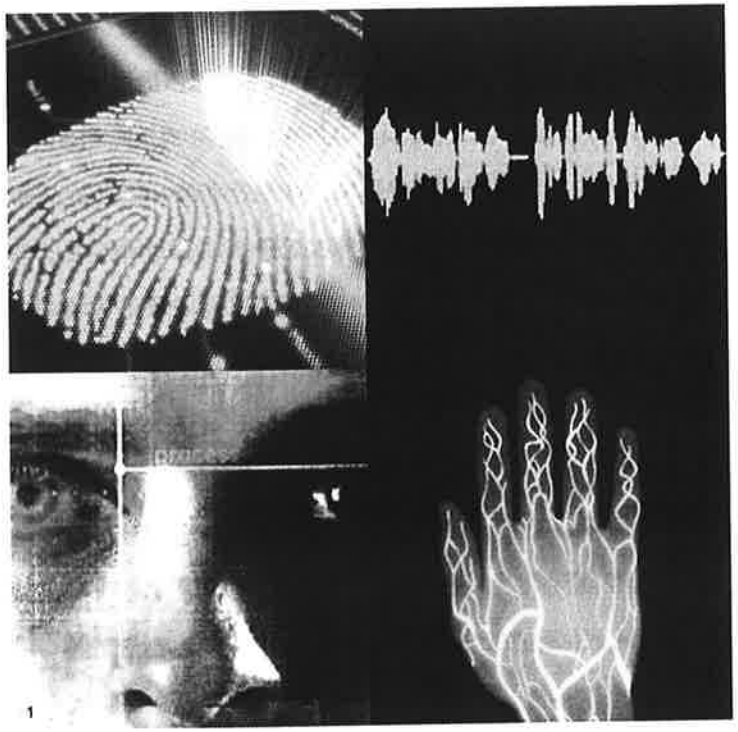
부르기도 합니다. 이런 것들을 우리는 흔히 유비쿼터스라고 부르죠. 언제 어디서나 감시가 행해지는 시스템입니다. 우리나라에도 강철 고리가 이미 존재합니다. 예를 들어서 자녀가 학원에 가면 학부모에게 연락이 갑니다. 만약 중간에 학원에서 나가면 그것도 학부모에게 연락이 갑니다. 학생을 관리하는 시스템이라고 하지만 학생들 입장에서는 갑갑합니다.

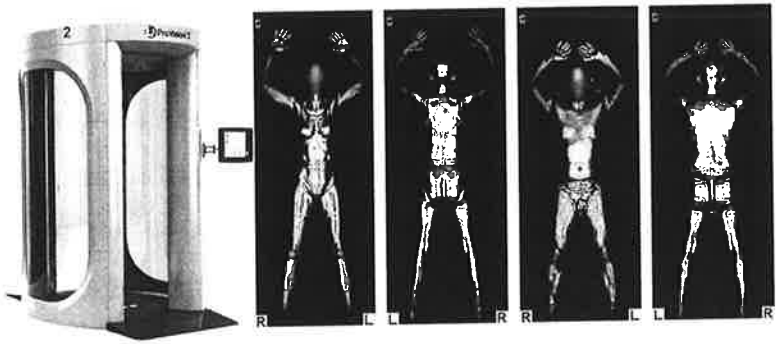
이런 시스템을 조금 더 건설적인 방법으로 활용할 수 없을까요? 저는 이런 시스템을 보고 아동 실종이나 유기견과 같은 문제를 떠올렸습니다. 가방이나 모자는 버릴 수 있어도 신발은 항상 신고 다니잖아요? 그래서 신발에 위치 추적 장치를 설치하는 시스템을 개발해 특허를 내려고 했는데 아쉽게도 벌써 개발되어 특허 등록이 되어 있더군요. 방금 말한 것들이 유비쿼터스를 활용한 시스템입니다. 주차장에서 차량번호를 인식해서 차단기를 올립니다. 등록된 차가 아파트에 들어오면 모니터에 통지해주죠. 심장박동을 항상 체크해서 갑자기 불규칙해질 경우 병원에 알려주는 시스템들도 있습니다. 학원이나 백화점 주변에 가면 광고들이 나오는 것도 무선 주파수 인증 기술(RFID, Radio-Frequency Identification)의 유비쿼터스를 이용한 것입니다. 우리가 어디에 있든, 어디로 가든 곳곳에 기록이 남기 때문에 빠져나올 수가 없습니다.

핸드폰 GPS를 켜놓고 있으면 어떻게 됩니까? 하루 종일 돌아다닌 행적이 다 기록이 됩니다. SF소설 속의 이야기가 아닙니다. 모두 가

능한 기술이며 지금도 쓰이고 있습니다. 예를 들어서 버스 도착 시간을 알려주는 어플리케이션도 이러한 유비쿼터스 센서 네트워크(USN, Ubiquitous Sensor Network)를 활용한 기술입니다. 버스정류장에 가면 몇 분 후에 버스가 온다고 나타나죠? 앞 버스와의 간격을 중앙 컨트롤 센터에서 모니터링하고 관제를 할 수 있는 것입니다. 버스의 실시간 이동 경로와 도로 정체 상황, 신호등 시간 등을 계산해서 지금은 초 단위로 버스 도착 시간을 알려줍니다. 대형 마트에서도 상품을 계산하지 않고 나오면 경고음이 울립니다. 이것도 RFID를 활용한 보안 장치입니다. 예전에는 물품이 섞이거나 재고 물품을 찾기가 힘들었는데 이제는 기록이 남기 때문에 관리가 한층 수월합니다. 도서관과 책에도 이 기술이 적용됩니다. 꼭 봐야 하는 책이 도서관에 한 권밖에 없고 대출도 안 됩니다. 서가에 가도 없습니다. 누군가가 혼자 보려고 숨겨놓았을 수 있습니다. RFID는 이렇게 책이 숨겨져 있다 해도 사서가 쉽게 찾을 수 있도록 돕기도 합니다.

USN과 관련된 부품을 사람의 피부 안쪽에 이식하는 기술도 있습니다. 섬뜩한 이야기입니다. 전자발찌를 찬 성범죄자 가운데 발찌를 떼어버리고 도주하는 경우가 발생하니까 아예 피부 속에 심는 경우도 있습니다. 심지어 부모가 자녀를 잃어버리지 않으려고 칩을 넣기도 합니다. 놀이동산 같은 곳에서 아이를 잃어버려도 금방 찾을 수 있도록 말입니다. 최근에는 바이오인식기술로 불리는 생체정보 인식 기술도 점점 진화하는 분야 가운데 하나입니다. 이미 휴대폰에도 지





1 한때 값비싼 보안 시스템이었던 생체인식은 현재 핵무기 발사 버튼부터 아파트 현관문까지 본인 확인이 필요한 수단에 적극 활용되고 있다.

2 미국은 9.11테러를 겪은 후 L3 provision2와 같은 전신 스캐너를 각 공항에 설치했다. 우리나라도 주요 공항에 설치했으며 개인의 프라이버시보다는 집단의 안보를 중요시하는 현대 보안의 시각을 잘 나타낸다.

문 인식 기술이 적용되었습니다. 지문은 실리콘으로 복제할 수 있으니 얼굴 인식, 홍채 인식, 정맥 인식, 성대 인식, 걸음걸이 인식 등 본인 확인 기술이 발달하고 있습니다. 나아가 하나의 정보에 의존하지 않고 여러 정보를 종합해 판단하는 기술이 보안에 쓰이고 있습니다.

미국은 9.11테러 이후 테러 방지와 보안을 위해 공항에 전신 스캐너를 설치했습니다. 전신 스캐너는 우리나라에도 공항 등에 설치되어 있습니다. 대표적으로 백스케터(backscatter)라는 제품이 있습니다. 저는 미국에서 전신 스캐너를 통과해봤는데 기분이 썩 좋지 않았습니다. 전신 스캐너의 장점은 테러범들이 금속탐지기에 걸리지 않도록 플라스틱으로 만든 무기까지 찾아낼 수 있다는 겁니다. 실제로 전신 스캐너를 통과하면 사람의 완전한 알몸이 투시됩니다. 그래서 지금은 실제 사람 모습이 아닌 사람 모형 모습에 금지된 물품이 적발되면 색깔로 표시되는 것으로 바뀌었습니다. 개인의 프라이버시권(right of privacy)을 보장하기 위함입니다.

마이너리티 리포트가 실현되는 미래

프리 크라임(Pre-Crime)이라는 말을 들어보셨나요? 프리 크라임이란 범죄가 발생하기 전에 범죄 장소, 방식, 피해자, 범죄자 정보를 예측하여 범죄를 예방하고 범죄자를 체포하는 시스템을 말합니다. 영화 〈마이너리티 리포트〉처럼 말이죠.

실제로 미국 중앙정보국(CIA)과 구글은 인터넷 정보를 실시간으로 분석하여 미래의 일들을 예측하는 리코디드 퓨처스(Recorded Futures)라는 기업을 지원하여 프리 크라임 시스템을 개발하고 있습니다. 미국 산타클라라 대학은 범죄 예측 서비스인 프레드폴(predpol)을 개발했습니다. 프레드폴이란 예를 들어 미리 범죄가 발생할 지역을 집중적으로 순찰하고 수사를 하는 것입니다. 미국과 영국이 도입했으며 특히 영국의 켄트 주는 프레드폴을 적극 활용하여 범죄발생률을 연간 14만 건에서 10만 건으로 약 30% 줄이는 효과를 봤다고 합니다.

미국 로스앤젤레스 경찰청은 빅 데이터를 기반으로 지리 정보를 분석하여 범죄를 예측하는 프로그램을 활용하고 있습니다. 제가 관심을 가졌던 프로그램 가운데 스타라이트 프로그램(Starlight program)이라는 것이 있습니다. 인물의 이동경로와 인적 네트워크를 통해서 테러 용의자 등을 찾고 현재 위치를 예측하는 프로그램입니다.

비단 범죄자뿐만 아니라 우리의 일상도 언제나 감시받고 분석되고 있습니다. 예를 들어 핀테크(Fintech)가 있습니다. 핀테크란 금융(financial)과 기술(technique)을 융합한 새로운 융합기술을 뜻합니다. 이와 함께 사물 인터넷(internet of things), 줄여서 IOT도 빼놓을 수 없습니다. 이런 것들이 어떻게 개인의 정보를 감시하고 활용하는지 살펴보겠습니다.

현대는 빅 데이터의 시대입니다. 빅 데이터 시대는 디지털 정보기

술이 있기에 가능해졌습니다. 예를 들어 우리가 누구에게 전화를 하고, 상점에서 신용카드를 쓰고, 현실 세계와 온라인 세계를 드나들 때 거의 모든 것이 기록으로 남습니다. 이러한 기록들을 연관 지어 분석을 해보면 우리의 간단한 개인정보를 비롯해 이동경로, 취미, 소득수준 등 수많은 정보를 알 수 있습니다. 심지어 좋아하는 색깔까지 말입니다. 이런 정보는 오래전부터 기업들이 활용해왔습니다. 신용카드의 혜택을 고르거나 상품을 구입할 때 포인트나 마일리지를 일일이 따져보잖아요? 기업은 고객에게 포인트로 보상을 해주면서도 엄청난 정보를 축적하는 겁니다.

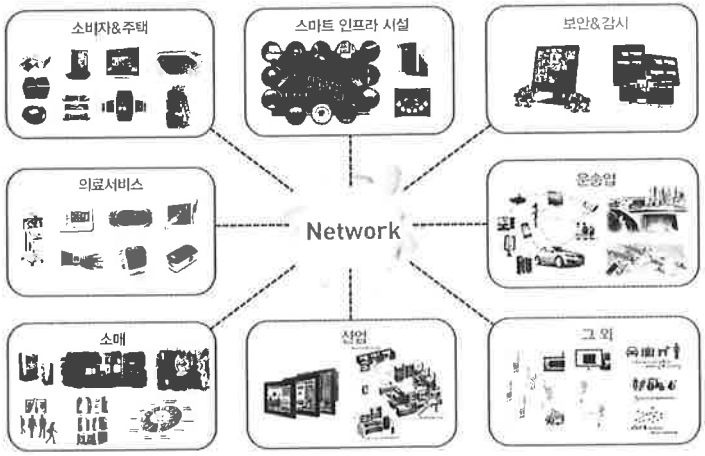
때로는 우리도 모르는 우리 정보를 기업이 먼저 알아챌 때도 있습니다. 미국의 대형마트인 타깃(TARGET)은 말 그대로 타깃을 완벽하게 공략하기로 유명한 기업입니다. 어떤 아저씨가 타깃에 항의 메일을 보냈습니다. 왜 우리 집에 출산 키트를 광고하느냐는 것이었죠. 하지만 아저씨는 모르고 타깃은 아는 비밀이 하나 있었으니, 아저씨의 딸이 임신을 했던 겁니다. 타깃은 임산부가 임신 초기에 많이 사는 영양제를 알고 있었습니다. 그리고 임신 중기가 되면 로션을 많이 산다는 것도 알고 있었습니다. 타깃은 그 아저씨의 딸이 초기에 여러 영양제와 논카페인 제품을 많이 사더니, 중기가 되어서 로션을 구입하는 것을 파악한 뒤 아저씨 집으로 출산 키트 광고지를 보냈던 겁니다. 이게 빅 데이터의 한 사례입니다. 마트가 빅 데이터를 활용한 유명한 사례는 또 있습니다. 바로 월마트의 '맥주와 기저귀 세트'입니다. 아이 아빠들은 기저귀를 사러 왔다가 맥주까지 장바구니에 넣는다는 소비 패턴을 분석한 예입니다. 개인의 스타일, 취향, 이런 것들이 다 공개되는 것이죠. 소비 패턴과 자사 상품을 연관 짓는 매칭 시스템, 고객의 라이프스타일, 고객의 행동 시점에 따른 욕구(needs)를 분석하고 예측하는 알고리즘이 있습니다. 신용카드 사용내역서부터 마트 영수증까지 우리 일상 정보는 CCTV 외에도 무수히 많은 금융기업과 유통기업들로부터 감시당하고 있습니다. 소비 데이터뿐만이 아닙니다. 온라인 쇼핑몰은 각각의 아이디가 언제, 어떤 상품을, 얼마나 자주 검색했는지 기록합니다. 이런 정보를 종합하여 분석하면 기업의 마케팅팀은 한 번도 본 적 없는 사람의 본인도 모르는 고유한 특성까지 분석합니다.

핀테크는 앞에서 이야기한 것처럼 금융과 IT가 합쳐진 것입니다. 우리나라의 삼성페이, 카카오페이 미국의 페이팔, 중국의 알리페이 등 다양한 시스템이 있습니다. 개인의 정보가 전자상거래업체에 계속 기록되는 것이죠. 전자상거래는 모바일화되고 있기 때문에 이런 추세는 점점 심해질 것입니다. 이러한 핀테크 관련 기업 상품들은 지금도 계속해서 출시되고 있습니다.

사물인터넷(IOT)은 개인정보 분석과 감시라는 측면에서 핀테크보다 우리에게 더욱 가깝고 위협적입니다. 사물인터넷이란 위에서 설명한 것처럼 사물들을 인터넷 네트워크로 연결하여 사물과 사물의 정보 혹은 사물과 개인의 정보를 공유하는 지능형 기술과 그 환경을

말합니다. 쉽게 말해서 주변의 모든 사물이 다 네트워크로 연결될 수 있다는 것입니다. 사물은 곳곳에서 정보를 수집하여 각종 서비스 분야에 제공됩니다. 사물인터넷의 네트워크에서는 인간이 배제되기도 합니다. 나아가 사물과 사물뿐만 아니라 현실의 사물과 가상세계의 사물이 유의미한 정보를 주고받으며 분석하기도 합니다. 인공지능이 좋은 예입니다. 냉장고에 물이 떨어지면 물을 채워달라고 하고, 집안 공기가 안 좋으면 공기청정기를 쓰기도 합니다. 아침에 커피를 즐긴다면 7시에 커피포트가 작동하여 커피를 만들어줍니다. 선진국들이 고령화사회로 진입하면서 독거노인의 안전과 건강을 체크하는 데 쓰이기도 합니다. 만약 사람이 움직이지 않은 채 어느 정도 시간이 지나면 자동적으로 병원이나 소방서에 신고가 들어가는 시스템이죠. 사물인터넷은 우리 신체의 상태를 체크하여 관리하는 기능도 합니다. 당뇨병과 같은 지병을 앓는 환자의 혈당 수치가 높거나 신장에 문제가 생기면 경고를 울리고 심할 경우 병원에 연락을 하는 것입니다.

이처럼 사물 인터넷은 현대인의 삶을 매우 편리하게 해줍니다. 하지만 그만큼 위험성도 크지요. 특히 해킹을 당할 경우에는 개인의 프라이버시 침해부터 생명의 위협까지, 다양한 위험에 직면하게 됩니다. 가장 대표적인 예로 웹캠 해킹이 있습니다. 지구 반대편에서 노트북이나 데스크탑의 웹캠을 해킹하여 사생활을 낱낱이 지켜보고 기록하고 유포할 수도 있습니다. 대표적으로 '미스 틴 USA' 캐시디 울



✖ 사물인터넷이란 기존의 인간과 인간의 통신을 넘어 사람과 사물, 사물과 사물이 통신하는 기술이다. 주택의 전등, 가스 밸브, 보일러를 비롯해 공장의 생산 공정의 기기들이 데이터 수집, 모니터링, 제어가 가능하다. 나아가 구글 글라스, 삼성 기어S와 같은 증강현실 기기를 다른 기기들과 연동하여 작동시킬 수 있다.

프의 웹캠 해킹 사건이 있습니다. 어떤 해커가 캐시디 울프의 웹캠을 해킹하여 사생활을 녹화한 후, 자신과 채팅을 하거나 더 선명한 사진을 보내거나 5분 동안 자신이 시키는 대로 행동하기 중에 하나를 선택하라고 협박을 했습니다. 캐시디 울프는 선택지에 없던 '경찰에 신고하기'를 택했고 해커는 체포되었죠. 스마트TV 또한 내장 카메라의 해킹 위험이 있습니다. 도시가스 조절기나 자동차도 예외는 아닙니다. 오히려 이 두 장치는 우리의 안전에 직결되어 있습니다. 자동차가 해킹당하여 브레이크를 밟아도 속도를 줄이지 못해 사고를 당하는 경우처럼 말입니다.

이와 같은 일은 사물인터넷이 해킹당할 위험이 존재하는 한 결코 사라지지 않을 겁니다. 실제로 유명 PC업체인 HP가 미국 가정의 사물인터넷 기기들을 조사한 결과 열 개 가운데 일곱 개가 데이터 보안에 취약한 것으로 드러났습니다. 사물인터넷의 빅브라더는 정보 권력을 쥔 특정 개인이나 집단이 아니라 해킹 기술을 보유한 불특정다수라는 점이 무서운 것입니다. 또한 책임 소재도 불분명합니다. 기기의 결함이나 소프트웨어 오류 혹은 해킹으로 가스가 누출되어 사고가 일어났다고 가정해보죠. 사고 원인이 명확할 경우에도 책임을 져야 하는 주체가 모호한데, 만약 사고 원인조차 알 수 없는 상황이라면 책임은커녕 해커의 소행인지 기기의 결함인지 알 수조차 없게 됩니다.

빅브라더와 리틀시스터의 감시탑에서 벗어나기

편리한 사물인터넷의 부작용은 결국 인권침해입니다. 사물인터넷이 새로운 파놉티콘(Panopticon)이 될지 모른다는 것이죠. 우리는 편리하다는 이유로 사물인터넷을 쓰지만, 실상은 사물인터넷의 정보를 독점한 이들이 감시탑에서 우리를 감시하고 통제한다는 뜻입니다. 미셸 푸코는《감시와 처벌》에서 바로 이 파놉티콘을 예로 들며 권력행사 방식이 변화했다고 말합니다. "권력은 소유하는 것이 아니라 작용하는 것이며, 억압하는 것이 아니라 생산하는 것"이라고

말이죠. 이 말의 주체를 현대 기업들에게 그대로 적용해봅시다. 오싹하지 않습니까? 정보혁명의 미래에 우리 인간이 자유와 해방을 맞이할 것이라고 단정할 수 있겠습니까?

우리를 편리하게 하는 기기와 시스템이 사생활을 침해하는 문명의 이기로 변질되고 있습니다. 진정 두려운 일입니다. 우리의 일상이 도청되고 감청됩니다. 첨단 도청장치를 사용하면 몇 백 미터 떨어진 곳에서도 대화를 엿들을 수 있습니다. 첨단 장비가 아니더라도 도청이 가능한 특수한 사례도 얼마든지 있습니다. 프린터, 에어컨, 세탁기를 이용한 도청입니다. 이런 생활·사무기기를 해킹하여 특수한 전자기장을 내뿜게 만든 후 0과 1로 신호를 보내게 합니다. 데이터 전송이 다소 오래 걸리는 단점이 있지만 컴퓨터나 스마트 기기 없이 정보를 빼내 올 수 있다는 점이 충격적입니다.

우리가 감시 사회로 점점 빠져들면서 생각해봐야 하는 중대한 문제가 하나 있습니다. '국가란 무엇인가'입니다. 예를 들어 2015년에 불거진 국정원 해킹 프로그램 도입 논란이 있습니다. 국정원이 이탈리아 밀라노에 본사를 둔 '해킹팀'이라는 기업으로부터 해킹 프로그램을 구입했습니다. 정부는 이 해킹 프로그램의 용도가 대북 첩보라고 하지만 해킹 대상으로 의뢰한 IP 138개를 분석해보니 국내 고층 빌딩의 공기조절 시스템과 CCTV 시스템이 포함되어 있었다고 합니다. 또한 해킹 가능한 프로그램에는 카카오톡을 비롯해 페이스북, 텔레그램 등의 SNS도 다수 확인되었죠. 국정원의 해명에도 불구하고

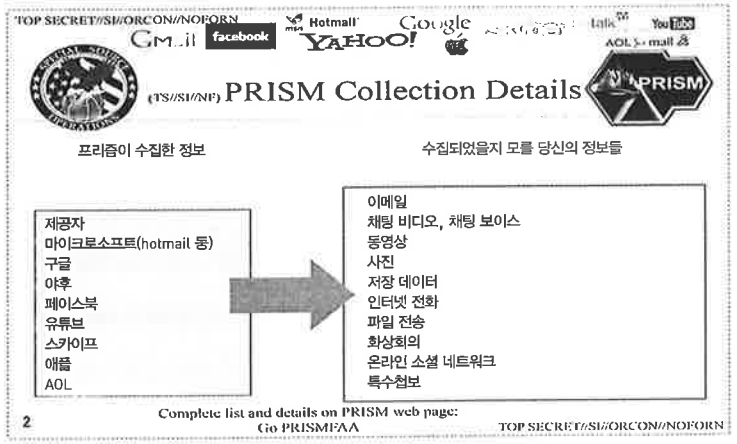
의혹이 가시지 않는 이유겠지요.

이쯤에서 질문 하나를 던져볼게요. 국가가 왜 필요합니까? 국가의 존재 이유가 뭡니까? 현대 국가는 사회주의와 자유주의 두 가지 성향을 모두 가지고 있습니다. 사회주의는 국민의 사회보장·사회복지를 위해, 자유주의는 자유와 조화를 보장하기 위해 필요합니다. 자유주의와 사회주의 모두 국가 존재를 전제로 의미가 있습니다. 국가가 없으면 사람들은 서로 감시하고 알아서 지켜야 합니다. 근대적 의미의 국가가 처음 등장했을 때, 자유권과 재산권을 일부 양보하면서 국가를 만들었다는 것이 사회계약설입니다. 문제는 국가 권력이 점점 강력해진다는 것이죠. 현대에 들어서 정보권력 측면에서 더욱 심각해졌습니다. 정보가 점점 국가에 집중되고 있기 때문입니다. 세계가 지식정보 사회로 나아가는 상황에서 정보의 중요성이 커졌습니다. 하지만 국가의 정보권력이 국민을 보호하고 자유를 보장하는 차원을 넘어서 위협하는 수준에 이르렀습니다.

정보권력은 국가와 시장 그리고 개인으로 나눠볼 수 있습니다. 가장 심각한 것은 국가의 정보권력 남용입니다. 국가가 정보권력을 남용할 때 국민의 인권이 침해받게 마련이죠. 미국의 정보권력은 9.11테러 이전과 이후로 확연하게 나뉩니다. 미국에서 10년 가까이 살았던 저는 9.11테러가 발생한 후 이곳이 내가 알던 미국이 맞나 싶을 정도로 달라졌다고 생각합니다. 미국 본토가 처음으로 공격을 받아 자국민이 희생되었다는 것은 거대한 충격이었습니다. 그 반동으로

1 미국 오바마 대통령은 프리즘 폭로 사건 이후 동맹국 정상들의 항의 전화에 시달려야 했다. 문제는 독일도 2012년에 미국의 힐러리 클린턴 당시 국무장관과 존 케리 현 국무장관의 위성전화 통화를 도청했다는 것이다.

2 적국을 포함해 동맹국과 자국민의 정보까지 불법 감청하여 문제가 된 미국의 프리즘 프로그램.



프리즘과 같은 광범위 도청 시스템이 등장했습니다.

시장의 정보권력은 어떤 상황일까요? 개인의 통화내역이나 문자서비스 내역이 KT와 LGT, SKT 등 통신사업자의 데이터베이스에 모두 기록되고 있습니다. 물론 일정 기간이 지나면 삭제가 된다고 하지

만 말입니다. 인터넷 포털사이트의 영향력도 무시할 수 없습니다. 이메일 기록, 쪽지, 카페, 블로그, 검색어 등 개인이 온라인에서 활동한 내역이 지문처럼 남습니다. 신용카드 회사부터 음식점 검색 어플리케이션 기업까지 개인의 정보를 수집하여 기업의 이익을 위해 활용합니다. 파워블로거도 권력자입니다. 자영업자들에게 횡포를 부렸다는 뉴스가 심심찮게 등장하곤 하지요.

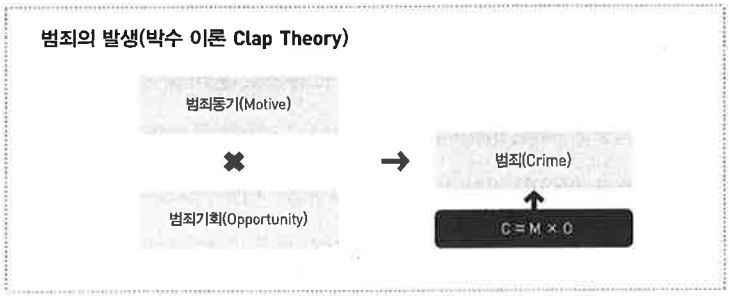
과거에 정보권력을 쥔 이들을 빅브라더라고 한다면 지금은 '리틀 시스터'가 있습니다. 기업, 개인의 정보남용 위험성이 커지고 있다는 뜻입니다. 해킹은 또 다른 측면의 위험입니다. 가장 유명한 해킹 집단으로 '어나니머스'를 들 수 있습니다. 영화 〈브이 포 벤데타〉를 보면 주인공 브이가 가이 포크스 가면을 쓰고 나옵니다. 어나니머스가 이 가면을 자신들의 심볼로 삼고 있죠. 어나니머스는 톰 크루즈가 어느 종교단체에서 강연한 것을 해킹한 것으로 첫 유명세를 탔습니다. 그렇다면 정보권력의 근간이 되는 정보기술은 근절해야 하는 걸까요? 그렇지 않습니다. 순기능도 얼마든지 있기 때문입니다.

범죄 예방을 위한 박수공식(C=M×O)

정보기술의 가장 대표적인 순기능은 편리성입니다. 현대 한국 사회에서 휴대폰이 없는 사람이 몇 명이나 될까요? 정보기술은 현대인에게 편리함을 주지만 더 많은 정보기술, 더 많은 IT 기기를 사용하면 그만큼 더 많은 정보가 외부로 흘러들어갑니다. 편리성과 보안성은 서로 반비례하는 법입니다. 만약 철저한 보안을 보장하는 사회가 된다면 우리는 지금보다 더욱 마음 편하게 정보기술을 활용할 수 있을 겁니다.

CCTV는 개인의 인권을 침해할 위험이 있지만 범죄 예방과 범죄자 체포에 기여를 하기도 합니다. 환경설계를 통한 범죄예방(CPTED, Crime Prevention Through Environmental Design)이 대표적인 예입니다. CPTED는 범죄를 유발하는 환경 요인을 제거하거나 최소화하여 범죄율을 낮추는 것이 목표입니다. 범죄 발생 지역을 은폐하는 게 아니라 오히려 잘 보이게 해서 범죄가 일어나지 않도록 하는 것이죠. 다른 예로 모스키토 시스템(The Mosquito)이 있습니다. 이 기계의 원리는 청소년만 들을 수 있는 16,000~18,500Hz의 주파수를 방출하여 불쾌감을 유발시킴으로써 자리를 뜨게 만드는 것입니다. 주로 폐가나 청소년출입금지 업소에 설치하며 청소년의 일탈을 방지하는 대표적인 시스템입니다.

이처럼 현대 정보기술은 범죄를 예방하는 데 큰 역할을 하기도 합니다. 범죄에 관한 여러 이론 가운데 '박수 이론'이 있습니다. 공식은 C=M×O입니다. C는 범죄(crime), M은 동기(motive), O는 기회(opportunity)입니다. 범죄가 발생하려면 범죄동기와 범죄기회가 만나야 한다는 뜻이죠. 범죄를 줄이려면 범죄동기와 가능하다면 범죄기회를



✖ 범죄는 범죄동기와 범죄기회가 만나 발생한다. 뒤집어 말하면, 동기나 기회 가운데 하나만 0이어도 범죄는 일어나지 않는다는 뜻이다.

줄여야 합니다. 범죄동기는 유전적인 코딩과 성장기의 코딩으로 벌어집니다. 코딩이 어떻게 발휘되느냐에 따라서 범죄자가 되느냐 되지 않느냐가 나뉩니다.

범죄에 대한 동기는 신념화와 합리화의 과정을 거치며 변화합니다. 코딩이 되면 편견이 됩니다. 더 심해지면 신념이 되고 말지요. 그러면 괴물이 되고 권력을 남용하게 되는 겁니다. 범죄기회는 감시가 미미할 때, 보안이 취약할 때 범죄율이 크게 증가합니다. 범죄동기는 어떻게 차단시켜야 할까요? 편견과 이기심을 없애야 합니다. 결과적으로 교육으로 범죄를 예방할 수밖에 없다는 뜻이죠. 이와 함께 민주주의와 법치주의를 강조해야 합니다.

그렇다면 정보권력의 범죄기회는 어떻게 줄일 수 있을까요? 가장 좋은 방법은 우리를 감시하는 사람들을 감시하는 것입니다. 이걸 시놉티콘(synopticon)이라고 합니다. '서로 동시에 감시한다'는 뜻이며

대중이 권력자를 역으로 감시한다는 뜻이죠. 지금 우리가 권력자들을 감시하는 정도로는 부족합니다. 미국의 예를 봅시다. 미국 국민은 9.11테러 이후 국가 안보를 최우선으로 여겼습니다. 자의에 따라 개인의 자유가 다소 줄어드는 것은 감내했죠. 하지만 국가가 정보권력을 쥐고 프리즘 시스템을 통해 동맹국과 자국민의 정보까지 감청했다는 사실에 미국민은 경악했습니다. 그리고 정부에게 국민의 개인정보 보호를 보장하라고 압박을 넣었습니다.

우리도 그렇게 해야 합니다. 국회, 법원, 헌법재판소, 언론, 시민단체를 통해 국가와 정보권력에 대한 감시를 지금보다 더 철저하게 해야 합니다. 개인정보 보호에 관련된 법도 강화해야 합니다. 시장의 정보권력도 감시해야 합니다. 2014년 1월에 언론을 통해 알려진 카드사 개인정보 유출사건을 보세요. NH농협카드는 개인정보 유출 확인 페이지에 입력한 정보를 암호화조차 하지 않고 평문으로 전송했습니다. KB국민카드는 개인정보 유출 확인 웹사이트를 만들어놓는다면서 타인의 생년월일과 주민등록번호 끝자리를 입력하면 이메일, 휴대전화를 비롯해 전체 주민번호, 자택주소, 결제계좌와 연소득까지 표시되게 만들었습니다. 두 카드사 모두 유출 확인 사이트를 통해 피해자의 정보를 더 널리, 더 많이 유출한 것이죠. 보안의 기본도 모르는 조치였습니다. 시장의 정보권력이 잘못된 길로 빠지지 않게 하기 위해서는 어떻게 해야 할까요?

우리를 감시하는 이들을 감시하라

지금까지 빅 데이터와 사물인터넷 그리고 핀테크는 완벽하지도 않거니와 권력으로 활용하려는 목적으로 얼마든지 우리의 인권을 침해하고 개인정보를 유출시킨다는 사실을 살펴봤습니다. 이 문제들을 단기간에 쉽게 해결할 방법은 없습니다. 왜냐하면 국가 정보권력의 순기능인 '보호'와 개인이 보장받아야 하는 '인권'이 때때로 상충하기 때문입니다. 모든 사람은 범죄로 인한 피해와 두려움으로부터 자유롭고 싶으면서도, 자신의 기본적인 인권을 보호받고 싶어 하기 때문에 갈등합니다. 더욱이 두 가지 기본적인 욕구 그 어느 것도 쉽게 포기할 수 있는 성질의 것이 아닌 데다가, 다른 한쪽의 축소를 수반한다는 점에서 범죄 통제를 강조하는 입장과 인권을 강조하는 입장은 첨예하게 대립할 수밖에 없습니다. 하지만 보호와 인권, 둘 모두 매우 중요한 가치입니다. 이는 시장과 개인의 정보권력에도 똑같이 작용합니다. 시장의 정보권력은 일견 우리에게 편리함을 제공하지만 동시에 개인정보 보호를 완벽하게 보장하지 않습니다. 개인의 정보권력도 마찬가지입니다. 우리가 어디서나 손쉽게 스마트폰으로 정보를 얻을 수 있도록 여러 개인이 정보를 공유하지만 그 과정에서 불가피하게 개인이나 단체, 국가의 정보가 유출됩니다. 모두 양면성이 있습니다.

정보권력이 문제가 된다고 정보기술을 폐기할 수는 없지 않습니까? 지구온난화를 방지한다는 이유로 석유 사용을 전면 금지할 수는 없는 것과 마찬가지입니다. 화석연료 사용으로 인한 대기오염 문제를 해결하기 위해 전기자동차 등과 같은 제3의 대안이 등장했습니다. 마찬가지로 정보권력의 남용을 막기 위해서는 감시자를 철저히 감시할 수 있는 '역감시 시스템'을 제대로 운용하는 것이 중요합니다. 권력기관과 국민이 동시에 서로를 감시하는 일종의 시놉티콘(Synopticon) 시스템이 필요한 것입니다. 이러한 역감시 시스템 작동 등을 통해 정보권력 남용에 따른 부작용을 최대한 줄여나가는 법적, 제도적 보완 노력이 필요하다고 봅니다.

미래에 우리의 일거수일투족과 나아가 사고까지 지배하려는 빅 브라더와 리틀시스터에에 맞서야 합니다. "We are watching you." 억압받지 않기 위해 대중이 정보권력을 쥔 자의 눈을 똑바로 보며 할 말입니다.